Edited by
Horst Treiblmaier · Roman Beck

Business Transformation through Blockchain

Volume II

palgrave
macmillan

Business Transformation through Blockchain

Horst Treiblmaier • Roman Beck
Editors

Business Transformation through Blockchain

Volume II

palgrave
macmillan

Editors
Horst Treiblmaier
Department of International Management
MODUL University Vienna
Vienna, Austria

Roman Beck
Head of European Blockchain Center
IT University of Copenhagen
Copenhagen, Denmark

ISBN 978-3-319-99057-6 ISBN 978-3-319-99058-3 (eBook)
https://doi.org/10.1007/978-3-319-99058-3

Library of Congress Control Number: 2018959421

This Palgrave Macmillan imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface Volume II

The second volume of *Business Transformation through Blockchain* contains four sections and an appendix. It starts with a selection of use cases from a variety of different industries, such as tourism, energy, the Internet of Things, and healthcare. In the following section on sustainability, several papers discuss the potential of the blockchain to create a more sustainable economy, ranging from a circular economy to questioning the economic growth paradigm as such. Societal impacts, which are closely connected to the preceding section, also deal with issues such as sustainability and a circular economy but also include topics related to digital identity and e-government as well as banking for the unbanked. The section on legal issues concludes this second volume by investigating whether smart contracts are a threat for the legal industry and how the blockchain might impact intellectual property management.

In the first section, selected use cases from different industries are presented. *Horst Treiblmaier* and *Irem Önder* use data from expert interviews to create a theory-based blockchain research framework for the tourism industry. *Jens Strüker*, *Simon Albrecht,* and *Stefan Reichert* have a close look at the energy sector and present some ideas on how blockchain might potentially impact this sector in the not-so-far-off future. *Chun-Feng Liao*, *Chien-Che Hung,* and *Kung Chen* examine the state of the art of the Internet of Things and consider design issues regarding blockchain integration from a software architecture perspective. In the second paper on the Internet of Things, authors *Daniel Burkhardt*, *Patrick Frey*, *Simon Hiller*, *Alexander Neff,* and *Heiner Lasi* argue that distributed ledgers will enable new opportunities to replace existing components on all layers of industrial IT architecture. *Sachin Shetty, Xueping Liang, Daniel Bowden, Juan Zhao,* and *Lingchen Zhang* present a mobile healthcare system for personal health data collection, sharing, and collaboration between individuals and healthcare providers, as well as insurance companies. The section about sustainability starts with *Marcus Dapp*, who argues for a new economic approach that has sustainability built into its core design by using cryptoeconomics based on blockchain technology to create incentive systems which encourage sustainable behavior. *Dave Leonard* and *Horst Treiblmaier* question the economic growth paradigm and ask the question whether cryptocurrencies can help to create a more sustainable economy. In the society section, *Niels Faber* and *Jan Jonger* address the question of how blockchain can be used to address societal changes and present a framework that helps to decouple assets and impacts. *Clare Sullivan* and *Eric Burger* examine the legal and technical implications of the application of blockchain technology to authenticate and verify identity for e-Government services and transactions. *Guillermo Jesús Larios-Hernández* and *Almendra Ortiz-de-Zarate-Béjar* elaborate on blockchain's decentralized approach to trust and how it can help to create trust in financial services among the unbanked. The section on legal issues is opened by *Bernhard Waltl*, *Christian Sillaber*, *Ulrich Gallersdörfer*, and *Florian Matthes* who investigate how blockchain can potentially disrupt the legal industry by differentiating between various pillars of the system. *Kensuke Ito* and *Marcus O'Dair* examine the application of blockchain technology to intellectual property management. Finally, this volume includes an appendix from *Aljosha Judmayer*, *Nicholas Stifter*, *Philipp Schindler,* and *Edgar Weippl* in which some central blockchain concepts are explained in a manner that is easy to understand.

It is too early to predict what the future will look like, given the novelty of blockchain. However, it can be expected that in the years to come we will hear about spectacular failures, amazing success stories, and unexpected use cases. It is therefore even more important that academics start to rigorously investigate this field and partner with practitioners in order to systematically investigate the potentials and pitfalls of blockchain technology. The two volumes of this book aim to support both academics and practitioners in better understanding potential implications of blockchain and in developing new ideas, innovations, and maybe even surprising new use cases. It will be an interesting journey, but one that has the potential to change business and society as we know them.

Vienna, Austria Horst Treiblmaier
Copenhagen, Denmark Roman Beck

Contents

Notes on Contributors

Simon Albrecht is a doctoral candidate at the chair of Information Systems at the University of Freiburg and research associate at the INEWI in Frankfurt. Earlier, he obtained his B.Sc. and M.Sc. in Economics at the University of Freiburg. Apart from holding Data Science/Business Intelligence Lectures and Seminars, his main research focus is on adoption, system design, and business models of the blockchain technology. Currently he is working on blockchain research studies (for dena and BDEW), as well as on blockchain implementations in demonstration projects (e.g. “enera”, funded by the Federal Ministry for Economic Affairs and Energy).

Daniel Bowden is the Chief Information Security Officer (CISO) for Sentara Healthcare, an integrated delivery system plus health plan—the largest health system in Virginia. Dan has been at Sentara since September 2016. He was previously CISO at University of Utah Healthcare and the University of Utah for over 3 years. Dan has worked in cybersecurity and technology in healthcare, higher education, banking, retail, and the military over the past 25 years. His current professional interests are DevSecOps, cybersecurity tradecraft at scale, and blockchain technologies.

Eric Burger is a Research Professor of Computer Science at Georgetown University in Washington, DC, USA. He received an SBEE, MBA, and PhD in Computer Science from the Massachusetts Institute of Technology, Katholieke Universiteit Leuven, and Illinois Institute of Technology. He is currently on detail to the United States Federal Communications Commission serving as Chief Technology Officer (CTO). Prior to his arrival at Georgetown in 2011, Dr. Burger held numerous CTO and SVP/VP Engineering roles at publicly listed, private equity, and venture backed corporations in the network equipment, enterprise software, and electronic design automation markets. His research interests include the technology, policy, legal, and economic aspects of cyber security, protocol design, secure communications, network access for underserved communities, and applications of distributed computing such as blockchain. Dr. Burger has served on numerous corporate boards and is currently Chairman of the Board of atfCYBER. Dr. Burger has numerous IEEE publications as well as law journal articles co-authored with Dr. Sullivan. He also has 20 issued US Patents and 18 published IETF RFCs. The RFC series define the protocols that create the Internet.

Daniel Burkhardt leads the research field on Distributed Blockchain and IIoT at the Ferdinand-Steinbeis-Institute. The field is divided into the areas of research, prototyping, transfer and projects, which together comprise an optimal environment in which to grasp the topic and provide expertise for the industry and academic partners.

During his time at Robert Bosch GmbH as a participant in the Junior Managers Program he had the opportunity to build up specialist knowledge in the areas of IoT, business intelligence, cloud computing and ecosystems in different departments. Additionally, he was able to enhance his competence in leadership. On his six month, short-term assignment in India, he overtook independent conception tasks and supported the realization of the IT reorganization.

Burkhardt deepened his theoretical knowledge during his Master's studies in information systems. And he got to know new IT sectors while studying at the University of Oregon, USA for seven months. In his Master's thesis he came to the conclusion that the connection of business and IT with the use of various methodologies, such as service-oriented architecture and enterprise architecture management, is essential to act fast in a volatile market.

Kung Chen is Professor of Computer Science and Management Information Systems at NCCU, Taipei, Taiwan. He received a PhD in Computer Science in 1994 from the Yale University and has since worked in both the academia and the industry for more than 20 years. His current research interests include blockchain, smart contracts, and token economy. At NCCU, he leads a team of four professors and more than 15 students that works on both theoretical and practical topics of blockchain, such as distributed consensus algorithms, privacy enhancement technologies, smart contract testing tool, and innovative applications. He also serves as the Vice Chairman of the FinTech Research Center at NCCU, which is also the FinTech center of the GloRIA Program launched by the Ministry of Science and Technology of Taiwan in 2017. His research has appeared in journals such as *Automated Software Engineering, Science of Computer Programming, International Journal of Medical Informatics, and Computer Methods and Programs in Biomedicine*.

Marcus M. Dapp is a senior PostDoc at the Professorship of Computational Social Science at ETH Zürich, Switzerland. His research focus is the potential of new modes of large-scale self-organization based on openness and decentralization paradigms: How can cryptoeconomic mechanisms built on distributed ledger technologies like blockchain empower P2P communities toward effective collective action—ideally to tackle global sustainability challenges. He coined the term "digital sustainability" in 2004 to describe the transfer of the sustainability concept to digital goods and runs the "digital sustainability" lecture at ETH since then, for which he was awarded a Golden Owl teaching award in 2012. He is responsible for the academic side of the Blockchain and IoT School (BIOTS), and coruns the seminar on Digital Ethics with Prof. Dr. Dirk Helbing. Prior to this, he led "Open Data and Information Management" at fortiss, an independent research institute affiliated with TU Munich. Before that, he was a co-founding board member of Open Knowledge Germany and an IT Strategist at the City of Munich. He holds a BA in Computer Science, an MSc in Technology Innovation Management, and received his PhD from ETH Zürich on the effects of software patent policy on open source innovation.

Niels Faber is a researcher at Radboud University Nijmegen and a lecturer at Hanze University of Applied Sciences in Groningen. His research focuses on the organisational aspects of sustainability. This is translated into themes such as new forms of organisation focusing on the circular economy in particular, the transition this entails, and measuring the progress made in it. He has written over 50 publications and, together with Jan Jonker, he is co-author of a series of online columns on the circular economy.

Patrick Frey is studying for a Master's in Information Engineering at the Institute of Technology in Karlsruhe. He is writing his Master's thesis at the Ferdinand-Steinbeis-Institute on intelligent multi-agent systems.

Before the Master's, he completed education as an IT specialist in the domain of system integration. He then studied for his Bachelor's degree in business informatics at the University of Applied Science, Karlsruhe. During this time, he worked as a software developer in a medium-sized software consulting company.

Ulrich Gallersdörfer is a researcher at the chair for Software Engineering of Business Information Systems (sebis) at the TUM since September 2017. He holds a master's degree in Information Systems. In his research, he focuses on applications and use cases of blockchain and distributed ledger technologies. As coordinator of the blockchain.tum.de cluster, he fosters interdisciplinary research in blockchain with different chairs of the TUM.

Simon Hiller works as a research assistant at the Ferdinand-Steinbeis-Institute, in the research area of industrial internet and Industry 4.0; his special subject topic is additive manufacturing.

From 2011 to 2015 he studied medical engineering (B.Sc.) at the University of Stuttgart, Germany and the Eberhard Karls University of Tuebingen, Germany. He graduated 2017 as Master of Business Engineering (MBE) at the Steinbeis University Berlin, Germany.

In his field of research, Hiller explores additive manufacturing as a technology from a business perspective. This includes additive manufacturing-enabled business models, value networks and platforms.

Chien-Che Hung received the BS degree in Management Information Science from the Chang Gung University in 2017. He is doing master's degree in Computer Science at NCCU, Taipei, Taiwan. His research interests include the blockchain technology and Web programming.

Kensuke Ito is a Ph.D. student in the Graduate School of Interdisciplinary Information Studies at the University of Tokyo. His primary interest is the process of value creation in the field of arts and culture. Specifically, he has been conducting a theoretical study in the field of *cumulative cultural evolution*, aimed at clarifying the determinants of the accumulation speed of cultural traits. His main contribution in the field is an application of the methods of economic growth theory, which is based on rational agents trying to maximise their own utility. In addition, he is researching blockchain technology as a practical output of his theory. By combining blockchain's technical property and appropriate incentive design, he is currently designing an autonomous system for promoting user-generated cultural accumulation.

Jan Jonker is Professor of Sustainable Enterprise at Radboud University. In addition, he has held the Chaire d'Excellence Pierre de Fermat at Toulouse Business School in France for the past two years. His work focuses on three related themes: the emergence of the WEconomy, the development of new business models, and transaction systems with more than money alone or 'hybrid banking'. Along with over 40 people, he wrote the bestseller 'Nieuwe Business Modellen; Samen Werken aan Waardecreatie' (2014), for which there is an English translation [New Business Models; Working Together on Value Creation], which is linked to a Massive Open Online Course at the platform Iversity. You can register for this free MOOC via: bit.ly/1TRfa8A. Jan Jonker and Niels Faber have recently been working together in a team on the National Survey of Business Models for the Circular Economy. The results of this survey were presented in May 2017 during a national conference. The report presenting the outcomes was published in Dutch and in an English translation.

Aljosha Judmayer is security analyst and researcher at SBA Research. His research focuses on cryptocurrencies and their underlying technologies and consensus mechanisms. He received his master's degree in Software Engineering and Internet Computing from TU Wien. He is working toward his PhD degree on foundations and applications of distributed ledger technologies (i.e., blockchains). His research interests include network security, resilience aspects of distributed systems, and systems security. He has participated in national and international cryptocurrency projects, including A2Bit and Bitcrime. Moreover, he has contributed to a book on cryptocurrency technologies and held tutorials on that topic at WWW 2016 and at ACM CCS 2016.

Guillermo Jesús Larios-Hernández is Professor of Entrepreneurship and Technology Transfer at Anáhuac University Mexico. He chairs the Entrepreneurship research group and academic programs. He holds a PhD in Economics from Mexico's National University (UNAM), a master's degree in Technology Commercialization in Institute IC2 from University of Texas, and a French Mastere in Satellite Communications Systems from Ecole Nationale Supérieure des Télécommunications. He has professional experience working at Siemens, AT&T-Alestra, and Global Affairs Canada. His research interest includes entrepreneurship, innovation and technology, blockchain entrepreneurship, economic systems, and the digital economy. His research has appeared in journals such as *Business Horizons*, *Information Technology for Development*, and *Technology Management & Innovation*.

Heiner Lasi is head of the Ferdinand-Steinbeis-Institute at the Steinbeis Foundation and Full Professor for Industrial Intelligence at the Steinbeis University Berlin. He also chairs the management board of the Steinbeis-Transferzentrum Innovationsforum Industrie (STCII), which runs the Industrial Internet Consortium German Regional Team. In applied research activities, he addresses topics in the field of industrial internet and Industry 4.0 from a management perspective.

He also serves on industrial and academic conference program committees and speaks on the challenges and chances of successfully adapting business capabilities based on digital transformation and new technologies.

David Leonard is a researcher and lecturer in the Department of Sustainability, Governance and Methods at MODUL University Vienna. David received his Ph.D. in Business and Socio-Economic Science from MODUL University in 2018. This research focuses on the governance role played by third-sector actors in steering economic activity toward models characterized by greater inclusiveness and reduced environmental impact. Based on a thorough understanding of the environmental challenges facing society from an ecological economics perspective, David's current research interests are focused on the implementation of reforms recognized as indispensable for the transition to a sustainable society. To these research endeavors, David brings a solid economic background and comprehensive knowledge of governance mechanisms at all levels. His research has appeared in the journal *Applied Economics*.

Xueping Liang is a visiting research scientist in Old Dominion University, USA. She is a PhD student in University of Chinese Academy of Sciences, and Institute of Information Engineering, Chinese Academy of Sciences. She received the BS degree (2013) from the Department of Electrical Engineering, Beijing Institute of Technology. From 2015 to 2018, she worked in Cyber Security Lab at Tennessee State University as a visiting scholar. Her research interests include the security of blockchain system and applications, decentralized architecture design, blockchain in healthcare, and Internet-of-Things (IoT). She has much experience in the data and information security analysis, and secure system architecture design. Her research has been presented in conferences such as IEEE CLOUD 2017, IEEE/ACM CCGRID 2017, ICICS 2017, MILCOM 2017, PIMRC 2017, and SECURECOMM 2018, and has appeared in journals such as *International Journal of Information Security and Privacy*, with a total of more than 12 scholarly papers published. She is a reviewer of the *IEEE Consumer Electronics Magazine* and The 15th International Conference on Information Technology (ICIT 2016).

Chun-Feng Liao is assistant professor in the Department of Computer Science and Program in Digital Content and Technologies at National Chengchi University (NCCU), Taipei, Taiwan. He received the BS and MS degrees in Computer Science from the NCCU and the PhD degree from National Taiwan University in 1998, 2004, and 2011, respectively. His research interests include blockchain-oriented software engineering, services computing, and context-aware pervasive systems and networks.

Florian Matthes holds the chair for Software Engineering for Business Information Systems at Technische Universität München. The current focus of his research is on technologies driving the digital transformation of enterprises and societies: enterprise architecture management, service platforms and their ecosystems, semantic analysis of legal texts, and executable contracts on blockchains.

Alexander Neff has worked as research assistant at the Ferdinand-Steinbeis-Institute for Digitalization since August 2018. He received his Bachelor's degree in social sciences from the University of Stuttgart in 2012 and his Master's in business sociology from the University of Trier in 2016. After his graduation he worked as an academic at the University of Heilbronn for Applied Sciences (Reinhold-Würth-Hochschule, Künzelsau), where he lectured in research methodologies and oversaw the market research projects of the students.

At the Ferdinand-Steinbeis-Institute, his research focus is on economic ecosystems (business, innovation and entrepreneurial ecosystems) and enterprise collaboration. In addition, he is assisting in the lectures on research methodologies in information systems at the Steinbeis University Berlin.

Marcus O'Dair is Associate Professor in Music and Innovation at Middlesex University in London, and convenor of the Blockchain for Creative Industries research and teaching cluster. He has published academic research in peer-reviewed journals including *Popular Music*, *IASPM@Journal* and *Strategic Change*, and contributed to edited collections including *Jazz and Totalitarianism* (2017) and *Punk Pedagogies* (2018). He has also written for publications including the *Guardian*, the *Independent*, the *Times*, the *Financial Times*, the *Irish Times,* the *Wire*, *Uncut* and *City Metric* (*New Statesman*), and appeared on CNN, BBC Radio 1, BBC Radio 3, BBC 6 Music and the BBC World Service. *Different Every Time*, his 2014 biography of Robert Wyatt, was a Radio 4 book of the week and was shortlisted for the Penderyn music book prize. He is currently examining the impact of blockchain technology on the creative industries as researcher in residence at Digital Catapult. A former session musician with Passenger, he has also released three acclaimed albums and toured Europe as one half of Grasscut.

Irem Önder is an Associate Professor at the Department of Tourism and Hospitality Management at MODUL University Vienna. She obtained her PhD from Clemson University, South Carolina, where she worked as a research and teaching assistant from 2004 until 2008. She obtained her master's degree in Information Systems Management from Ferris State University, Michigan. Her main research interests include information technology and tourism economics, specifically big data analysis, smart destinations, decision support systems, blockchain, and tourism demand forecasting. She serves on the editorial boards of *Journal of Travel Research* and *Journal of Information Technology and Tourism*. Her research has been published in journals such as *Annals of Tourism Research, Tourism Management, Journal of Travel Research, Tourism Economics,* and *Journal of Information Technology and Tourism*.

Almendra Ortiz-de-Zarate-Béjar holds a master's degree in Public Administration and is pursuing PhD in Strategic Management and Development Policies at Anáhuac University Mexico. She is a researcher at the Anáhuac Center for Research in International Relations and columnist at the Anáhuac International Forum of the *Excélsior* newspaper and the magazine *Consultoría*. Her work includes titles such as "Libya the end of the spring. The Libyan conflict analyzed by theories of IR", "Diplomatic Relations between Cyprus and Latin America", "Humanitarian crisis: Unaccompanied migrant minors from Central America to the US-Mexican border", and "Financial inclusion, mobile banking and remittances in Mexico and the Philippines".

Stefan Reichert has obtained a doctoral degree in Information Systems in 2018 from the University of Freiburg in Germany. He obtained his M.Sc. in Economics at University of Freiburg and his B.Sc. at the University of Heidelberg. Besides his work as a consultant in the energy sector, he is a guest lecturer for energy trade at the INEWI in Frankfurt. As part of his research experience, he was involved in various research projects within the European Union and Germany. In the EU-funded research project "iUrban", he was a work package leader for the University of Freiburg. His research focuses on the evaluation of flexibility in energy generation, consumption, and storage, as well as data-driven business models in the energy sector.

Philipp Schindler holds a master's degree and is employed as researcher and IT security expert at SBA Research. In May 2015, he received his bachelor's degree in Software and Information Engineering from the Vienna University of Technology. Alongside his studies he gathered two years of experience working as an informatics teacher and IT system administrator. In 2015/2016, he was accepted for the university's high potential program TUtheTOP in cooperation with Accenture and Infineon. In his master thesis (Software Engineering and Internet Computing at TU Wien) he focused on the areas of security and scalability of distributed ledger technologies and their consensus algorithms. He is part of the blockchain research group at SBA Research, led by Edgar Weippl and Aljosha Judmayer, and pursuing his PhD studies at TU Wien.

Sachin Shetty is an associate professor in the Virginia Modeling, Analysis, and Simulation Center at Old Dominion University. He holds a joint appointment with the Department of Modeling, Simulation and Visualization Engineering and the Center for Cybersecurity Education and Research. Sachin Shetty received his PhD in Modeling and Simulation from the Old Dominion University in 2007. His cyber security lab at VMASC conducts basic and applied research on developing cyber risk and resilience techniques to protect next generation Internet, cloud, mobile, and critical infrastructure. Recently, he is developing blockchain empowered solutions to address cyber security issues in distributed systems for Air Force Research Lab, Air Force Space Command, Department of Energy, and Sentara Healthcare. His laboratory has received over $10 million in funding from National Science Foundation, Air Office of Scientific Research, Air Force Research Lab, Office of Naval Research, Department of Homeland Security, and Boeing. He has authored and coauthored over 140 research articles in journals and conference proceedings and two books. He is the recipient of DHS Scientific Leadership Award and has been inducted in Tennessee State University's million-dollar club. He has served on the technical program committee of ACM CCS, IEEE INFOCOM, IEEE ICDCN, and IEEE ICCCN.

Christian Sillaber is a senior researcher and lecturer at the University of Innsbruck. He holds a PhD in computer science and a law degree. His research projects focus on compliance and governance in decentralized cryptocurrencies, privacy management and enforcement in virtual currency ecosystems, and the role of technology in regulatory compliance. He is a member of ISO/ASI working groups on blockchain standardization and privacy and executive committee member of the GI working group on legal informatics.

Nicholas Stifter received a master's degree in Computer Science Management with distinction and a bachelor's degree in Software Engineering from Vienna University of Technology. He is working toward his PhD degree on security and maintainability aspects of block chain technologies and smart contracts, and his research interests include Nakamoto consensus, distributed agreement protocols and computing education for distributed systems topics.

Jens Strüker is the managing director of the Institute for Energy Economics (INEWI) at Fresenius University of Applied Sciences Frankfurt, Germany. Jens received his PhD and habilitation in information systems and business administration from the University of Freiburg, after working as a visiting researcher at SAP Labs, Palo Alto. Currently, he is supervising several publicly and industry-funded blockchain research projects. He authored the study "Blockchain in the Energy Sector" for the German Association of Energy and Water Industries (BDEW). Furthermore, he has been an advisory board member of the Energy Web Foundation since 2017 and a member of the "working group energy" for the German Federal Government's Digital Summit in 2018. Jens is a regular keynote speaker at events across the world (Europe, Asia, Africa, and the Americas) with speeches like "The Way to a Real-time Energy Economy" at the 2017 European Commission High-Level Meeting "Interoperability to create the Internet of Energy" and "The Promise of Blockchain to Change the Utility Industries" at the International SAP Conference for Utilities in Lisbon in 2017. His research has appeared in journals such as *European Journal of Informations Systems, Communication of the ACM, Wirtschaftsinformatik (Business & Information Systems Engineering)*.

Clare Sullivan is a cyber lawyer and visiting professor at the Georgetown University Law Center, where she is also Fellow at the Center on National Security and the Law. Professor Sullivan is the author of internationally published articles on digital identity, blockchain technology, privacy, cyber security, and international law; and government reports including the first report on international trade-based money laundering. She is the author of *Digital Identity*, the first international legal study of the legal implications of digital identity. In 2016, Professor Sullivan was appointed consultant to the Commonwealth Secretariat to examine the privacy and data security issues for Commonwealth countries. The following year, he was engaged to develop data protection guidelines for USAID for its international activities. Professor Sullivan has recently completed research for the US Department of Defense on the national security implications of e-Residency. She is currently undertaking a number of projects for the private sector including examining the legal implications of business-to-business sharing of cyberthreat information internationally; a project on the international privacy and data protection implications of the Internet-of-Things (IoT) era, and an associated project on the impact of international data protection regulation on artificial intelligence and deep learning.

Horst Treiblmaier is a Professor in International Management at MODUL University Vienna, Austria. He received a Ph.D. in Management Information Systems in 2001 from the Vienna University of Economics and Business in Austria and worked as a Visiting Professor at Purdue University, University of California, Los Angeles, University of British Columbia, University of Technology in Sydney and the Kazakhstan Institute of Management, Economics and Strategic Research (KIMEP). He has more than 15 years of experience as a researcher and consultant and has worked on projects with Microsoft, Google, and the United Nations Industrial Development Organization. His research interests include the economic and business implications of blockchain, cryptoeconomics, methodological, and epistemological problems of social science research and gamification. Currently he serves on the board of the 'City of Blockchain', an Austrian association promoting the blockchain and cryptographic technologies. His research has appeared in journals such as Information Systems Journal, Structural Equation Modeling, The DATA BASE for Advances in Information Systems, Communications of the Association for Information Systems, Information & Management, Journal of Electronic Commerce Research, Journal of Global Information Management, Schmalenbach Business Review, and Wirtschaftsinformatik (Business & Information Systems Engineering).

Bernhard Waltl has been a researcher at the chair for Software Engineering of Business Information Systems at the Technical University of Munich (TUM) since May 2014. In 2017, he visited Stanford University for a research exchange in which he worked on projects with regard to applied artificial intelligence, explainable artificial intelligence, and smart contracts. He is in the program committee of legal informatics conferences and co-organizes workshops on legal data analytics at international conferences.

Edgar Weippl is the research director of SBA Research and an assistant professor at TU Wien. His research focuses on applied concepts of IT security. He worked in many national and international research projects. He has authored numerous articles that have appeared in many journals and has presented more than 100 papers at peer-reviewed conferences. After graduating with a PhD from TU Wien, Edgar R. Weippl worked in a research startup for two years. He then spent one year teaching as an assistant professor at Beloit College, WI, USA. From 2002 to 2004, while with the software vendor ISIS Papyrus, he worked as a consultant in New York (USA), Albany (USA), and Frankfurt (Germany). In 2004, he joined TU Wien and founded SBA Research together with Prof. Dr. A Min Tjoa and Mag. Markus Klemen. Edgar R. Weippl (CISSP, CISA, CISM, CRISC, CSSLP, CMC) is member of the editorial board of *Computers & Security* and organizes the ARES conference.

Lingchen Zhang is a research associate in Institute of Information Engineering, Chinese Academy of Sciences. He received a PhD in Information Security in 2015 from the University of Chinese Academy of Sciences and worked as research associate at Tennessee State University. He has more than ten years of experience as a researcher and engineer in the area of information security. His research interests include the protocols of key exchange and management, data protection and trusted boot of embedding system, application of blockchain, and IoT security.

Juan Zhao is a postdoctoral fellow in Precision Medicine Center at Vanderbilt University Medical Center. She holds a PhD in Computer Science (2012) from the University Chinese Academy of Sciences and BS (2006) from Shandong University. From 2012 to 2015, she worked as a research assistant fellow, senior engineer and product manager in Chinese Computer Network Information Center, Chinese Academy of Sciences. From 2015 to 2017, she worked in Cyber Security Lab at Tennessee State University as a postdoc fellow. She has much experience in the data and information analysis, and system architectures design. Her research interests lie in machine learning and data mining theories and applications in biomedical informatics, healthcare, and security. Her research focus is to leverage deep learning/machine learning and a huge healthcare data at Vanderbilt University Medical Center to enhance disease prediction. She was also interested in the blockchain in healthcare and IoT.

List of Figures

List of Tables

Part I

Selected Use Cases

1

The Impact of Blockchain on the Tourism Industry: A Theory-Based Research Framework

Horst Treiblmaier and Irem Önder

Introduction

Digitalization is a trend that has heavily impacted the tourism industry. Horwath HTL (2015), the world's largest hospitality consulting brand, points out that technological (r)evolution and digital channels belong to the mega trends in tourism which will influence mid- and long-term tourism development. The World Economic Forum (WEF) (2017, p. 3) states in its report on digital transformation in the aviation, travel, and tourism industry that "there is widespread recognition among industry leaders that the role of digital technology is rapidly shifting, from being a

H. Treiblmaier (✉)
Department of International Management, MODUL University Vienna, Vienna, Austria
e-mail: horst.treiblmaier@modul.ac.at

I. Önder
Department of Tourism and Service Management, MODUL University Vienna, Vienna, Austria
e-mail: irem.onder@modul.ac.at

H. Treiblmaier, R. Beck (eds.), *Business Transformation through Blockchain*,
https://doi.org/10.1007/978-3-319-99058-3_1

driver of marginal efficiency to an enabler of fundamental innovation and disruption". The WEF details recent industry trends, such as a growing demand for travel, the rise of the digital consumer, changes to the security landscape, and technological trends such as the rise of intelligent automation and the dominance of digital platforms. As a side note, the term "blockchain" is mentioned only once in their 40-page report as a potential enabler for the safe and secure exchange of personal data.

The academic tourism community has long acknowledged technology and especially the impact of the Internet as an important and timely research topic. Standing et al. (2014) identified a total of 288 relevant academic publications published between 2001 and 2010 that scrutinize the impact of the Internet in travel and tourism and classified this existing research according to seven main areas: tourism sector studies, e-business, information search, online purchasing, marketing, website analysis, and e-research methods. Interestingly, they conclude that "what can be gleaned from the earlier years of Internet and tourism research is that practitioners and experts alike tend to underestimate the impact of the Internet in the future" (p. 111).

In a recent study, Gelter (2017) provides a comprehensive and current overview of the relevant academic literature inside and outside of the tourism research community. He clusters the various ongoing trends into categories including e-tourism, Internet, smart technology, cloud computing, big data, new digital travelers, gamification, and social networks: a bundle of mega trends which heavily impact on what he calls "digital tourism". Blockchain technology is described as "a revolutionary technology that in the future will transform financial transactions, and strongly influence [the] tourism industry" (p. 74). More specifically, he writes that "Blockchain will create unique opportunities for travel companies to track their customer's preferences, build more personalized and meaningful interactions, and extract more value from loyalty programs" (p. 75).

Hence, it can be concluded from previous studies in combination with ongoing technological developments that the tourism and travel industry is still in a transition period which is characterized by a strong transformation of the role of stakeholders and their respective interaction processes. Blockchain represents the latest development in a long line of technological innovations that bear the potential to significantly shape the tourism and travel industry in the not-too-distant future. To date, there exists a dearth of scholarly literature in tourism-related journals exploring the phenomenon in great detail and helping to lay the theoretical foundation for future studies in this area. In this chapter we will help to close this gap. We argue that through systematic research, academia can help the industry to better understand how to best cope with blockchain technology and how to fully exploit its potential. More specifically, we strive to answer the following research questions:

RQ1: How will blockchain impact existing structures (e.g., networks) and relations in the tourism industry?
RQ2: What resources/capabilities will tourism organizations need to be able to cope with Blockchain-induced changes?

In the following sections, we present the results from qualitative interviews with the managers of several European Destination Management Organizations (DMOs) who outlined their ideas and visions on how blockchain might potentially affect the industry. We apply four widely used theories from social science research to develop frameworks and propositions that can help to guide future tourism and travel research.

Methodology

The goal of this study is to understand and classify the perception of blockchain by tourism industry professionals as well as to develop a theoretically sound research agenda based on these findings. Our focus was on DMOs, which are responsible for the management of the wide variety of elements that make up a destination. Thus, DMOs possess an excellent overview of ongoing tourism-related activities in a specific region as well as their respective implications. They are therefore perfectly suited to comment on the "big picture" of the tourism industry, which includes a multitude of stakeholders with differing interests (Manente and Minghetti 2006). In order to attract visitors to destinations in a highly competitive international market, destinations need to offer good value to their customers. This can be successfully achieved only through collaborative efforts by diverse actors at the destination, from airport infrastructure to hotel developments and the public transport network. Destination management involves coordinated management of attractions, amenities, accessibility, marketing, human resources, and destination-image-related issues. DMOs are responsible for leading and coordinating activities with their partners, for promoting the destination, and for providing strategic leadership for destination development (World Tourism Organization 2007). Three levels of DMOs exist: (1) National Tourism Organizations (NTOs, e.g., Austrian National Tourist Office); (2) regional, provincial, or state DMOs (e.g., Colorado state tourist office); (3) local DMOs for cities or smaller geographic areas (e.g., Paris Tourist Office). DMOs can be publicly funded, private profit-oriented organizations, or a mixture of both.

To the best of our knowledge, this is the first qualitative in-depth study to investigate the phenomenon of blockchain in the tourism and travel industry. Therefore, we decided to conduct an explorative study to uncover potential advantageous and disadvantageous impacts of the blockchain for different stakeholder groups. We conducted interviews with DMO managers from ten major European cities, namely Amsterdam, Berlin, Brussels, Copenhagen, Genoa, Helsinki, London, Tallinn, Valencia, and Vienna, representing ten different countries. These cities are in varying regions with diverse potentials and tourism strategies, and therefore present ideal units to explore the phenomenon under investigation. A purposive sampling approach was used to ensure a heterogeneous and diverse sample (Shadish et al. 2002).

The interviews were semi-structured and were supported by a guideline that was drafted by the researchers based on internal discussions and available literature on blockchain in general as well as its potential implications for tourism. Due to the novelty of the subject, the majority of the literature consisted of consulting studies and industry reports (e.g., Horwath HTL 2015; World Economic Forum 2017).

The recruitment of the participants was done in person during a major tourism conference. Subsequently, a follow-up email was sent with information regarding blockchain technology in general and links to short videos on YouTube explaining the concept in more detail. The email included an invitation to choose a date and time for the interviews. The interviews took place between October 17 and November 29, 2017. All the interviews were conducted in English via Skype and were recorded with the Amolto call recorder. The average duration for each interview was about half an hour. Six interviewees were male and four were female, with age ranging from 27 to 50 years. All interviews were analyzed following the standards of qualitative content analysis and grounded theory (Glaser and Strauss 1967; Hsieh and Shannon 2005). The job titles of the interviewees were quite diverse and included Head of Marketing, Head of Research, and Head of Information Technology. This was in line with the overall purpose of our qualitative and explorative study which was to gather a multitude of diverse and potentially contradictory statements.

Each interview started with general questions regarding the attitudes of individuals toward blockchain and their perceptions of how this technology might potentially affect the tourism industry. Generally speaking, the overall sentiment was that blockchain has a lot of potential, but concrete use cases in the tourism industry are unclear at the moment. One respondent commented that "*At this moment Blockchain is a very good technology for Bitcoin, but there are no other real applications*", while another stated that *"If you have the perfect technology, but you do not have good applications, then you cannot create any value out of this."* There were also several references made regarding the ongoing hype and the intense media coverage which led to the conclusion that "*…Blockchain is not going to change everything."*

Furthermore, the complexity of the technology turned out to be a major obstacle for future applications, as is evidenced by one brief statement: *"I think nobody really understands it."* Finally, one respondent acknowledged the versatility of the technology and highlighted the prevailing uncertainty regarding future implementations: *"Blockchain is a technology, it is a new tool. Everything that can be done with this technology can be done for good or for bad."* Notwithstanding the existing lack of understanding and especially the absence of use cases in the tourism industry, all interview partners were highly interested in its future development and in potential applications that can help to generate business value. There was a general consensus that the tourism industry needs to deal with blockchain and its potential implications: *"Any company can benefit from Blockchain if it is among the first to find a way to do it. This is always the case with new technologies. There are potentials and threats for everyone."*

In the following sections, we focus on the expected implications from a theoretical perspective. Rather than concentrating on specific use cases, which are outlined in the practitioner literature (e.g., Tapscott and Tapscott 2016), we investigate the potential impact of blockchain on tourism from a theoretical angle. In doing so, we apply four commonly used academic theories which help to shed light on future blockchain-influenced relationships between humans as well as on organizational business models in the tourism industry.

Tourism and Blockchain: Four Theoretical Lenses

Tourism is an academic discipline that applies a multitude of theories, most of which were developed and refined in other academic fields, to study predominantly applied problems. The focus of inquiry in tourism has shifted over the years from what Cohen and Cohen (2012, p. 2195) call "earlier discourses of authenticity and the tourist gaze" to theoretical approaches which "reflect a broader meta-theoretical re-orientation in contemporary sociology and philosophy." Similar to other academic communities, the grounding of novel research findings in established theories fosters the advancement of coordinated research activities in the academic tourism community. Some authors favor the application of the so-called "practice theories," which use social practices as the starting point for theorizing and further research (Lamers et al. 2017), while others build on well-established theoretical foundations that have been previously tested in a number of different settings across industries and academic disciplines (Bricker and Donohoe 2015). In the following sections we follow the latter approach and use four complementary theories that are widely popular in the social sciences, namely, agency theory (AT), transaction cost theory (TCT), resource-based view of the firm, and actor network theory (ANT), to investigate social and organizational blockchain-related issues in tourism. Previous research has highlighted the suitability of these theories to study different aspects related to organizational structures and management issues, or, more specifically, the mitigation of agency problems, the coordination of transferred rights of disposals, the reciprocated interaction between institutions, and the coordination of relational assets (Halldórsson et al. 2007). In each section, we first briefly introduce the theory and provide a couple of examples of previous applications to tourism research. We then use the findings from the expert interviews to illustrate how the respective theory can be used to further investigate the implications of blockchain on the tourism industry.

Agency Theory

Agency costs are the sum of monitoring expenses by the principal, bonding expenditures by the agent, and residual loss (Jensen and Meckling 1976). They are caused by the principal's desire to control, monitor, and supervise the agent, so that the latter performs the tasks in the best interest of the former. AT has previously been used to explain conflicts of interest and strategies for solving incentive problems (Eisenhardt 1989). In tourism research, AT has previously been used, for example, to explain the owner/manager relationship in tourism-based condominiums (Guilding et al. 2005), as well as to better understand the contractual relationships between hotel operating companies and hotel owning companies (Rodríguez 2002).

Following the basic tenets of AT, we categorized and clustered the experts' statements according to the presumed impact of blockchain on communication flows and relationships between principals (e.g., travelers) and agents (e.g., booking agencies). Table 1.1 shows the respective categories that emerged from the interviews on the left and several sample statements on the right. In order to allow for efficient and effective communication flows, it is crucial to specify the exact *role* of each market participant and their respective rights and duties, since this subsequently determines the allocation of tasks as well as the flow of information. Blockchain has the potential not only to alter communication flows, but also to change the responsibilities associated with specific roles. Some roles might even become redundant. However, it might as well be the case that existing *relationships* render blockchain unnecessary, especially

Table 1.1 Categories for agency theory and blockchain

Category	Sample statements
Roles	*If you think about online travel agencies (OTA), it's very unclear what the role of each player is. We have limited information about the bookings from OTAs and almost no information from conventional tour operators. Not enough data are being shared* *Blockchain will […] change our roles and activities. We have to adapt*
Relationships	*The possibilities to have direct relationships increases […] because they can trust you and they can work directly with you without other intermediaries* *… because of the existing relationships in the tourism industry I don't see the big impact or big influence of blockchain*
Trust	*It's relatively open what people will charge for anything. We are open. As long as organizations are honest, transparency is not an issue* *[…] whatever helps us to get more data […] creates transparency for us as an organization. This in turn fosters trust*
Transparency	*You can create a blockchain for a specific group. It's up to you. If you want to make it transparent you can. If you want to hide information that is also possible* *We have a global connected project that attracts airlines and they usually rely on really fast information and sometimes they are in other parts of the world and signing the contracts can take a couple of days. In that project blockchain will make sense as well. And transparency across borders will help to make contracts run faster* *It could be possible to bring different stakeholders together. For example, by using smart contracts and having transparent financial relationships* *[…] if you book a hotel you can easily see which part of the money goes where […] you have more transparency, you say OK this is what the hotel is getting, this is what intermediaries are getting and so on*
Disintermediation	*[…] if it really works people will not need a third-party provider* *Bookings between different stakeholders can be made easier* *We have the […] card, we have […] partners there, they just use two weeks of negotiating new contracts and sending them back and forth and blockchain will save them a lot of time*

in those cases where *trust* contributes to the functioning of stable business relationships. On the other hand, blockchain can also generate trust by increasing *transparency*. In turn this will allow for faster transaction processing and connecting business partners across regions. *Disintermediation*, namely the substitution of middlemen, is expected to have a huge impact on existing business relationships. By removing various layers from the value network, bookings can be made easier and faster.

Transaction Cost Theory

TCT deals with the impact of transaction and production costs on different types of governance structures. The design of efficient inter-organizational and intra-organizational structures determines the size of an organization and its interchange with relevant markets (Coase 1937). Transactions costs include ex ante costs of initiation (e.g., search and information costs), agreement (e.g., costs of negotiations and reaching an agreement), and ex-post costs of adjustment and control (Picot et al. 1997). Strebinger and Treiblmaier (2006) have shown that TCT can be used to better understand structural and procedural organizational changes caused by the introduction of E-Commerce. Similarly, blockchain has the potential to significantly disrupt existing market and organizational structures. TCT has been applied as a theoretical lens in recent tourism research to better understand the emergence of the sharing economy, as is evidenced by platforms such as Airbnb (Akbar and Tracogna 2018). The authors compared different forms of governance mechanisms (i.e., pure markets, hierarchies, sharing platforms) and developed various propositions pertaining to the propensity of platform owners to adopt mechanisms of platform integration. Transaction costs have also been applied as the underpinning framework to explore the role of trust and formal contracts in dyadic and network cooperation among tourism entrepreneurs (Czernek et al. 2017).

Table 1.2 lists the respective categories that emerged from the interviews. Blockchain may change existing *market structures*, although it is currently unclear in which direction. It is seen as a tool which allows for direct connection with final customers, but it may also lead to centralized

Table 1.2 Categories for transaction cost theory and blockchain

Category	Sample statements
Market structures	*It will benefit small companies and service providers more, since they can easily connect with the final customer* *DMOs are like the middle in a lot of cases, so I think it can be good for people to have a centralized system that people can refer to* *If there is no major innovation, which redefines the whole market, just those big players (*e.g., *online travel agencies) will get stronger and stronger*
Communication structures	*[Maybe] with blockchain there will be faster information exchange, faster communication between devices*
Cost reduction	*There will be a reduction in transaction costs. That could also be beneficial for a public institution to show how they are going to save money* *So if you have someone who is alone in the market, then he has the chance to raise the price as he wants, which is the risk of a central infrastructure system. In this case blockchain could be an opportunity to bring these costs down*
Cost increase	*If you are using the blockchain infrastructure to secure every transaction, you need this capacity for each participant, which makes it much more expensive* *We also need to consider new legal requirements pertaining to, for example, "anti money laundering" and "know your customer" regulations*
Transparency	*If the blockchain combines all tourism data, including tour organizations and bus companies, the data is available for planning purposes, which allows for greater transparency*
(Dis) intermediation	*The transportation system would definitely benefit from identification tokens, because it is complicated to buy tickets if you are not from XXX* *A lot of transactions will take place directly between consumers and suppliers without any intermediaries* *I think there will probably still be room for some intermediaries that provide additional services both to the supplier and to the client*

information systems, which provides an advantage for companies that already dominate the market. Consequently, *communication structures* may change. Direct and computer-mediated information in combination with accessibility and immutability of information can lead to an increase in communication speed. As far as the *costs* are concerned, the impact of blockchain is unclear. Some respondents expect a *reduction* of costs, which may be caused, for example, by more efficient market structures, while others fear an *increase* in costs due to the recording of each and every transaction in combination with legal requirements. Increased *transparency* was mentioned as a major driver for future developments. Similar to the expected impact of blockchain on costs, the interviewees disagreed as to what extent the technology might lead to *intermediation* or *disintermediation*. Some suspected that existing market leaders might grow even bigger, while others reason that the technology will allow customers to directly connect with service providers. Alternatively, new intermediaries might emerge that understand the technology and develop innovative business models.

Resource- and Capability-Based Views

The resource-based view (RBV) is a theory (alternatively: managerial framework) that focuses on an organization's internal resources as a means of excelling in the market. According to RBV, it is only a subset of an organization's resources which helps to create competitive advantage and an even smaller subset that accounts for long-term superior performance. In order to sustain competitive advantage, companies need to possess and protect scare resources. Those resources comprise all tangible and intangible assets that a firm uses for choosing and implementing its strategies (Wernerfelt 1984; Barney 1991). Makadok (2001) synthesizes resource-based and dynamic-capability views, and differentiates between two distinct mechanisms, namely resource-picking and capacity-building, both of which companies can use to create economic rents. He defines 'capability' "as a special type of resource—specifically, an organizationally embedded nontransferable firm-specific resource whose purpose is to improve the productivity of the other resources possessed by the firm" (p. 389). Tourism research has applied RBV, for instance, to better understand sustainable competitive advantage among tourism organizations (Evans 2016). Another example comes from Denicolai et al. (2010) who explore the relationship between the networking approach of tourism

Table 1.3 Categories for resource- and capability-based views and blockchain

Category	Sample statements
Resources	*This could be amazing for transportation. Can you imagine a public transportation system that can use this sort of technology? It's incredible* *You can get rid of all the loyalty cards once travelers are connected to the identification tokens*
Processes and management	*All the processes from accounting to business intelligence […] could potentially be professionalized* *All kinds of supply chains can be managed better. This is a very interesting use case* *I think there will be more and more demand for data analysts. People who can actually make use of this information, all of this data which is made available as a result of blockchain* *Blockchain is also just a database which needs human knowledge and expertise to be integrated into certain domains*
Competitive advantage	*A worldwide operating tourism company has much more opportunities to use blockchain technology* *Probably this development will widen the gap between organizations who are able to mine this data and turn it into extra money and those organizations who will not have the knowledge or the competencies to do that*

firms and the development of tourism core-competences. More specifically, they use a resource-based approach to investigate the determinants of tourism core-competence development.

Table 1.3 lists the relevant statements from the survey participants that are related to various resources or capabilities. Obviously, blockchain itself constitutes a *resource*, but it is mainly the resulting applications on top of this platform that can lead to superior performance and subsequently competitive advantage. One example for such an application involves measures that make the transportation system more efficient. As far as *processes and management* are concerned, the interviewees came up with several examples, ranging from the implementation of new accounting and business intelligence procedures to the complete restructuring of supply chains. Especially the field of data analysis was of special interest for several respondents. They also highlighted the fact that human capital will still be needed to actually capitalize on the potentials of blockchain.

In order to gain *competitive advantage*, however, several conditions need to be favorable for the companies. This includes, for example, an appropriate organizational scale which determines the amount of capital available to invest in new technologies and the benefit gained from doing so. Blockchain thus poses a potential risk for companies that lack the financial means and knowledge to participate in this development.

Actor Network Theory

ANT explores different roles within a network. The focus of ANT is on networks of relationships which constitute the main building blocks of society. Actors can not only be persons, but also objects (including technological artifacts such as blockchain) and organizations. Existing network structures can be severely disrupted when individual parts of the network change (Latour 2005). Within tourism research ANT has been applied in a number of different settings, such as the creation of so-called tourismscapes, which simultaneously integrate people, objects, technologies, and spaces that can subsequently be ordered and scrutinized (van der Duim 2007). Jørgensen (2017) has shown how ANT can be used to create a framework to analyze tourism distribution by focusing on the link between producers of tourism services and their consumers. Paget et al. (2010) applied ANT to better understand the impact of innovations in a French ski resort. They found that new associations arose between actors and non-human entities, and showed how existing resources can be used to develop new and innovative products. Van der Duim et al. (2013) even argue that ANT "enables a radical new way of describing tourism by critically investigating its ontological conditions" (p. 3).

Table 1.4 shows the respective categories that emerged from the analysis of the interview data with a focus on ANT. First, we discovered several *determinants of relationships*, which include the necessity for companies to maintain good relationships with their customers (both B2C and B2B), and therefore a high importance of reputation. Furthermore, the *service component* of relationships may be affected. Several participants actually highlighted the potential of blockchain to improve customer service by,

Table 1.4 Categories for actor network theory and blockchain

Category	Sample statements
Relationship determinants	*Many organizations focus on their reputation* *We strive to maintain good relationships with our customers. Blockchain may help us with that*
Service components	*When you are paying for the accommodation, you can be sure that the accommodation will be reserved* *The big advantage is of course transparency, but I think there is also the need of somebody steering this. Because of transparency there is a risk that there are too many opportunities and it is unclear which of those could be used right now* *We can offer additional services to our customers with blockchain*
Network structures	*I am always thinking from the travelers' point of view. Because when you buy packages, there are a lot of middlemen in between. And you could probably cut them out, if there exists transparency between organizations and what they offer* *All the bookings that you do are based on trust. All the booking processes will be affected by this* *I think people are concerned that they make a transaction with a company that they are not familiar with. This could potentially become less of an issue with blockchain technology* *Who will control the blockchain network?*

for example, guaranteeing reservations, increasing transparency and offering additional services. However, it was also mentioned that someone (i.e., a human being) needs to manage the transition process and decide on how to capitalize on the benefits of blockchain. The core element of ANT is the network and the relationships between the actors within. Any changes in the *network's structure* can potentially disrupt its functioning. This especially pertains to the removal of middlemen (i.e., disintermediation) and the opportunities for customers to easily establish business relationships with hitherto unknown companies. Blockchain guarantees the execution of contracts and will likely lead to increased trust that is based on the availability and immutability of information. Network structures will be fundamentally altered and one participant raised the question of who will be in control. Given that blockchain is a peer-to-peer network without any built-in control structures, the overall structure of the existing network can significantly change, which will in turn also influence all kinds of business relationships.

Conclusion and Implications

In this paper we propose a multi-theoretical approach to better understand the potential implications of blockchain for the tourism industry and to lay the foundation for further research in this area. As a starting point we used two research questions pertaining (1) to the impact of blockchain on existing structures and relations in the tourism industry and (2) the resources and capabilities companies need to be able to cope with Blockchain-induced changes. We used four theoretical approaches to analyze data from 10 qualitative interviews with DMO managers and to create categories that convey the essence of our findings.

We started with a framework suggested by Halldórsson et al. (2007) for supply chain management that includes four frequently used theories from economics and the social sciences. The four theories help to detect important issues when it comes to the presumed impact of blockchain. While several important overlaps may exist, AT and TCT in general deal with structural issues related to the tourism industry, whereas RBV and ANT provide important insights regarding management issues. AT focuses especially on roles and relationships between humans. By increasing the transparency of transactions, blockchain has the potential to fundamentally alter existing business relations. The level of trust needed to form business relationships may decrease and structural changes such as disintermediation might occur as a result. TCT takes a broader perspective by investigating market and communication structures and allowing for the assessment of optimal organizational size. It is primarily the anticipated changes in transaction costs caused by blockchain, which will have a substantial impact on organizational structures. As forecast by the DMOs, blockchain will simultaneously yield cost reductions in some areas and increases in others, which, according to TCT, will lead to the adaption of organizational and market structures. From an RBV perspective, blockchain constitutes a new resource if applied appropriately. It will also impact inter- and intra-organizational processes and management structures that will ultimately affect an organization's level of competitive advantage. This is especially important in an industry that is as interconnected as the tourism industry. Finally, ANT helps to illuminate how blockchain will impact relations between various actors in the tourism network. The overall importance of existing relationships might decline due to the potential of blockchain to ensure trust and transparency. However, research is needed to discover the extent to which blockchain can actually fulfill such promises and how different actors in the system will benefit from them. Taken together, all four theoretical approaches help to shed light on different aspects of blockchain's implications for the tourism industry. This might lead to simultaneous structural and procedural changes on an organizational and/or market level, and to strategic changes on an organizational and/or regional level (cf., Treiblmaier and Strebinger 2008; Strebinger and Treiblmaier 2004). DMOs are responsible for promoting specific geographical areas and need to take into account the potential systemic impact of blockchain not only for individual companies, but rather for an intricate network of actors interacting with each other in various roles.

We believe that academia and industry are closely connected in this emerging research field and that by asking the right questions and applying the appropriate methodology, academia can make a major contribution to support the industry in making sound managerial decisions. One major finding from our interviews was that the current level of knowledge about blockchain and its potential implications for the tourism industry is low and many respondents stated that they would appreciate more information and support in that matter. Given the fast progress in this field and the existing uncertainties caused by ongoing media hype, we believe that it is the responsibility of academic research to take an impartial and objective stance. We therefore suggest that future research builds upon our framework and extends it further by closely investigating current Blockchain-related developments and their impact on the tourism industry. By integrating new findings into our model, researchers can help to create a comprehensive theory-based framework that comprehensively describes, explains, and predicts the impact of blockchain on the tourism industry.

References

Akbar, Y. H., & Tracogna, A. (2018). The Sharing Economy and the Future of the Hotel Industry: Transaction Cost Theory and Platform Economics. *International Journal of Hospitality Management, 71*, 91–101.

Barney, J. B. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management, 17*(1), 99–120.

Bricker, K., & Donohoe, H. (2015). *Demystifying Theories in Tourism Research*. Oxfordshire: CABI.

Coase, R. H. (1937). The Nature of the Firm. *Economica, 16*(4), 386–405.

Cohen, E., & Cohen, S. A. (2012). Current Sociological Theories and Issues in Tourism. *Annals of Tourism Research, 39*(4), 2177–2202.

Czernek, K., Czakon, W., & Marszałek, P. (2017). Trust and Formal Contracts: Complements or Substitutes? A Study of Tourism Collaboration in Poland. *Journal of Destination Marketing & Management, 6*(4), 318–326.

Denicolai, S., Cioccarelli, G., & Zucchella, A. (2010). Resource-Based Local Development and Networked Core-Competencies for Tourism Excellence. *Tourism Management, 31*(2), 260–266.

Eisenhardt, K. M. (1989). Agency Theory: An Assessment and Review. *Academy of Management Review, 14*(1), 57–74.

Evans, N. G. (2016). Sustainable Competitive Advantage in Tourism Organizations: A Strategic Model Applying Service Dominant Logic and Tourism's Defining Characteristics. *Tourism Management Perspectives, 18*, 14–25.

Gelter, H. (2017). *Digital Tourism – An Analysis of Digital Trends in Tourism and Customer Digital Mobile Behavior, Report*. resources.mynewsdesk.com/image/upload/t_attachment/ecdf34yro7o8jjvwm8ji.pdf. Accessed 22 Feb 2018.

Glaser, B., & Strauss, A. L. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago: Aldine Publishing Company.

Guilding, C., Warnken, J., Ardill, A., & Fredline, L. (2005). An Agency Theory Perspective on the Owner/Manager Relationship in Tourism-Based Condominiums. *Tourism Management, 26*(3), 409–420.

Halldórsson, A., Kotzab, H., Mikkola, J. H., & Skjøtt-Larsen, T. (2007). Complementary Theories to Supply Chain Management. *Supply Chain Management: An International Journal, 12*(4), 284–296.

Horwath HTL. (2015). *Tourism Megatrends: 10 Things You Need to Know About the Future of Tourism, Report*. horwathhtl.com/files/2015/12/Tourism-Mega-Trends2.pdf. Accessed 22 Feb 2018.

Hsieh, H.-F., & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research, 15*(9), 1277–1288.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. *Journal of Financial Economics, 3*(4), 305–360.

Jørgensen, M. T. (2017). Reframing Tourism Distribution – Activity Theory and Actor-Network Theory. *Tourism Management, 62*, 312–321.

Lamers, M., van der Duim, R., & Spaargaren, G. (2017). The Relevance of Practice Theories for Tourism Research. *Annals of Tourism Research, 62*, 54–63.

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford University Press.

Makadok, R. (2001). Toward a Synthesis of the Resource-Based View and Dynamic-Capability Views of Rent Creation. *Strategic Management Journal, 22*(5), 387–401.

Manente, M., & Minghetti, V. (2006). Destination Management Organizations and Actors. In D. Buhalis & C. Costa (Eds.), *Tourism Business Frontiers: Consumers, Products and Industry*. Oxford: Elsevier Butterworth Heinemann, (pp. 228–237).

Paget, E., Dimanche, F., & Mounet, J.-P. (2010). A Tourism Innovation Case: An Actor-Network Approach. *Annals of Tourism Research, 37*(3), 828–847.

Picot, A., Bortenlanger, C., & Rohrl, H. (1997). Organization of Electronic Markets: Contributions from New Institutional Economics. *Information Society, 13*, 107–123.

Rodríguez, A. R. (2002). Determining Factors in Entry Choice for International Expansion. The Case of the Spanish Hotel Industry. *Tourism Management, 23*(6), 597–607.

Shadish, W. R., Cook, T. D., & Campbell, D. T. (2002). *Experimental and Quasi-Experimental Designs*. Boston: Houghton Mifflin.

Standing, C., Tang-Taye, J.-P., & Boyer, M. (2014). The Impact of the Internet in Travel and Tourism: A Research Review 2001–2010. *Journal of Travel & Tourism Marketing, 31*(1), 82–113.

Strebinger, A., & Treiblmaier, H. (2004). E-Adequate Branding: Building Offline and Online Brand Structure Within a Polygon of Interdependent Forces. *Electronic Markets, 14*(2), 153–164.

Strebinger, A., & Treiblmaier, H. (2006). The Impact of Business to Consumer E-Commerce on Organizational Structure, Brand Architecture, IT Structure and their Interrelations. *Schmalenbach Business Review, 58*(1), 81–113.

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York: Penguin.

Treiblmaier, H., & Strebinger, A. (2008). The Effect of E-Commerce on the Integration of IT Structure and Brand Architecture. *Information Systems Journal, 18*(5), 479–498.

Van der Duim, R. (2007). Tourismscapes: An Actor-Network Perspective. *Annals of Tourism Research, 34*(4), 961–976.

Van der Duim, R., Ren, C., & Jóhannesson, G. T. (2013). Ordering, Materiality, and Multiplicity: Enacting Actor-Network Theory in Tourism. *Tourist Studies, 13*(1), 3–20.

Wernerfelt, B. (1984). A Resource-Based View of the Firm. *Strategic Management Journal, 5*(2), 171–180.

World Economic Forum. (2017). *Digital Transformation Initiative: Aviation, Travel and Tourism Industry*. White Paper, Geneva.

World Tourism Organization. (2007). *A Practical Guide to Tourism Destination Management*. Madrid: UNWTO.

2

Blockchain in the Energy Sector

Jens Strüker, Simon Albrecht, and Stefan Reichert

The digitization of the energy industry continues to pick up speed. A new driver of this rapid development is currently the blockchain technology, which could, according to many experts, usher in the next stage of development of the Internet. Blockchains have the potential to optimize energy management processes in almost all stages of the value chain while coping with the rising complexity of the increasingly decentralized energy system.

For the integration of a large number of prosumers into the energy system, the underlying IT architecture will have to ensure an efficient and secure distribution of data. In this respect, the blockchain technology has

J. Strüker
Fresenius University of Applied Sciences, Idstein, Germany

S. Albrecht
University of Freiburg, Freiburg im Breisgau, Germany

S. Reichert (✉)
BearingPoint, Frankfurt, Germany
e-mail: stefan.reichert@bearingpoint.com

H. Treiblmaier, R. Beck (eds.), *Business Transformation through Blockchain*,
https://doi.org/10.1007/978-3-319-99058-3_2

made headlines in tech, and finance press, being mostly known for a utilization as decentralized databases in financial deployments, most famously Bitcoin. After the technology made its first appearance in Nakamoto (2008), diverse authors have centered articles around blockchain-related issues. Among those, most focus on the technological architecture and its characteristics (e.g. Decker and Wattenhofer 2013; Pilkington 2016), anonymity and privacy (e.g. Zyskind et al. 2015), or the applications in finance (e.g. Fanning and Centers 2016). Today, the fundamental necessity of information systems (Wissner 2011; Colak et al. 2016) as well as accompanied potentials and value increasing applications (Gungor et al. 2013) have finally raised awareness in the energy sector (e.g. Albrecht et al. 2018). A study from the Federal Association of the German Energy and Water Industries (BDEW) analyzes the potential of energy-related applications and corresponding challenges (BDEW 2017).

Digitalization and decentralization are putting households and companies in the focus of the energy system, as they increasingly participate actively in market affairs through small-scale interactions. However, not only users and consumers may benefit from the blockchain technology. From an economic point of view, the possibility of increasing network utilization and efficiently organizing the allocation of flexibilities of any size seems particularly interesting. The ability of a blockchain to make even the smallest transactions cost-effective ultimately means new degrees of freedom, for example for the provision of control energy, direct electricity trading between market players or so-called "shared investments". In combination with the digitization of metering processes, blockchain technology supports new forms of product differentiation, including generation type, location, and time. Correspondingly, there are already a significant number of specific pilot projects in all value-added stages of the energy industry. Examples are the charging infrastructure for e-mobility, the certification of green and regional electricity, neighborhood and tenant electricity concepts, the provision of control energy and wholesale electricity. These are analyzed in course of the chapter.

The Transition of the Energy Sector and the Upcoming Market Challenges

The emergence of renewable, distributed energy resources (DERs) and smart grids is expected to create a network, in which billions of devices could automatically communicate with each other. The increasing share of these energy resources might establish a zero marginal cost market in which single units of generated power will have no significant costs anymore (Schlemmermeier and Drechsler 2015). Concurrently, competition impacts on wholesale prices and margin rates. Utilities are pressured to adjust to the change. The energy market is facing changes induced by technological and socioeconomic developments. The following trends can be observed (Edelmann 2014):

- The **energy generation** transitions from conventional thermal power plants to DERs, often renewables (Fig. 2.1). This induces fluctuating supply, increasing uncertainty, and a demand for information services;
- **Energy trade** becomes more complex. Local markets are being established, opportunities emerge, streamlining the digital infrastructure gains in relevance;

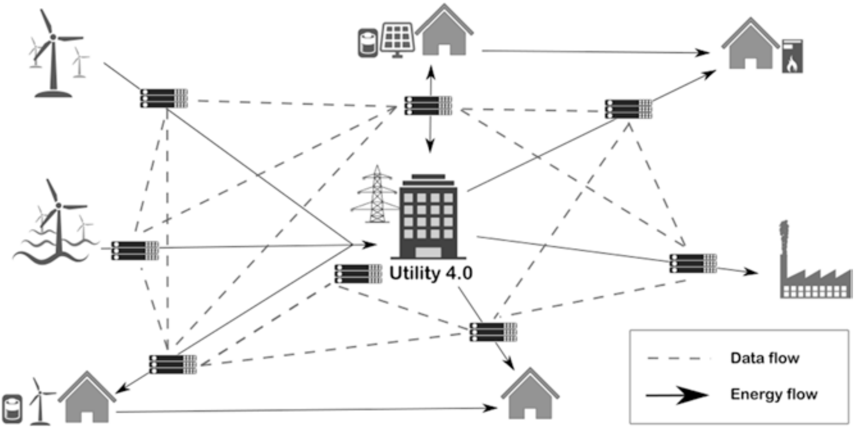


Fig. 2.1 Future energy market

- The **energy distribution**, now utilizing bidirectional flows of energy and data, is getting more dynamic (weather reliant plants, storage);
- The **metering infrastructure** is getting digitized. The smart meter rollout (in Germany beginning in 2017 [EnWG 2011]) is starting to replace analogous meters with smart meter gateway (SMGW) tethered devices;
- **Customer relations** are being confronted with a new kind of emancipated customer, who is less reliant on the utility and who takes social and environmental issues into consideration.

According to Dalkmann (2014), stated trends can be classified in three major socioeconomic phenomena: (1) *Volatility*: The heterogeneous generation is causing high fluctuations. Accordingly, supply and price are subject to high levels of uncertainty. (2) *Locality*: DER such as power-heat coupling plants, photovoltaic installations, and biogas plants are becoming more popular for residents and local organizers. An increasing share of energy demand can be provided locally, making the grid-balancing a challenging task. (3) *Participation*: The traditional role of a utility is to locally provide a commodity to passive customers. The changes of the energy market have an empowering potential for customers, enabling them to optimize domestic consumption and to switch retailers. The establishment of local community projects to increase the share of local and green power is one instance. In Germany, households, small businesses, and local governments invest in more than 800 of these projects (Ott and Wieg 2014). This may encourage utilities to actively pursue the development of more differentiated products to saturate these emerging segments of demand.

In Kolks et al. (2012), the authors identified competition as a major challenge for local utility companies. In the last few years, multiple German cities started to either remunicipalize formerly privatized utilities or establish new ones. Consequently, local and national competition increases while customers are able to choose the utility providing the most suiting retail products. The diversification of energy demand is another challenge for utilities. Customers may demand more options for the individualization of their consumption, controllable, and autarky-fostering solutions, representing an emancipated relationship to the company. Utilities ought to develop products that enable risk-seeking customers to optimize their individual costs while providing risk minimization for risk-adverse customers.

Along with the transitioning environment, the business needs of utilities change as well. Due to the decrease in volume and profitability of the conventional business areas, companies ought to discover or create new value streams to foster growth. This includes the reconceptualization of customer relation strategies. Utilities can generally be classified as risk-averse. Innovation on information and communications technology gets easily disregarded. Most do not operate an internal research and development (R&D) department, spending less than 1% of net sales on R&D (European Commission 2013; Daim et al. 2013). This innovational inertia creates opportunity for market-external agents, aiming to secure their share of novel business areas. According to Edelmann (2014), the following business areas qualify for market penetration by external agents (Table 2.1).

Accordingly, in the studies by Edelmann (2014) and Schlemmermeier and Drechsler (2015), the authors identify critical issues to be in the focus for changing energy business models. The "winners of the coming smart market" will have to satisfy a number of conditions. They need a clear vision for a strategic positioning in the market, as well as for a product portfolio and a targeted market share. They need to build up internal

Table 2.1 Exogenous sources of competition in transitioning energy markets (based on Edelmann 2014)

Area	Task	Competitors from…
Smart home services	Home Automation, Energy management	Entertainment industry, Automotive
Customer relations	Billing, visualization	Telco, Retail, Technology
Metering	SMGW-Administration, Remote meter reading	Technology
Data management	Data mining, Analytics, Load profile segmentation	Business analytics
Grid and distribution	Grid monitoring, Microgrid operations	Industry
Energy generation	DER, Renewables, Storage	Technology, Automotive

proficiency as well as business cooperations with intermediaries and service providers. Furthermore, innovation capabilities and technological excellence will play a crucial role, in combination with a strong corporate identity and customer focus. These developments and contemporary challenges of the energy sector display a necessity for technological innovation to transform utilities' business processes.

The generation of electricity is increasingly determined by decentralization, digitization, and decarbonization. As a result, it is becoming more and more fragmented, the number of prosumers, that is consumers who are also producers, is steadily increasing and DERs, such as PV rooftop installations, batteries, and electric vehicles, will continue their growth in the coming years. In addition to loads of all kinds in households and businesses, they are increasingly being controlled via the Internet. The shift in the value chain to a bidirectional relationship between energy production and consumers is gradually progressing. At the same time, the economic pressure is steadily increasing to make distributed resources usable for both the grid and the market. In the next chapter, we will outline how blockchain technology promises to reshape the interaction between different market actors.

The Promises of Blockchain in the Energy Sector

The blockchain technology promises to be able to organize and track very small energy flows and control signals at the lowest transaction costs. It fits seamlessly into strategies that put the customer at the center. Overall, processes and business models are increasingly determined by the changing needs of customers. As a result, direct investments in generating plants, the purchase of small quantities, as well as their processing, billing and flexible delivery make the overall energy system much more complex overall. Blockchain technology promises to contribute to managing this emerging complexity through controlled data usage (data sovereignty) and direct interaction between actors (disintermediation). Possible applications of blockchain technology in the energy sector are discussed intensively. In 2016, a study by the German energy agency (dena) analyzed some applications about their potential. Significant potential was identified, above all, in direct transactions between customers, including financial settlement, as well as in the areas of clearing and settlement and certifications of origin. A study by the BDEW, published in 2017, further analyzes specific use-cases as well as the main determining success factors. The reduced need for intermediation (disintermediation) can simplify many processes, such as the change of providers or even the organization of ancillary services, and possibly organize them more cheaply. Equally feasible is the automated transfer of duties, levies, charges, or compensation through a blockchain. Complex documentation processes can be eliminated or reduced for all actors involved. It should be noted here that the boundary between the optimization of existing processes and the redesign of processes is fluid.

In addition to distributed generation, the number of loads of all kinds rapidly increases that are controlled via the Internet (production machines, lighting, ventilation, vehicles, heaters, etc.). Irrespective of the question of suitable market design, the integration of these IoT resources into the electricity system as active market participants is urgently required from an economic perspective: unused capacities and (long term) storages represent opportunity costs. The direct interaction of devices promises to improve the utilization of networks and the allocation of flexibilities significantly. In such a real-time energy industry, millions of devices are fine-tuning their behavior based on market and network signals. For a realization, however, it is necessary to carry out each of these microtransactions safely and efficiently and to make them comprehensible. Blockchain technology promises here to be a major contributing factor. New degrees of freedom may also arise for the design of the balancing group management, if a real-time management is possible. If small-scale infeed and outfeed of electricity becomes cost-effective, then product differentiation by type, location, and time becomes possible (e.g. the detection of local green wind power). Due to increasing self-sufficiency, neighborhood electricity and the usage of electric cars, the typical 4000 kWh household will no longer be the standard in the future. A resulting increase in the number of prosumers and the ongoing electrification of the heating and transport sector are expected to generate considerable pressure for local supply and demand to be networked. This also applies to the aforementioned expansion of Internet-enabled consumption and generation facilities. The discussions about neighborhood and tenant electricity models are an indicator for the evolution of decentralized market scenarios. Ultimately, the speed of these developments will significantly affect the opportunities for blockchain technology.

Categorization of Blockchain Types

Public (Permissionless) Blockchains

The most popular blockchains, such as Ethereum or Bitcoin, are permissionless and public. In principle, they are accessible for everyone, given the appropriate infrastructure (Table 2.2). Participants are usually anonymous to other participants and represented only by a random ID as personal address. In first instance, there is no central provider to supervise the ongoing traffic. Public blockchains typically rely on the so-called Proof-of-Work (PoW) consensus mechanism for validating new data blocks. For this, miners compete against each other to solve a computa-

Table 2.2 Criteria for public, private, and consortium blockchains (based on BDEW 2017)

	Public	Private	Consortium
Access	Permissionless	Permissioned	Shared permissioned
Personal Information	Pseudonymity	Known	Known
Device Authentication	Not required	Required	Conditional
Consenus Mechanism	PoW, PoS	PoA, PBFT	PoW, PoS, PoA
Security	Decentralized control	Single point of failure	Various
Transaction Speed	Low (PoW)	High	Higher than public
Energy Consumption	High (PoW)	Low	Rather low
System Costs	High	Presumably low	Medium to low
Individual Costs	Low	Rather high	Various

tional puzzle, where the winner gets to update the database and typically receives a reward in the specific digital currency (Swan 2015). Then the process starts again from the beginning for each new block. The correctness of the solved puzzle and the integrity of the whole blockchain is verified by all participating servers. This advanced consensus mechanism makes trust between individual actors obsolete, as the majority of all participants supervises the entire history of transactions. The reliability of a public blockchain heavily depends on a sufficiently high number of participants as miners, who provide the needed computational power and storage capacities. In various initiatives, tremendous effort goes into working on alternatives to the PoW with less resource consumption, such as the Proof-of-Stake (PoS) (Buterin 2014). If these efforts are successful, public blockchains have two major advantages over private or consortial blockchains: Firstly, it allows the participation of random devices (machines, mobile phones, tablets, etc.) that are unknown to each other and not needed to be trustworthy. Secondly, there is no necessity that a consortium or private provider has to admit new blockchain-based applications. In a future IoT scenario, with random devices communicating on a near real-time basis, these two characteristics may prove fundamentally important.

Private (Permissioned) Blockchains

For permissioned and private blockchains, access is only granted to known participants, who might have rights to read and/or write data. The provider has full control over the blockchain and he knows all participants a priori. Thus, in most cases, private blockchains do lack the properties of anonymity and irreversibility. The provider generally has the possibility to set back certain processes in the blockchain, even though specific designs may vary. The abandonment of the PoW consensus mechanism and the irreversibility of the blockchain could greatly increase the processing speed and scalability. The validation of single blocks is thereby possible at much lower consumption of resources, as not all participants are simultaneously working on the solution of the algorithmic puzzle. An alternative to the PoW consensus mechanism for private blockchains is the Proof-of-

Authority (PoA), where only a single node generates new data blocks. With private blockchains, it is possible to develop and deploy new applications rapidly. The most promising fields of application may be internal business processes, targeted toward a high throughput of data. It is possible to cut off and archive the blockchain at frequent intervals, for example yearly, which can reduce the size of the storage volume significantly. Private blockchains do not necessarily need an underlying digital currency, as no financial incentives need to be set for miners.

Consortium Blockchains

Consortium blockchains (or special-purpose blockchains) as semiprivate blockchains (shared permissioned blockchains) are oftentimes regarded as a compromise between public and private blockchains. Here only verified participants are allowed to validate blocks. Optimized consensus algorithms permit significantly faster transactions than public blockchains. They do not necessarily need an underlying digital currency, although tokens can be useful for setting incentives. Generally, consortium blockchains offer the possibility to be tailored toward the specific requirements of the energy market, for example by giving up the property of anonymity or by an increase of the transaction volume depending on the application. Currently, the Web Energy Foundation plans to establish and operate a consortium blockchain, specifically designed for the energy sector (Rocky Mountain Institute 2017). In this respect, the question of interoperability between different types of blockchains (public, private, and consortium) and industries is regarded as one of the key success factors of the blockchain technology (Underwood 2016).

What Are the Most Promising Areas for Blockchain Applications in the Energy Sector?

At present, a large number of energy providers and startups are working on the testing of blockchain solutions such as Ethereum, Hyperledger, BigChain, or Tendermint. In the foreground is usually the optimization of energy management processes such as billing, management of data, or processes for the change of electricity suppliers. The classic value chain of the energy industry is becoming increasingly interconnected and new applications can no longer be assigned exclusively to one area. In the following, some selected application fields are shown and the impact on the classical value chain is outlined.

Charging Infrastructure for E-mobility

The use of electromobility requires an area-wide charging station infrastructure. A very decentralized distribution and a large number of different operators make today's billing procedures very complicated. For example, the process of recognizing the user upon authorization at a charging station may currently be delayed due to a multitude of requests at different instances. Through the use of a blockchain method for detecting the vehicles and for communication as well as billing of the amount of electricity purchased, the processing speed can be significantly increased. The consumer at a public reference point could be immediately recognized and settled. This leads to a comfort gain for the customer, cost reduction for the provider, as well as detailed billing of the actual electricity purchased. In addition, the customer remains in control of his mobility data at all times. A current project for this is, for example, Share & Charge of Innogy and slock.it, in which the billing of the electricity purchased for electric cars is tracked and billed based on blockchains. Participants will also be able to make their private charging stations available to other electric motorists. Payment and billing is done automatically via blockchain-based smart contracts.

Certification of Energy Products

Customers comparing electricity tariffs containing exclusively renewable energy sources are oftentimes lacking the required information about the origin of their accounted electricity. Even though over 700 different retailers in Germany offer green electricity tariffs, the standards between individual contracts vary significantly. In many cases, only a certain percentage of the electricity comes from renewable sources. In order to provide green electricity, individual renewable power plants are typically certified by a number of institutions in a costly process. The energy generated in these plants can then be traded as renewable energy certificates (Brey 2013). The implementation of a blockchain-based system could significantly increase the transparency by making transactions between producing unit and consumer publicly available and thereby raise trustworthiness of green products for end consumers.

The tamper-proof decentralized storage of data in a blockchain enables a transparent documentation of transactions that can be reviewed by all users and is therefore comprehensible. Certificates for renewable and regional electricity production, for example, can be documented on blockchain from the beginning of the production stage. As a result, products such as green and regional electricity can be developed, which are undoubtedly traceable to a source and invulnerable to manipulation. In addition, certificates for tradable emission or CO_2 products are conceivable.

Generating plants, such as PV rooftops or CHPs, can write their own generation services directly into a blockchain via a terminal connected to the Internet. The documentation of the feed-in or any consumption is, therefore, guaranteed. However, it has to be ensured that the system on site (generation plant, measuring equipment) is correctly authenticated and that therefore no incorrect values are invariably written to a blockchain. For example, it must still be ensured that it is an actual PV system that feeds-in locally and that the generated electricity is billed via a calibrated meter.

One solution already available on the market is the so-called GrünStromJetons of startup StromDAO. These assess the current electricity consumption of a household with the green electricity share present in the respective postal code area at the time of consumption in the regional electricity mix, the so-called green electricity index (based on regional generation structure, network topography, weather forecast, and load profile). The participating households receive units of the tradable cryptocurrency GrünStromJetons, depending on their green electricity purchase, with more GrünStromJetons for more related green power. Thus, the tokens provide information on the sustainability of individual electricity purchases or indirectly on the network efficiency of consumption behavior. Furthermore, in addition to the criteria of time and place of power consumption or power generation, it can also be differentiated according to the contribution to grid stability as a criterion of the value for the grid. This, in turn, can serve as a basis for corresponding electricity tariffs for private customers. For the heating and gas market, the examples given are basically transferable.

Neighborhood Models and Microgrids

The ability to conduct secure transactions between agents without an intermediary, to account for them accurately, and to establish automated contractual relationships through smart contracts, enables not only new energy products but also new options for tenant electricity and neighborhood models. The Brooklyn Microgrid in New York City has experienced great media attention in 2016. The blockchain startup LO3 Energy is realizing a peer-to-peer exchange platform (i.e. exchange directly between private subscribers without intervening intermediaries) for electricity (e.g. Mengelkamp et al. 2018). Apart from the regulatory environment, this project fulfills all relevant components of an efficient microgrid energy market, for example microgrid, grid connection, information system, market mechanism, price mechanism, and energy management system. The focus of interest is the market for peer-to-peer solutions, especially for companies: It is expected that especially microgrids and distribution grids are increasingly turning into so-called "transactive grids", in which network-specific requirements and restrictions will be taken into account. By linking with blockchain technology, this creates the prerequisites for transparent and efficient energy trading between a large number of participating systems and the most diverse players, especially in systems with many decentralized units. As a result, the efficiency of the overall system might be increased and customers might profit from cost advantages and opportunities for new business models.

The common basis of the various tenant electricity and neighborhood models is that the generated energy quantities are recorded and written into the blockchain via intelligent measuring systems. There, the transactions are automatically executed and documented between the participants. Decentralized and self-managing, smart contracts ensure that electricity is demanded, for example, when a price threshold is undercut or green electricity or local electricity is available. Billing is also automated. One way to establish an appropriate business model is, for example, the operation of a local donor network, which supports providers to generate regionally renewable energy. For this reason, Conjoule's pilot project brings together private photovoltaic systems with local buyers based on the blockchain. In addition, there is the opportunity to automate energy management for households via smart contracts. Flexible consumers are shifting their demand over time or storing cheap, local, or green electricity. Under certain circumstances, active participation in other markets, such as the market for regulatory power, may be possible.

Local Smart Markets and Energy Trading

Fluctuating renewable energy generation forces utilities to cover their energy demand in smaller time horizons as the actual amount of produced energy in the future is subject to uncertainty. The rising number of decentralized prosumers demand an active participation in the energy market. A central energy trading platform, such as the European Energy Exchange, is not entirely suitable to address local energy imbalances in a decentralized energy sector. Local platforms, on the other hand, induce three major problems. First, operating a platform is costly, as each transaction has to cover its individual costs. Second, a platforms provision would be organized by a single business, performing as an intermediary and charging service fees. Third, the IT infrastructure of a platform usually remains on a single server system, limiting its resilience against attacks. The blockchain technology can potentially solve all three problems. First, blockchains are decentralized and implemented in all participating smart meter devices. A trustful intermediary is not required since the technology allows trustless interactions. Second, a blockchain network is based on an almost autonomous code; therefore, transactions can be processed by smart contracts. Thus, the absence of third parties may potentially decrease transaction costs. Third, based on the decentralized and cryptographic characteristics, blockchains can provide a high resilience against attacks.

Overall, blockchains offer great potential in electricity trading and are a key enabler of balancing and managing the grid from the bottom up instead of today's top-down approach (Morris 2017). Blockchain technology promises direct and anonymous trading in a variety of power market products without the need to resort to a marketplace or intermediary. The main reason for this is the fact that the blockchain allows trusted transactions between unknown actors. An implementation of this idea was presented, for example, with the blockchain application Enerchain in November 2016 and is being carried out by 22 companies in a pilot project. An expansion to balancing group management is also conceivable in the future. Thus, the transmission of relevant information can be made more efficient as well as the load and generation forecast by integrating a variety of micro devices. The actual consumption and production values can be automatically recorded, compared with the forecast and calculated. While technically the balancing group size can be reduced down to final consumers or terminals, among other things the balancing group responsibility raises a number of unanswered questions (e.g. organization of residual electricity supply).

Asset Management

The installed measuring technology and the transfer of data into the blockchain can also be used for asset management. The monitoring and documentation of plant conditions enables efficient management of these plants. This provides operators, regulators, investors, and insurers with accurate and reliable information on the nature and condition of the asset and its ownership status. From this predictive maintenance cases can be constructed, that is, measures for the anticipatory maintenance of plants. Other applications include proving the operational capability of, for example, wind turbines in the event of network bottleneck-induced feed-in reduction, the tamper-proof and distributed storage of ownership and its transaction, as well as efficient auditing. Cost reductions can be achieved here through disintermediation, that is, the elimination of an intermediary, and process acceleration as well as increased resilience of plant monitoring and control that is related to decentralization.

The overlaps between the applications shown here underpin the previous statement regarding the breakup of the traditional value chain by new technologies. Just as the individual economic sectors of mobility, energy and communication are becoming increasingly interconnected, the use of innovative technologies, such as blockchain, blurs the boundaries between the parts of traditional energy supply companies. This creates the need to redesign and rethink conventional corporate structures.

Key Determinants for Blockchain in the Energy Sector

Technical Limitations and Determinants

The applicability of the blockchain technology for processes in the energy value chain depends on technical criteria, such as transaction speed, energy consumption, IT security, and reliability, but also on economic factors and the general acceptance of the technology.

Technical Challenges

Comparable to other fields, the success of blockchains in the energy sector depends largely on the overall development of this technology. For instance, the resilience against internal or external threats has yet to be investigated. That incorporating smart contracts on the blockchain causes inherent vulnerabilities toward outside attacks shows the prominent case of the Ethereum-based application of the Decentralized Autonomous Organization. After attackers were able to temporarily drain a large amount of Ether by exploiting a certain loophole in the code of the blockchain, the organization was eventually able to retrieve the stolen Ether by rolling back the transactions (Del Castillo 2016). However, concerns remained that this so-called "hard fork" might undermine the perception that the blockchain is immutable, and that contract agreements, once settled, would be final. Even though this particular case can be traced back to flawed design, it also raises questions about how decentralized the blockchain really is if major threats should occur.

The cost-effectiveness of blockchains compared to other technologies and the current intermediary-based system will be a major determinant. A network based on P2P-transactions is only feasible if it is able to lower transaction costs significantly. The current versions of blockchains, however, do not come at zero cost, since the so-called PoW concept for the generation of blocks requires extensive amounts of computing capacity (Tapscott and Tapscott 2016). Upcoming blockchains might incorporate a different validation concept, the PoS, which promises further improvements in efficiency (Watanabe et al. 2016). A functioning PoS mechanism could significantly reduce the needed computational capacity, as it is not needed that all connected processors compete against each other on a solution to an algorithmic puzzle, as it is in the PoW. However, this might in return exhibit certain risks regarding the consensus mechanism and allow single participants unwanted exploitation possibilities. More alternatives are being tested out, for example the Delegated PoS by Steemit, EOS, and BitShares or the Byzantine Fault Tolerance by Ripple (Glazer 2018). One of the biggest technical challenges is the scalability of transactions inside the blockchain network. Current blockchains are not yet suitable for high-frequency transactions, especially when taking transaction fees, for example, as the 0.0001 Bitcoin per transaction for the Bitcoin network. In addition to that, the shared ledger will grow much faster. Due to the fact that each participant needs the full ledger to be part of the network, the integration of new participants will be more difficult. The privacy properties of blockchains might constitute a problem as well. The technology provides pseudonymity with a unique address, but it is possible to identify entities behind the blockchain address by analyzing the data on the blockchain (Shrier et al. 2016). Another critical issue is the standardization. The blockchain is a young technology and each initiative is developed on its own individual solution. Standardized blockchain protocols allow the development of software that is more geared to market solutions.

The consumption of permissionless blockchains stems from the computational effort to execute the PoW consensus mechanism. There are no precise calculations for blockchain's energy consumption because the load of the participating devices is not available. However, approximations suggest the total power consumption for instance for the Bitcoin blockchain to be comparable to a developing economy (Digiconomist 2017). The PoS mechanism exhibits lower power consumption since less participants are required to verify transactions. Permissioned and consortium blockchains perform verifications on only a few nodes or cloud solutions and do not consume more energy than conventional database systems. The ecological factors of energy consumption reveal an underlying conflict between decentralized technologies and the aim for green energy. While western enterprises are using permissionless blockchains to reduce transactions costs, datacenters in developing countries fueled by coal may become new pollution havens by verifying their transactions.

Transaction Speed

Already today, the procurable capacity of public blockchains in transactions per second (TpS) is sufficient for applications such as the certification of green electricity and local community/neighborhood power supply. For a wide-spread use of the blockchain technology, however, the limited transaction speed of public blockchains is one of the key limiting factors, e.g., Ethereum currently allows only 10–20 TpS. For comparison, the Visa Network has a maximum capacity of 56,000 TpS and makes 2000 TpS on average, and PayPal runs an average of 155 TpS (Mougayar 2016). A future energy market, with a great number of devices communicating in real-time, sets high requirements for the number of transactions. Current blockchains are not yet suitable for high-frequency transactions (Fig. 2.2).

The reason for this low speed is the employment of the PoW consensus mechanism that is used to validate the transactions. In the medium term (Serenity Release, expected in 2018), the public blockchain Ethereum intends to switch to the less computation-intensive and thus faster PoS consensus mechanism. The promise associated with this change is an up to ten-fold acceleration of the transaction speed. Furthermore, the idea is to further increase the speed by splitting up and parallel processing the transactions in the so-called sharding consensus mechanism. In addition, the shared ledger will grow fast. Since each participant in a public blockchain network needs the full ledger to be part of the network, the integra-

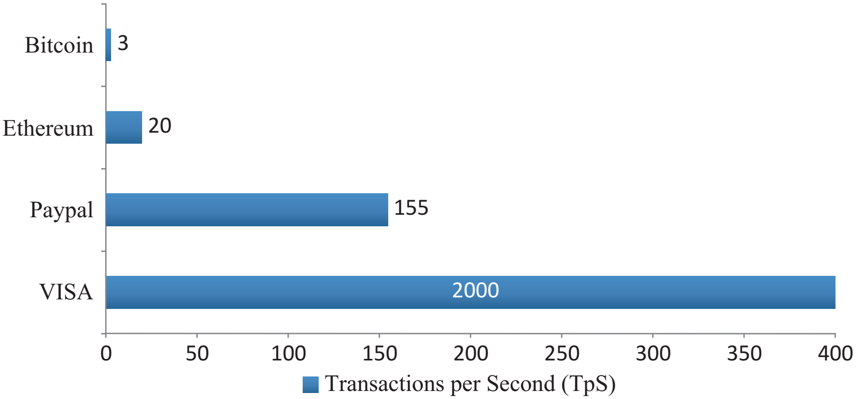


Fig. 2.2 Transaction speed of payment systems (Based on Mougayar 2016; BDEW 2017)

tion of new ones will be difficult. Today, the Bitcoin blockchain, for example, has a size of about 80 gigabytes (Blockchain Info 2016). The future energy market, with a vast amount of production and consumption units communicating on a near real-time basis, sets quite high requirements regarding the number of transactions.

Private blockchains generally do not exhibit technology-related restrictions regarding their transaction speed. As all nodes within a private network are known and regarded trustworthy, they can handle the validation of transactions in an uncomplicated way. This can be done through the so-called PoA mechanism, which might be better suited for high transaction speeds.

Operation and Transaction Costs

The cost-effectiveness of blockchains compared to other technologies and the current intermediary-based system will be a major determinant. A network based on P2P-transactions is only feasible if it is able to lower transaction costs significantly. While the cost of operating private blockchains is generally relatively low and comparable to cloud solutions, in actual practice, the costs mainly depend on the chosen design and thus cannot be estimated without better understanding the specific application requirements first.

On the other side, the costs are perceived as a key obstacle to the spread of the public blockchain technology. Operating the Ethereum network currently costs about 93,440,000$ per year and the Bitcoin network approximately 657,000,000$ per year (Slock.it 2017). The operational costs of an application on the public blockchain mostly consist of the total of transaction fees required to operate it. A simple Ethereum transaction costs about 21,000 gas, which translates to about 0.12 cents at an exchange rate of exchange rate of 300 $/ETH (Wood 2014; Etherscan.io 2017). Compared to existing payment service providers (e.g. a transaction with PayPal costs € 0.35 plus 1.9% of the transaction volume), blockchain transactions are already inexpensive. Average-sized transactions are, therefore, already economically feasible through public blockchains. However, these are still too high in the context of microtransactions. For instance, a typical new refrigerator consumes energy of about 12 eurocents per day on average (150kWh/a × 29 cent/kWh). Flexible purchases of small amounts of electricity from different sources with several transactions per day can thus not be realized economically.

Upcoming blockchains might incorporate a different validation concept, the PoS, which promises improved efficiency. A functioning PoS mechanism could significantly reduce the necessary computational capacity, since not all connected processors compete against each other on an algorithmic puzzle, as in the PoW. This, however, might pose certain risks regarding the consensus mechanism, possibly allowing participants unwanted exploitations. One of the biggest technical challenges is the scalability of transactions inside the blockchain network. If companies manage to reach a critical mass fast enough then private blockchains could prevail. A possible reason for this development is that private blockchains lure more capital, as they promise to develop a proprietary application. In general, the development of two approaches is also conceivable: a peculiar altruistic public blockchain part and a consortium or private blockchain part for business applications. Due to the competition between the various systems, the costs will possibly continue to fall. Furthermore, as high license and software costs are no longer required, consumers are faced to lower costs due to the fact that these services are handled via the blockchain, for example for the neighborly trade of electricity and the exchange of flexibility.

Costs

While the cost of running private blockchains is relatively low and comparable to cloud solutions, the costs for public blockchains are perceived as a major obstacle to the spread of the technology. A simple Ethereum transaction without smart contracts option costs about 21,000 gas (about 1.5–3 cents). By combining transactions, this value can be roughly halved. Compared to existing payment service providers (for example, a transaction at PayPal costs around € 0.35 plus 1.9% of the transaction volume), blockchain transactions are already cheap. As a result, transactions can now be economically represented using public blockchains. In the context of microtransactions, however, these are still too high. On average, a new refrigerator consumes electricity worth about 12 cents per day (150 kWh/a × 29 cents/kWh). Small-scale, flexible purchases of electricity from different sources (for example, from a neighbor with a PV system or a battery) and with multiple transactions per day cannot currently be economically implemented (using public blockchains).

Security

According to current knowledge, the PoW procedure is safe. So far, there was no hack of the actual blockchain, but only the applications on it. However, the security tests are still pending for the "proof-of-stake" mechanism. Private and consortial blockchains are classified as security-friendly between public blockchains and the use of non-blockchain-based methods. However, a common security vulnerability seems to be that very few developers develop these algorithms, and very few, in turn, review these algorithms, even though everything is open source. However, in order to guarantee resilience and thus a lasting security of supply in the energy industry, the entire system, that is the blockchain application as well as other parts of the system, such as smart meters and gateways, must withstand the safety tests.

What Is the Legal Framework for Blockchain?

General Contract and Data Protection Laws

The use of blockchain applications raises a variety of legal issues. These are increasingly being discussed and analyzed in the literature. The legal questions can be clustered into various topics, which can roughly be assigned to general contract law, data protection and IT security law, as well as energy law. A practically relevant case for blockchain applications are the so-called smart contracts. However, the term encompasses more than just contracts in the narrower sense of civil law. It goes beyond this by including the use of software that controls and/or documents or even triggers a legally relevant activity, for example, in the context of existing contractual relationships (Schrey and Thalhofer 2017). Thus, smart contracts can themselves be contracts or just a functional annex to a contract (Jacobs and Lange-Haustein 2017). Smart contracts are code-based and are handled by software applications. On the basis of specified conditions, the software automatically checks whether the predefined conditions exist and carries out the legally relevant activity (matchmaking).

There will be areas where smart contracts are unlikely to ever replace a comprehensive contract. At least more complex contracts are characterized by a certain degree of openness, which can be interpreted case-specifically by experienced lawyers. There are fundamentally different contractual principles that set limits for business via smart contracts. These limits ultimately define what properties should have trades that can reasonably be handled through smart contracts. As far as the conclusion of the contract itself by blockchain is concerned, it should be noted that the general civil law knows no immutable transaction history. These include, for example, the invalidity of contracts, the countervailability of contracts, the repayment after retirement, or the pending invalidity of contracts with minors until they are approved by the legal representative. Here, if necessary, a “reverse transaction” takes place (Schrey and Thalhofer 2017). For the related valuation issues in the analog world, the use of lawyers is required and in case of dispute even often the courts. As a result, transactions through smart contracts should be designed to be as little as possible vulnerable to such disruptions (Jacobs and Lange-Haustein 2017). The smart contract should have the ability to handle bad services at the program level (Kaulartz and Heckmann 2016).

Another relevant topic that sets limits for blockchain applications is data protection law. It accesses where personal data is processed and stored in the blockchain. These include, for example, the right of deletion stipulated from May 2018 by the EU General Data Protection Regulation as well as the "right to be forgotten" and the right to data portability (so-called "victim rights"). In a blockchain, neither data of single individuals can be removed nor finally transferred. Under certain circumstances, a regular complete separation of historical records is possible. Further consideration is needed here as to how the data protection requirements with regard to personal data in the blockchain can be implemented.

Last but not least, IT security regulations must be obliged. When exchanging personal data, network status data and master data originating from intelligent measuring systems, the high technical and cryptographic requirements of the Smart Meter Guidelines of the German Federal Office for Information Security (BSI) apply. In the case of business processes and in market communications, the corresponding requirements are formulated by the Federal Network Agency. Finally, operators of critical infrastructures are obliged to implement IT security standards, which are controlled by the Federal Office for Information Security in terms of their relevance with regard to security of supply.

Energy Regulation

The blockchain technology enables, among other things, the direct settlement of small amounts of electricity (and heat) between households and companies at low transaction costs. In this area, however, there are various legal requirements to consider. In this aspect, we focus on the German energy regulation here, but similar requirements can be found in most markets.

The requirements of the German Energy Industry Act (EnWG), the Electricity Network Access Ordinance (StromNZV), and the associated specifications of the Federal Network Agency are decisive for market access and the exchange of energy via a public network. The StromNZV regulates the conditions for feed-ins of electrical energy into supply points of the electricity networks and the associated simultaneous output of electrical energy at spatially remote consumption points of the electricity supply networks. For the use of the networks and the exchange of energy, it is necessary to conclude a network usage contract and a balancing group contract and to comply with the rights and obligations specified therein. The balancing group contract must be concluded between the transmission system operators and the balancing group managers and regulates the rights, obligations, the necessary information, and data exchange liabilities. These obligations apply to the exchange of energy between market actors, irrespective of which instrument (bilateral business, brokerage, stock exchange transaction, or blockchain technology) has been agreed.

Access to the balancing energy market is regulated by the StromNZV regulations, so that the use of blockchain technology is a new control and billing tool. It requires the prequalification of the plants for the control energy market and the participation in the tenders of the transmission system operators. In addition, the physical feed-in and billing is represented by the schedule management of the balancing group's electricity, so that the conclusion of a balancing group contract is also necessary for the exclusive provision of control energy to the transmission system operator. In addition, the rules of StromNZV for the provision of balancing power by final consumers must be complied with, so that in future small-scale plants and consumers can participate in the balancing energy market. To this end, the Federal Network Agency is aiming for a fix, the cornerstones of which were consulted in the spring of 2017. Thus, the provision of control energy can only be offered with strict control over a blockchain until further notice. Adherence to compliance for wholesale market operations also applies to quantities of energy traded through blockchain technology. For example, the obligation to report transaction data on wholesale energy transactions at European level is covered by the REMIT Regulation.

According to the EnWG, the obligation to report this activity to the regulatory authority is connected to an energy supply to household customers (§ 5 EnWG 2005). In order for the BNetzA to be able to perform its legally assigned supervisory tasks, it is necessary to have a deliverable address for administrative acts in the event of a regulatory application of blockchain. In the current report on digital transformation, the BNetzA is cautiously positioning itself on the subject of blockchain. The developments in terms of energy demand and computing power are to be awaited and tested against the background of security of supply to be guaranteed.

Energy supply contracts also have to meet specific legal requirements. Only by way of example, the obligation to include provisions on the duration of the contract, the price adjustment, termination dates, and notice periods, the customer's right of withdrawal, liability, and compensation arrangements for non-compliance with contractual services and information on the rights of household customers with regard to dispute resolution (§ 41 EnWG 2005). These requirements would at least have to be represented by a framework agreement on the basis of which individual electricity deliveries will be handled via smart contracts.

Conclusion and Outlook

The distributed system architecture of the blockchain harmonizes excellently with an increasingly decentralized energy industry. Greater IT security, efficiencies, potential cost reductions, and transparency are all powerful arguments in favor of blockchain technology that energy companies should use for themselves. New blockchain-based business models and applications are emerging at a fast pace. The maturity of blockchain technology in terms of speed, energy consumption, IT security, reliability, governance, interoperability, and cost-effectiveness is also rapidly evolving. However, it should be noted that currently almost all blockchain applications and projects are still far from having a high market penetration.

In the everyday life of the energy industry, the blockchain technology will only be competitive if important regulatory framework conditions have been clarified. In addition to fundamental challenges in terms of data protection or liability law, specific energy management issues remain unresolved at the moment. Blockchain applications make it possible to automate existing and new energy management processes and to present them in an immutable and transparent manner. Especially for the integration and orchestration of decentralized devices, systems and storages, the blockchain can serve as an instrument to enable real-time communication (e.g. storage recharge), documenting it with proof and providing it as a basis for further applications. A key success criterion will be the integration of blockchain applications into existing standard energy management processes and software. Once interoperability improves, penetration is expected to increase rapidly.

References

Albrecht, S., Reichert, S., Schmid, J., Strüker, J., Neumann, D., & Fridgen, G. (2018). Dynamics of Blockchain Implementation – A Case Study from the Energy Sector. In *Proceedings of the 51st Hawaii International Conference on System Sciences* (pp. 3527–3536). Hawaii: Waikoloa Village. https://scholarspace.manoa.hawaii.edu/handle/10125/50334.

BDEW. (2017). *Blockchain in der Energiewirtschaft – Potenziale für Energieversorger*. Berlin: BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.

Blockchain Info. (2016). *Bitcoin Stats – Bitcoin Currency Statistics*. https://blockchain.info/de/stats

Brey, M. (2013). Warum Nur Wenige Ökostromtarife Die Energiewende Wirklich Vorantreiben. *Econeers Blog*. https://blog.econeers.de/warum-nur-wenige-oekostromtarife-die-energiewende-wirklich-vorantreiben/

Buterin, V. (2014). Slasher: A Punitive Proof-of-Stake Algorithm. *Ethereum Blog*. https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/

Colak, I., Sagiroglu, S., Fulli, G., Yesilbudak, M., & Covrig, C.-F. (2016). A Survey on the Critical Issues in Smart Grid Technologies. *Renewable and Sustainable Energy Reviews, 54*. Elsevier, 396–405.

Daim, T. U., Oliver, T., & Iskin, I. (2013). Research and Development (R&D) Portfolio Management in the Electric Utility Sector. *Benchmarking: An International Journal, 20*(2), 186–211. Emerald Group Publishing Limited. https://doi.org/10.1108/14635771311307678.

Dalkmann, U. (2014). Ansätze im Smart Market für Energie-Vertriebsunternehmen. In: Aichele C., Doleski O. (eds) Smart Market. Springer Vieweg, Wiesbaden, Germany.

Decker, C., & Wattenhofer, R. (2013). Information Propagation in the Bitcoin Network. In *13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P 2013 – Proceedings*. IEEE Computer Society. Trento, Italy.

Del Castillo, M. (2016). Ethereum Executes Blockchain Hard Fork to Return DAO Funds. *Coindesk*. http://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds/

Digiconomist. (2017). Bitcoin Energy Consumption Index. https://digiconomist.net/bitcoin-energy-consumption. Accessed 25 July 2017.

Edelmann, H. (2014). Die Chancen Neuer Und Etablierter Anbieter Im Smart Market. In *Smart Market –Vom Smart Grid Zum Intelligenten Energiemarkt* (pp. 765–793). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-02778-0_27.

EnWG. (2011). Gesetz Über Die Elektrizitäts-Und Gasversorgung (Energiewirtschaftsgesetz -EnWG) – Novelle 2011.

Etherscan.io. (2017). *The Ethereum Block Explorer*. https://etherscan.io. Accessed 15 Oct 2017.

European Commission. (2013). *EU R&D Scoreboard: The 2013 EU Industrial R&D Investment Scoreboard*. Brussels: Office for Official Publications of the European Communities.

Fanning, K., & Centers, D. P. (2016). Blockchain and Its Coming Impact on Financial Services. *Journal of Corporate Accounting & Finance, 27*(5), 53–57. https://doi.org/10.1002/jcaf.22179.

Glazer, P. (2018). An Overview of Cryptocurrency Consensus Algorithms. *Hackernoon*. https://hackernoon.com/an-overview-of-cryptocurrency-consensus-algorithms-9d744289378f

Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2013). A Survey on Smart Grid Potential Applications and Communication Requirements. *IEEE Transactions on Industrial Informatics, 9*(1), 28–42. IEEE.

Jacobs, C., & Lange-Haustein, C. (2017). *Blockchain Und Smart Contracts: Zivil- Und Aufsichtsrechtliche Bedingungen*. ITRB.

Kaulartz, M., & Heckmann, J. (2016). Smart-Contracts-Anwendungen der Blockchain-Technologie. *Computer & Recht, 32*(9), 618–624.

Kolks, U., Pippert, A., & Meyer, J. (2012). Energie Erlebbar Machen – Mit Innovativen Angeboten Kunden Gewinnen. In *Smart Energy* (pp. 81–99). Berlin/Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-21820-0_4.

Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., & Weinhardt, C. (2018, January). Designing Microgrid Energy Markets: A Case Study: The Brooklyn Microgrid. *Applied Energy, 210*. Elsevier, 870–80. https://doi.org/10.1016/J.APENERGY.2017.06.054.

Morris, J. (2017). A New Coalition Looks to Accelerate the Pace of Blockchain in the Energy Sector. *Greentech Media*. https://www.greentechmedia.com/articles/read/bringing-blockchain-technology-to-the-grid#gs.wuvVMW8

Mougayar, W. (2016). *The Business Blockchain : Promise, Practice, and Application of the next Internet Technology*. Hoboken: Wiley.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Ott, E., & Wieg, A. (2014). Please, in My Backyard – die Bedeutung von Energiegenossenschaften für die Energiewende. In C. Aichele & O. Doleski (Eds.), *Smart Market*. Wiesbaden: Springer Vieweg.

Pilkington, M. (2016). Blockchain Technology: Principles and Applications. In F. X. Olleros & M. Zhegu (Eds.), *Research Handbook on Digital Transformations*. Cheltenham.

Rocky Mountain Institute. (2017). Energy Companies Join Forces with Rocky Mountain Institute and Grid Singularity to Launch Global Blockchain Initiative for Energy. *Press Release: Energy Web Foundation Launch*. https://www.rmi.org/about/news-and-press/press-release-energy-web-foundation-launch/

Schlemmermeier, B., & Drechsler, B. (2015). Vom Energielieferanten Zum Kapazitätsmanager – Neue Geschäftsmodelle Für Eine Regenerative Und Dezentrale Energiewelt. In *Marketing Erneuerbarer Energien* (pp. 129–159). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-04968-3_6.

Schrey, J., & Thalhofer, T. (2017). Rechtliche Aspekte der Blockchain. *Neue Juristische Wochenschrift: NJW, 70*(20), 1431–1436. ISSN 0341–1915. https://dialnet.unirioja.es/servlet/articulo?codigo=6176693.

Shrier, D., Wu, W., & Pentland, A. (2016). *Blockchain & Infrastructure (Identity, Data Security)* (pp. 1–19). Massachusetts Institute of Technology – Connection Science.

Slock.it. (2017). Private vs. Public Chain. https://blog.slock.it/public-vs-private-chain-7b7ca45044f. Accessed 23 Oct 2017.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. Sebastopol: O'Reilly and Associates.

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money Business, and the World*. New York: Penguin Publishing Group.

Underwood, S. (2016). Blockchain Beyond Bitcoin. *Communications of the ACM, 59*(11), 15–17. https://doi.org/10.1145/2994581. ACM.

Watanabe, H., Fujimura, S., & Nakadaira, A. (2016). Blockchain Contract: Securing a Blockchain Applied to Smart Contracts. In *2016 IEEE International Conference on Consumer Electronics (ICCE)*. Las Vegas.

Wissner, M. (2011). The Smart Grid – A Saucerful of Secrets? *Applied Energy, 88*(7), 2509–2518. Elsevier.

Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. *Ethereum Project Yellow Paper*, 151. http://www.cryptopapers.net/papers/ethereum-yellowpaper.pdf

Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. In *Proceedings – 2015 IEEE Security and Privacy Workshops, SPW 2015* (pp. 180–184). San Jose. https://doi.org/10.1109/SPW.2015.27. IEEE.

3

Blockchain and the Internet of Things: A Software Architecture Perspective

Chun-Feng Liao, Chien-Che Hung, and Kung Chen

We can perceive the advent of smart living spaces attributed to the fast emerging of Internet of Things (IoT) technologies. By combining with the blockchain technology, many innovative business models can be brought into reality. This chapter examines the state of the art and design

C.-F. Liao (✉)
Department of Computer Science, National Chengchi University,
Taipei, Taiwan

Program in Digital Content and Technologies, National Chengchi University,
Taipei, Taiwan
e-mail: cfliao@nccu.edu.tw

C.-C. Hung
Department of Computer Science, National Chengchi University,
Taipei, Taiwan

K. Chen
Department of Computer Science, National Chengchi University,
Taipei, Taiwan

Department of Management Information Systems, National Chengchi
University, Taipei, Taiwan

H. Treiblmaier, R. Beck (eds.), *Business Transformation through Blockchain*,
https://doi.org/10.1007/978-3-319-99058-3_3

issues of IoT and the blockchain integration from software architecture perspective. In particular, four typical architectural styles for such systems are presented and discussed. The presented architectural styles are useful for helping developers make appropriate design decisions.

Introduction

Recent years have seen increased attention being given to the digital cryptocurrency systems. The blockchain, which originally served as the decentralized platform for verified transactions on the cryptocurrency systems, is probably the most important innovative technology being directly derived from the initial cryptocurrency system (Nakamoto 2008; Wood 2014). Conceptually, the blockchain is a kind of secured distributed data storage where the validity of data is verified by peers. The consensus of peers is achieved based on pre-determined algorithms (e.g. Proof-of-work [PoW] or Proof-of-stake). Therefore, the blockchain enables distributed applications (DApps) to reach consensus in a trustless network without a centralized authority. As reaching consensus among trustless peers is hard (Fisher et al. 1985), the blockchain technologies facilitate many innovative business models that are not easy to realize previously such as ride-sharing (Yuan and Wang 2016), health care (Mettler 2016), medical data access (Azaria et al. 2016), and agri-food supply chain tracing (Tian 2016).

According to Rivera and van der Meulen (2014), the number of interconnected smart objects (i.e. the IoT) will exceed 25 billion in 2020 and go beyond 100 billion by 2050. As a result, current centralized models, either the brokered model (Banks and Gupta 2014) or the client-server model (Bormann et al. 2012), are not sustainable to the future needs. Specifically, the rapid growth of the number of connected things brings about new issues on scalability, security, and privacy. Due to the decentralized nature, the blockchain is considered to be a promising solution to these challenges (Brody and Pureswaran 2014). In addition to distributed transaction processing, an IoT system built based on the blockchain inherently supports peer-to-peer messaging and distributed file sharing among a large number of devices. Besides, the blockchain can also provide a secure billing layer so that it is straightforward to build a peer-to-peer marketplace among things being interconnected by the blockchain network (Christidis and Devetsikiotis 2016).

Meanwhile, it is also important to note that the blockchain itself is not the silver bullet for all problems of IoT systems. Justifications of using the blockchain must be made in advance to avoid the development efforts become a pointless blockchain project (Infante 2018). Even for a justified blockchain-driven IoT (B-IoT) system, it is also important to systematically investigate how the overall architectural design affects the quality attributes of the system. The design issues of a B-IoT system are more complex than a traditional blockchain-driven Web application as a Web application operates only in the cyberspace, whereas a B-IoT system usually involves cyber–physical integration. Unfortunately, as the blockchain and IoT are emerging technologies, the design issues and architectural styles of both the blockchain and IoT systems are still not well-explored (Weyrich and Ebert 2016; Porru et al. 2017), not to mention their combination.

This chapter focuses on the software architecture perspective of B-IoT systems. The next part of this chapter outlines the state of the art of B-IoT research achievements as well as practical applications. Then, we shall explore the challenges faced by the IoT industry and why these problems can be solved by the blockchain technologies. Here we also introduce a case for a B-IoT system, which serves as the context of discussions on the design issues. Next, four typical architectural styles for B-IoT are presented and discussed. Preliminary evaluation of different styles is provided to compare the pros and cons of each given style. Here we focus on established blockchain technologies such as the Bitcoin, Ethereum, or Hyperledger Fabric (Cachin 2016). Architectural design issues of alternative distributed ledger technologies such as the IOTA Tangle (Kusmierz 2017) and blockDAG (Lewenberg et al. 2015) are out of the scope of this chapter.

State of the Art

In the study by Conoscenti et al. (2016), the authors performed a comprehensive literature review on applications of the blockchain and divided the use cases into five categories: data storage management, trade of goods and data, identity management, rating system, and other. The authors notice that among these categories, data storage management, trade of goods and data, and identity management are typical examples where the blockchain has the potential to strengthen the IoT systems. For a specific example of B-IoT data storage management, when combined with a peer-to-peer distributed file system such as IPFS (Benet 2014), the blockchain can be the backbone for establishing a robust and scalable firmware update service for the managed IoT devices (Lee and Lee 2017). Also, Liang et al. (2017) propose to enhance the resilience of IoT data using the blockchain. Examples for trade of goods and data include peer-to-peer smart lock services (Prisco 2016; Han et al. 2017), decentralized electronic marketplaces (Subramanian 2017), thing-to-thing micro payment (Lundqvist et al. 2017), and energy trading (Aitzhan and Svetinovic 2016). Finally, as pointed out by Kshetri (2017), blockchain-based identity management can be leveraged to strengthen the security of IoT systems. Examples include the use of the blockchain to identify the battery in an electric vehicle battery refueling system (Hua et al. 2018) and blockchain-based decentralized authorization service for IoT (Andersen et al. 2017).

Brody and Pureswaran's (2014) influential article pioneered the research of B-IoT. They pointed out the limitations of the current centralized architecture of IoT systems and suggested that there should be a paradigm shift to a decentralized one based on the blockchain technology. Christidis and Devetsikiotis (2016) further elaborate and evaluate this argument and identified several design issues to be addressed before B-IoT systems can be widely accepted and deployed. The most notable issues are the insufficient computing power and storage of IoT devices. There are two typical solutions to these issues. The first approach is to design a new IoT-friendly blockchain which employs a new data structure and new consensus algorithms to ensure the data consistency of the ledgers. For instance, IOTA (Kusmierz 2017) uses Tangle as the underlying data structure. Another new blockchain model for IoT is the Tweetchain (Buccafurri et al. 2017). In Tweetchain, consensus is reached when there is a sufficient number of valid confirmation tweets from the peer nodes. However, as noted by Yeow et al. (2017), the consensus mechanism and security of these new ledger models may have flaws as they are not rigorously verified. Also, it is very hard to employ these new chain models if the B-IoT system is not built from the ground up since due to the existence of legacy blockchain platforms.

An alternative way to deal with the issue of insufficient computing power and storage of IoT devices is to introduce an adaptation node so that the IoT devices can be bridged (by the adaptation node) to the blockchain platform. In the architecture proposed by Samaniego and Deters (2016), there is a one-to-one mapping between a virtual resource, which plays the role of an adaptation node, and an IoT device so that the computational and storage loads can be shifted from the device to a more powerful server. Likely, Teslya and Ryabchikov (2017) proposed an integration architecture for integrating an Industrial IoT (IIoT) platform, Smart M3, with the blockchain. At the core of this architecture is an integration component, which acts like a one-to-one proxy by transforming and transmitting messages between an IIoT node and a blockchain node. In the study by Dorri et al. (2017), a lightweight private immutable ledger architecture is proposed to bridge the gap between an IoT system and the classical blockchain. The adaptation nodes are realized based on the Edge/Fog computing paradigm. That is, the adaptation nodes are hosted by an intermediate computing node between the IoT devices and the cloud. For example, in a smart home, the adaptation nodes are deployed on a home gateway (Özyılmaz and Yurdakul 2017). Detailed studies on designing Edge-centric B-IoT systems can be found in the studies by Kshetri (2017) and Stanciu (2017).

Only a few attempts have so far been made to study the aforementioned issues from the software architecture perspective. Among these works, Xu et al. (2017) performed a comprehensive investigation on the architectural design of blockchain-based systems. The architectural design issues of B-IoT systems are more complex in the sense that, in addition to the original issues, B-IoT systems involve cyber–physical integration. A preliminary study on architectural design issues of B-IoT systems can be found in the study by Liao et al. (2017).

Motivation

In this section, we discuss the motivation of B-IoT systems. Specifically, the challenges faced by traditional IoT systems and why these challenges can be solved by blockchain technologies. As noted by Brody and Pureswaran (2014), the use of IoT technology only succeeded so far in high-value application areas such as jet engine monitoring, smart metering, and healthcare management. The high cost of maintenance (e.g. firmware/software updates) and network connectivity makes it hard to earn profits from the deployed IoT services. It is also hard to ensure security and privacy in current IoT systems by a traditional *security through obscurity* approach. Given that perfect trust on the Internet is not possible nowadays, a *security through transparency* approach is more feasible since the vulnerabilities of a system are publicly aware and can be verified. Following these observations, Brody and Pureswaran (2014) argues that the things should be democratized in the sense that there is no centralized server in a democratized IoT system. Instead, the system composed of connected trustless peers, where all business logic is driven by the consensus among these and all state changes (transactions) must be agreed/verified by some peers. In this way, the blockchain is apparently the key to democratize an IoT system, as it is decentralized, transparent (each peer can examine the transaction records), and the states can only be changed based on consensus. Furthermore, by combining the blockchain and IoT, it is possible to create a transparent and liquid marketplace for physical assets among trustless peers, where IoT makes the physical assets accessible, and the blockchain usually comes with a native billing layer.

Design Issue

Let us now turn to the design issues which originate from combining the blockchain and IoT. There are many design decisions to be made in the process of designing a B-IoT system. However, because of the lack of systematic analysis of the architectural design issues, many B-IoT systems are still designed impromptu. In this section, we shall reveal such design alternatives and how they impact the overall non-functional quality attributes of a B-IoT system.

The Location of Blockchain Endpoints

From a network's point of view, the blockchain is essentially a peer-to-peer network. In this article, a peer node in the blockchain is called a blockchain endpoint. In a blockchain, each endpoint keeps its copy of global block data. The consistency among the copies is ensured by the underlying consensus algorithm of the blockchain such as PoW, proof-of-stake, or Practical Byzantine Fault Tolerance. An endpoint is also responsible for verifying transaction requests. A transaction request in the blockchain represents a claim of state change. In a PoW blockchain, endpoints can be configured so that they are responsible for generating new blocks through a competitive process called mining. As an incentive to mining, cryptocurrencies are awarded to the endpoint that successfully generates a new block. Obviously, a blockchain endpoint is burdened with computation (transaction processing and mining) and storage loads (block data). To perform transactions (e.g. receiving or sending digital currencies and changing contract states) on the blockchain, an IoT device can either be part of the blockchain (by serving as an endpoint) or delegate its requests to a blockchain endpoint which serves as the adaptation node for IoT devices to the blockchain.

In practice, both approaches work, but each method brings about different impacts on the system's quality attributes. As mentioned, to serve as an endpoint in the blockchain, the additional burden for an IoT device is twofold: (1) The computation load for transaction processing and mining; (2) The storage requirement for storing the global block data. In short, the price to pay is the higher cost for IoT devices. In many IoT usage scenarios, it is infeasible to deploy such high-end IoT devices. In some blockchain implementations, the endpoints can be configured so that the computation or storage loads can be reduced. In Ethereum, for example, the mining function can be turned on or off dynamically and remotely without shutting down the node. Besides, an endpoint can be configured so that it is in the Fast Sync mode or the Light Sync mode. In the Fast Sync mode, the endpoint does not process transaction requests. Instead, it just gets a snapshot of global data after a certain number of blocks are generated. In the Light Sync mode, the endpoint gets only block headers and current states of the blockchain. The block data are retrieved on demand from nearby fully functional endpoints.

On the other hand, if the transactions are delegated to the adaptation node, then the computation and storage load can be shifted to the adaptation node, which is typically deployed on the edge or the cloud. However, if no redundant adaptation nodes are deployed, then the adaptation node itself can be the single point of failure. Also, in order to delegate the transactions to an adaptation node, the IoT device must have the private key and accounts being transferred to the adaptation node. In other words, the delegating node must trust the delegated node and the network, which is potentially a security vulnerability. However, there is a technique to alleviate this issue. In Ethereum and Bitcoin, a transaction can be constructed and then signed by a private key in an off-chain node. Then, the signed transaction can be verified and processed by a remote blockchain endpoint without the private key. This technique is known as the raw transaction processing. To sum up, the decisions of the whether to and how to deploy a blockchain endpoint on an IoT device have significant impacts on the non-functional qualities of the system and thus are an essential architectural consideration.

The Distribution of Business Logic and Data

When considering the design issues of B-IoT systems, it is helpful to further divide them into two groups, namely, the front-end and the back-end. This section focuses on the back-end of a blockchain application, which includes the blockchain infrastructure and legacy enterprise systems that interact with the blockchain application to fulfill the business needs. The front-end of a blockchain application refers to the user interfaces (UIs) or physical IoT devices. The design issues of the front-end are taken up in the next section.

In the back-end of a blockchain application, the states and business logic for querying and modifying the states are reified as a smart contract. Technically, a smart contract is a serialized stateful business object stored in the blockchain. Such a stateful object consists of a set of states and scripts (methods). After a contract is deployed, a unique address, serving as the reference to the contract, will be generated. Then, every endpoint of the blockchain can access the smart contract through the reference. In practice, many smart contracts have to interact with external legacy systems. For instance, a smart contract may need to get data from a database or to modify external data as a result of reacting to the contract state change. Therefore, in addition to the blockchain infrastructure and the smart contracts, the back-end of a real-world blockchain applications also include legacy enterprise systems such as Web servers, application servers, and databases. Therefore, the design consideration of the distribution of business logic and data for the back-end of a B-IoT system is typically similar to that of a general blockchain application. In the back-end of a B-IoT system, the business logic and data can be placed either in the smart contract or in the external enterprise systems. To benefit from the blockchain technology, the business logic and data must be deployed as smart contracts in the blockchain. Nevertheless, it is usually not a good practice to put all logic and data in the smart contract. If block data are replicated in each node, putting all data in the blockchain can quickly drain out the network bandwidth and the storage spaces. Also, due to the low transaction processing rate, not every business logic is suitable for being placed in a smart contract. These new alternatives raise new design consideration for developers, that is, which parts of logic and data are suitable for placing in the blockchain and which parts are not.

The Mechanisms of Cyber–Physical Integration

The front-end of a blockchain application refers to UIs or physical IoT devices. Theoretically, a front-end of a blockchain application needs to "wrap" an endpoint as the block data and smart contracts are only accessible through an endpoint. In the real world, this is not always necessary because most endpoint implementations of popular blockchain technologies expose remote accessible APIs (Application Programming Interfaces). For instance, both Bitcoin and Ethereum endpoints expose JSON-RPC and many other language-specific APIs. The most popular architecture of a blockchain application consists of a Web page hosted on a Web server, where the front-end logic is embedded in the HTML using JavaScript. The JavaScript manipulates the endpoints through the endpoint-exposed API to interact with the smart contract. However, the architecture mentioned above must be extended in a B-IoT system, since both Web-based UIs and IoT devices belong to the front-end.

The style of cyber–physical integration is an important issue for IoT systems and has a great impact on system quality attributes when designing an IoT system based a blockchain. For example, before a user can use a rented smart thing, what is the target of the payment? If each smart thing is associated with a smart contract, then the user can transfer payments to the thing, where the payment is processed by the blockchain endpoint embedded in the thing (on-chain). Otherwise, the processing of the transaction has to be delegated to a powerful off-chain node (e.g. servers in the edge or cloud). Another issue is how the service provider finds and controls things. For example, after the payment is confirmed, the renting service unlocks the rented device either by WebSocket (off-chain) or by issuing a contract event (on-chain).

In general, the off-chain approaches are considered to be less secure. To extend the functionality of the blockchain, the off-chain approaches attach additional links, which are not part of the blockchain network and therefore vulnerable, to the blockchain endpoints. As mentioned, to delegate the transaction processing to a server, the server must have the private key, making the design deviating from one of the key motivation of using the blockchain: working in a trustless network. Finally, overuse of off-chain mechanisms is harmful to a decentralized architecture, since delegating the tasks to the servers is a move toward the centralized approach, making the use of the blockchain less meaningful. Consequently, the system designer must strike a balance between the use of off-chain mechanism and the cost of IoT devices (computing power and storage).

Architectural Styles

By taking the design considerations mentioned in the previous section into account, we can come up with four typical architectural styles for B-IoT services. Based on the placement strategy of blockchain endpoints, the four architectural styles are called Fully Centralized, Pseudo Distributed Things, Distributed Things, and Fully Distributed.

Before going into the details of the styles, it is beneficial to take a look at an illustrative use case of a B-IoT system so that we can explain these styles in a precise and concrete manner. The scenario is a blockchain-based vehicle-renting service, which is similar to Slock.it (Prisco 2016). In such a scenario, users can search for a smart car and then rent and pay for it using their smartphones. After payment is confirmed, the smart vehicle is automatically unlocked. The car will be automatically locked again after the lease time has expired. As a proof of concept and a target of the investigation, we have realized a prototype of such platform on Ethereum. Inside the smart vehicle is an Arduino, an open source reprogrammable electronics platform, for controlling the motor and interacting with the instrument panel. There is also a Raspberry Pi, a popular open source low-cost yet powerful (with ARM-based CPU) embedded computer, which hosts the software and (optionally) the light node.

Figure 3.1 illustrates the general usage scenario for the vehicle-renting service driven by B-IoT. The details of each step in Fig. 3.1 are explained below.

1. The vehicle owner first configures the parameters of the vehicle to be rented. For example, the account and the renting price. These parameters are then encoded as a blockchain transaction that updates the contract state.
2. A user wants to rent the car using a smartphone. First, the smartphone scans the QR code, which indicates the account address of the device owner. After that, the user decides to rent the vehicle. The user trans-

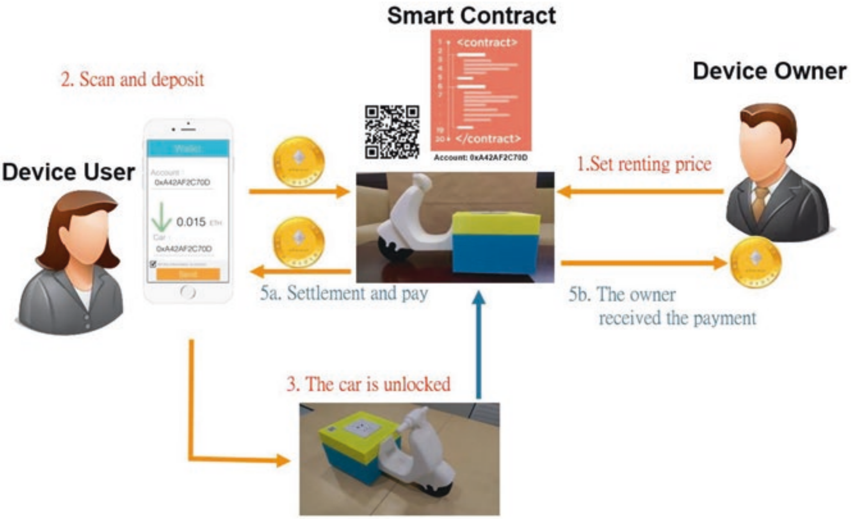


Fig. 3.1 A car renting platform scenario

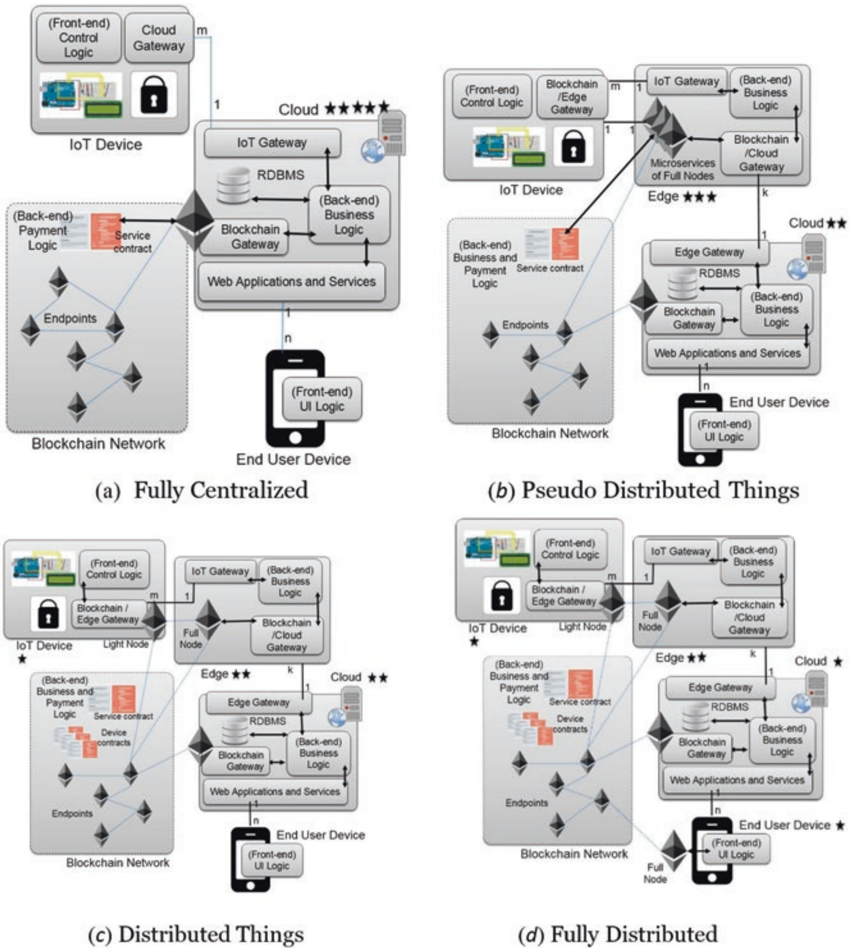
fers money (cryptocurrency) to that account using the DApp installed on the smartphone. This action leads to another transaction being submitted and processed on the blockchain.

3. Based on the contract logic, the car finds that the transaction is valid. Thus, the vehicle is unlocked and can be used by the user.
4. The renter can operate the vehicle during the renting period.
5. To return the vehicle, the renter presses a button on the dashboard of the vehicle. According to the rules encoded in the smart contract, the money stored in the smart contract is cleared: the renting fee is withdrawn from the deposited money; the remaining money is returned to the renter's account. Also, the state of the smart contract is modified to reflect the fact that it is returned by the user and is available for rent.

Now we are ready to examine the details typical for B-IoT architectural styles. In the following, we examine each of the architectural styles based on the three design issues: the locations of blockchain endpoints, the distribution of business logic and data, and the mechanisms of cyber–physical integration. It is important to point out that the architectural styles presented here are not an exhaustive list of all possible cases. There are many intermediates between the presented styles, which are chosen based on representativeness and popularity. The purpose of these styles is to serve as a useful starting point so that the developer can customize the architecture to make the system more suitable for specific needs.

Fully Centralized

One naive approach is shown in Fig. 3.2a. The architecture is essentially identical to the traditional centralized IoT system except that there is a blockchain endpoint deployed in the cloud. This architecture includes four major components: the cloud, the IoT device, the end-user device, and the blockchain network. The front-end includes the control logic for operating the sensors and actuators on the IoT device and the UI logic for interacting with users. The back-end includes the payment logic in the smart contract and the general business logic placed in the cloud. All system states are also kept in the cloud.



(a) Fully Centralized

(b) Pseudo Distributed Things

(c) Distributed Things

(d) Fully Distributed

Fig. 3.2 Architectural styles of B-IoT systems. The number of stars indicates the degree of computation and storage loads of each component

Apparently, there is one and only one blockchain endpoint in the system, so that the whole B-IoT system is virtually a node in the blockchain. The consequence is that the blockchain only serves as a billing layer and that all transactions (both database and the blockchain) and most of the back-end business logic are performed in the cloud. Also, all system states are kept in the database in the cloud. This architectural style employs the traditional cyber–physical integration mechanism. That is, it interacts with the cloud through the gateway. The IoT device is not aware of the blockchain.

Figure 3.2 also reveals the distribution of computation and storage loads using the star marks. It is assumed that the total computation and storage loads for the overall system is five stars. The cloud component in Fig. 3.2a is marked by five stars so that virtually all computation and storage resources are centrally provided by the cloud platform. In this sense, this architectural style is called Fully Centralized. From the blockchain's point of view, most of the system components (except for the payment logic) are off-chain. In other words, the blockchain is only used as a billing layer. This design departs from the decentralization philosophy of the blockchain and does not benefit much from the blockchain technology: scalable and distributed consensus. Consequently, this architecture is generally not an appropriate choice if the main objective is to deal with the problems of an IoT system by decentralizing the system but the design is still a centralization. However, this architecture style can be useful if there is already a legacy IoT system and the development team wants to test the blockchain technology by integrating payment functionality. As a result, the main advantage of this style is that it is a transparent yet naive way to combine an IoT system with a blockchain.

Pseudo Distributed Things

To embrace the philosophy of decentralization, we need to make most of the entities in the system as a peer in the blockchain network. Ideally, each IoT and end-user device should be a blockchain endpoint. As mentioned, due to the low-cost requirement of computing power, storage, and network bandwidth in IoT systems, placing a fully functional blockchain endpoint in each device is usually not feasible in reality. As mentioned, one approach to remedy this problem is to introduce adaptation nodes so that the devices can be bridged to the blockchain. A typical architectural style to realize this approach is called Pseudo Distributed Things. As shown in Fig. 3.2b, an additional edge component is added, which hosts a set of blockchain endpoints serving as the adaptation nodes. The IoT device can send a transaction to the blockchain by composing a signed and serialized raw transaction and then delegating the transaction processing task to the adaptation nodes. Depending on the number of IoT devices, the edge server may need to initiate one or more endpoints. An efficient way to manage these dynamically allocated endpoints is to use the Microservice architecture (Nadareishvili et al. 2016).

Most of the endpoints are deployed to the edge. Thus, the computation and storage loads are shifted from the cloud to the edge. As shown in Fig. 3.2b, three out of five stars indicate that the loads are marked on the edge. Also, this architectural style facilitates more flexible distribution of business logic, as some business logic can be placed at the edge. It is also possible to place business logic in the smart contract as each IoT device can invoke the contract methods (via the adaptation nodes). However, as IoT devices must communicate with the edge server through the network, putting too much logic in the contract also leads to more traffic among IoT devices and the edge server. This is usually undesirable as the bandwidth of an IoT network is typically limited and thus very precious. As for the cyber–physical integration mechanism, this architectural style supports both on-chain (through the adaptation node) and off-chain (through the IoT gateway in the edge server) integrations. On-chain cyber–physical integration is more secure and scalable, but the price to pay is the bandwidth of IoT network.

This architecture is called Pseudo Distributed Things in the sense that the endpoints are physically located on the edge but can be logically associated with IoT devices. The introduction of the edge server provides the flexibility of this architectural style: the IoT devices can act as peers in the blockchain network while the endpoints need not be deployed on these devices. Conversely, the cost is heavier device-edge traffic. Therefore, when using this style, the developer needs to strike a balance between decentralization and the use of IoT network resources.

Distributed Things

Recently, major blockchain platforms started to support different synchronization modes. In Hyperledger Fabric, there are four types of blockchain endpoints (member service node, validating node, non-validating node, and application node) and each type is with different synchronization mode. In Bitcoin, there is a mechanism called Simplified Payment Verification (SPV). By SPV, a device with insufficient computing and storage resources is able to request the blockchain data from nearby trusting full nodes instead of downloading the whole copy of the blockchain. Ethereum introduces the concept of the light client, which can perform the tasks of an endpoint in a low-capacity environment. The core idea is that each light client is assisted by some light servers and a peer serves as a full node hosted on a more powerful machine (e.g. the edge server) so that the light client can perform partial tasks and keep partial data at a time. Such improvements allow us to place light client endpoints on some high-end IoT devices, so that the Distributed Things architecture can be realized. As shown in Fig. 3.2c, the computation and storage loads are shifted to the IoT device, making the overall architecture more decentralized.

With the support of the full node on the edge server, the endpoints (light client) can be placed in the IoT devices. The main improvement is that the IoT devices can process the transactions on their own so that the traffic from the device-edge is greatly reduced. Such an architecture makes the IoT system logically decentralized as all IoT devices are part of the blockchain. Also, more business logic can be placed in the smart contract as each device can directly react to the contract event. Like Pseudo Distributed Things, the Distributed Things architecture supports both on-chain (through the light client) and off-chain (through the IoT gateway in the edge server) integrations. In the on-chain integration approach, the IoT gateway is removed from the IoT device since it is now controlled directly by reacting to the contract events. If the IoT device is powerful enough for hosting an endpoint, then implementing the system following the Distributed Things style is a good choice. The main obstacle that prevents the developer from using this style is the cost of IoT devices.

Fully Distributed

The architecture can be Fully Distributed if an endpoint is also deployed in the end-user device. In the Fully Distributed architecture, the service provider does not implement payment logic. Instead, a user pays directly to the address of the smart contract associated with the thing one is going to rent. Again, as shown in see Fig. 3.2d, one star representing the computation and storage loads can be shifted from the cloud to the end-user device making the overall architecture even more decentralized.

The Fully Distributed architecture is identical to Distributed Things architecture except that in Fully Distributed architecture, all user devices have endpoints (either full nodes or light clients) installed. Hence, all components in the B-IoT system become a peer node in the blockchain network. Figure 3.2d also reveals that a star is moved from the cloud to the end-user device to reflect the offloading of most of the cloud's computation and storage burdens. Storing a large amount of data in the blockchain is considered harmful as the stored data are replicated and stored by all peers. Thus, in most cases, the cloud is still required as B-IoT systems need a place to hold the data that are not kept in the blockchain. Theoretically, this is the ideal architectural style for B-IoT systems as in such architecture all entities, including the end-user device, are part of the blockchain. For a public B-IoT system, it is usually impractical to expect that all users have the endpoint installed on their devices which makes this architectural style infeasible. However, for a private B-IoT system used by a small group of users, it is possible to have the endpoint installed on the end-user devices. In such case, a Fully Distributed architecture is possibly a good choice.

Discussions

Avoiding Pointless B-IoT Projects

We have mentioned that before starting to build a B-IoT system, a justification of using the blockchain in an IoT project has to be made to avoid a "pointless blockchain project". Greenspan (2015) provides a useful guideline for evaluating general blockchain usages. These rules are also applicable to B-IoT projects. Generally speaking, there must be a need for a scalable shared database and the database is going to be modified by many un-trusted nodes. Also, there must be a need that the transactions (for modifying the database) are created by peers that do not trust each other. In the vehicle-renting service example, vehicle devices (IoT devices) and user devices (the smartphones) do not trust each other, but they need to interact and share service states via the blockchain to deliver the service. Also, note that storing data in the blockchain is expensive as all full nodes must hold a copy of the block. As a result, storing potentially large amounts of sensor data in the blockchain does not make sense. In fact, the storage of the blockchain is usually referred to as a distributed ledger instead of a distributed database to avoid the misleading and inappropriate use of the blockchain.

Selecting an Architectural Style

Table 3.1 is a summary of the quality attributes of the architectural styles discussed. The first column shows the distribution of endpoints. The more places in which the endpoints can be deployed, the higher the degree of decentralization the overall architecture. As mentioned, the degree of decentralization affects how the overall system can benefit from the blockchain. The second column is the distribution of back-end business logic. It can be observed that when the overall architectural style is closer to Fully Centralized architecture, then more business logic is implemented in the cloud. In contrast, more business logic is shifted to the smart contract as the degree of decentralization increases. Finally, when the style is more distributed, less off-chain links are needed. Ideally,

Table 3.1 A summary of architectural styles for blockchain-driven IoT systems

Style name	Endpoint location	Back-end business logic	Minimal off-chain links
Fully Centralized	Cloud	Cloud+++, Contract(+)	m + n
Pseudo Distributed Things	Cloud and edge	Cloud++, Edge+++, Contract+	m + n
Distributed Things	Cloud, edge, and IoT devices	Cloud++, Edge++, Contract++	n
Fully Distributed	Cloud, edge, IoT Devices, and user devices	Cloud+, Edge+, Contract++	0

Business logic: +++=mostly, ++=many, +=some, (+)=very few
n number of user devices, *m* number of IoT devices

one should design systems so that the architectural style is as close to a Fully Distributed architecture as possible. Because when there are more off-chain links, the system is less robust and less secure.

Implementing Architectural Styles

Among the four architectural styles, implementing Fully Centralized and Fully Distributed is straightforward as the former is similar to a legacy enterprise system and the latter is similar to a typical blockchain application. Implementing the two intermediate styles is less intuitive and needs more sophisticated designs. Let us first make a more in-depth exploration of the implementation issues for the Pseudo Distributed Things style. The key technique is called "raw transaction". It is also known as "signed transaction" as the core idea is to have the serialized transaction constructed by the IoT device and then signed using the private key embedded in the device. After that, the signed transaction is sent to the edge and processed by a full node. To realize such a design, libraries for private key recovery (e.g. Keythereum) and transaction processing (e.g. ethereumjs-tx) are needed. It is noteworthy that there is a potential vulnerability in the link that connects IoT devices and the edge server. In Ethereum, the core technology to realize the Distributed Things style is the Light Ethereum Subprotocol (LES) mechanism. The prerequisite of this style is to have an endpoint being deployed on the IoT devices and then adjust the synchronization mode so that the endpoints become a light client that interacts with a full node by LES. In this way, the IoT devices can act like a blockchain peer and can check account balance or obtain block information without any intermediate entities.

Conclusion

Until recently, designing B-IoT systems is still considered as a very challenging task. This chapter presents integration design issues of IoT and the blockchain from a software architecture perspective. In addition, we also reviewed the most notable characteristics: endpoint locations, distribution of business logic, and cyber–physical integration. Based on these issues, four representative architectural styles are presented and examined. The introduced architectural styles are useful for helping developers to make appropriate design decisions. Theoretically, a developer should design B-IoT services so that they are as close to the Fully Distributed architecture as possible. Nevertheless, one may find that other styles are more appropriate because of efficiency or cost considerations. Until recently, many fundamental parts of the blockchain are still unstable. Most of them have significant impacts on the architectural considerations. A notable example is the consensus algorithm. Selecting the most appropriate consensus algorithm for B-IoT is a controversial issue and is still under active research. Hopefully, these new changes can support more innovative and flexible architectures and help developers to design a more decentralized IoT in a cost-efficient manner.

References

Aitzhan, N. Z., & Svetinovic, D. (2016). Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Transactions on Dependable and Secure Computing* (pre-print). https://doi.org/10.1109/TDSC.2016.2616861.

Andersen, M. P., Kolb, J., Chen, K., Fierro, G., Culler, D. E., & Popa, R. A. (2017). Wave: A Decentralized Authorization System for IoT Via Blockchain Smart Contracts. *Technical Report UCB/EECS-2017-234*, EECS Department, University of California, Berkeley.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). Medrec: Using Blockchain for Medical Data Access and Permission Management. In *Proceedings International Conference on Open and Big Data* (OBD) (pp. 25–30), NY, USA. IEEE.

Banks, A., & Gupta, R. (2014). *MQTT Version 3.1. 1*. OASIS Standard. http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/csprd02/mqtt-v3.1.1-csprd02.html. Accessed 14 Feb 2018.

Benet, J. (2014). IPFS-Content Addressed, Versioned, P2P File System. arXiv Preprint arXiv:1407.3561. https://arxiv.org/abs/1407.3561. Accessed 14 Feb 2018.

Bormann, C., Castellani, A. P., & Shelby, Z. (2012). CoAP: An Application Protocol for Billions of Tiny Internet Nodes. *IEEE Internet Computing, 16*(2), 62–67.

Brody, P., & Pureswaran, V. (2014). *Device Democracy: Saving the Future of the Internet of Things*. https://www-935.ibm.com/services/multimedia/GBE03620USEN.pdf. Accessed 14 Feb 2018.

Buccafurri, F., Lax, G., Nicolazzo, S., & Nocera, A. (2017). Overcoming Limits of Blockchain for IoT Applications. In *Proceedings 12th International Conference on Availability, Reliability and Security* (p. 26). NY, USA. ACM.

Cachin, C. (2016). Architecture of the Hyperledger Blockchain Fabric. *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*. Chicago. https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf. Accessed 14 Feb 2018.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access, 4*, 2292–2303. IEEE.

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A Systematic Literature Review. In *Proceedings 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications* (AICCSA) (pp. 1–6), NY, USA. IEEE.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an Optimized Blockchain for IoT. In *Proceedings Second International Conference on Internet-of-Things Design and Implementation* (pp. 173–178). NY, USA. ACM.

Fisher, M. J., Lynch, N., & Paterson, M. S. (1985). Impossibility of Distributed Consensus with One Faulty Process. *Journal of the ACM, 32*(2): 374–382, ACM.

Greenspan, G. (2015). *Avoiding the Pointless Blockchain Project*. https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project. Accessed 14 Feb 2018.

Han, D., Kim, H., & Jang, J. (2017). Blockchain Based Smart Door Lock System. In *Proceedings 2017 International Conference on Information and Communication Technology Convergence* (ICTC) (pp. 1165–1167). NY, USA. IEEE.

Hua, S., Zhou, E., Pi, B., Sun, J., Nomura, Y., & Kurihara, H. (2018). Apply Blockchain Technology to Electric Vehicle Battery Refuelling. In *Proceedings of 51st Hawaii International Conference on System Sciences* (pp. 4494–4502), Atlanta, GA, USA. Association for Information Systems.

Infante, R. (2018). *Building Ethereum DApps: Decentralized Applications on the Ethereum Blockchain*. Shelter Island, NY. USA. Manning Publications.

Kshetri, N. (2017). Can Blockchain Strengthen the Internet of Things? *IT Professional, 19*(4), 68–72.

Kusmierz, B. (2017). *The First Glance at the Simulation of the Tangle: Discrete Model*. https://iota.org/simulation_tangle-preview.pdf. Accessed 14 Feb 2018.

Lee, B., & Lee, J.-H. (2017). Blockchain-Based Secure Firmware Update for Embedded Devices in an Internet of Things Environment. *The Journal of Supercomputing, 73*(3), 1152–1167. Springer.

Lewenberg, Y., Sompolinsky, Y., & Zohar, A. (2015). Inclusive Blockchain Protocols. In *Proceedings International Conference on Financial Cryptography and Data Security* (pp. 528–547). Heidelberg, Berlin. Springer.

Liang, X., Zhao, J., Shetty, S., & Li, D. (2017). Towards Data Assurance and Resilience in IoT Using Blockchain. In *Proceedings 2017 IEEE Military Communications Conference* (MILCOM) (pp. 261–266). NY, USA. IEEE.

Liao, C.-F., Bao, S.-W., Cheng, C.-J., & Chen, K. (2017). On Design Issues and Architectural Styles for Blockchain-Driven IoT Services. In *Proceedings International Conference on Consumer Electronics-Taiwan* (ICCE-TW) (pp. 351–352). NY, USA. IEEE.

Lundqvist, T., de Blanche, A., & Andersson, H. R. H. (2017). Thing-to-Thing Electricity Micro Payments Using Blockchain Technology. In *Proceedings Global Internet of Things Summit* (GIoTS) (pp. 1–6). NY, USA. IEEE.

Mettler, M. (2016). Blockchain Technology in Healthcare: The Revolution Starts Here. In *Proceedings 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services* (Healthcom) (pp. 1–3). NY, USA. IEEE.

Nadareishvili, I., Mitra, R., McLarty, M., & Amundsen, M. (2016). *Microservice Architecture: Aligning Principles, Practices, and Culture*. Sebastopol, CA, USA. O'Reilly Media, Inc.

Nakamoto, S. (2008). *Bitcoin: A Peer-To-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf. Accessed 14 Feb 2018.

Özyılmaz, K. R., & Yurdakul, A. (2017). Integrating Low-Power IoT Devices to a Blockchain-Based Infrastructure: Work-in-Progress. In *Proceedings Thirteenth ACM International Conference on Embedded Software 2017 Companion* (p. 13). NY, USA. ACM.

Porru, S., Pinna, A., Marchesi, M., & Tonelli, R. (2017). Blockchain-Oriented Software Engineering: Challenges and New Directions. In *Proceedings 39th International Conference on Software Engineering Companion* (pp. 169–171). NY, USA. IEEE.

Prisco, G. (2016). Slock.it to Introduce Smart Locks Linked to Smart Ethereum Contracts, Decentralize the Sharing Economy. *Bitcoin Magazine*. Available https://bitcoinmagazine.com/articles/sloc-it-to-introduce-smart-locs-lined-to-smart-ethereum-contractsdecentralize-the-sharing-economy-1446746719. Accessed 14 Feb 2018.

Rivera, J., & van der Meulen, R. (2014). *Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units by 2020*. http://www.gartner.com/newsroom/id/2636073. Accessed 14 Feb 2018.

Samaniego, M., & Deters, R. (2016). Hosting Virtual IoT Resources on Edge-Hosts with Blockchain. In *Proceedings 2016 IEEE International Conference on Computer and Information Technology* (CIT) (pp. 116–119). NY, USA. IEEE.

Stanciu, A. (2017). Blockchain Based Distributed Control System for Edge Computing. In *Proceedings 21st International Conference on Control Systems and Computer Science* (CSCS) (pp. 667–671). NY, USA. IEEE.

Subramanian, H. (2017). Decentralized Blockchain-Based Electronic Marketplaces. *Communications of the ACM*, *61*(1), 78–84. ACM.

Teslya, N., & Ryabchikov, I. (2017). Blockchain-Based Platform Architecture for Industrial IoT. In *Proceedings 21st Conference of Open Innovations Association FRUCT* (p. 42). NY, USA. IEEE.

Tian, F. (2016). An Agri-Food Supply Chain Traceability System for China Based on RFID & Blockchain Technology. In *Proceedings 13th International Conference on Service Systems and Service Management* (pp. 1–6). NY, USA. IEEE.

Weyrich, M., & Ebert, C. (2016). Reference Architectures for the Internet of Things. *IEEE Software, 33*(1), 112–116.

Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. *Ethereum Project Yellow Paper*. https://bravenewcoin.com/assets/Whitepapers/Ethereum-A-Secure-Decentralised-Generalised-Transaction-Ledger-Yellow-Paper.pdf. Accessed 14 Feb 2018.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., & Rimba, P. (2017). A Taxonomy of Blockchain-Based Systems for Architecture Design. In *Proceedings IEEE International Conference on Software Architecture* (ICSA) (pp. 243–252). NY, USA. IEEE.

Yeow, K., Gani, A., Ahmad, R. W., Rodrigues, J. J., & Kwangman, K. (2017). Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues. *IEEE Access, 6*, 1513–1524.

Yuan, Y., & Wang, F.-Y. (2016). Towards Blockchain-Based Intelligent Transportation Systems. In *Proceedings IEEE 19th International Conference on Intelligent Transportation Systems* (ITSC) (pp. 2663–2668). NY, USA. IEEE.

4

Distributed Ledger Enabled Internet of Things Platforms: Symbiosis Evaluation

Daniel Burkhardt, Patrick Frey, Simon Hiller, Alexander Neff, and Heiner Lasi

Introduction

The Internet of Things (IoT) is formed by the fusion of Information Technology (IT) and Operation Technology (OT), enabling assets to support human beings ubiquitously. In this way, many new opportunities but also challenges arise that need to be leveraged in order to add value. Interconnectivity between the assets on the edge is one condition that needs to be achieved to realize this vision.[1] Additionally, data is required to be interoperable on the platform layer. Both challenges are approached by IoT platforms. However, from the user perspective IoT platforms effect a centralization of data and overtake its ownership, which has manifold consequences. One example is the current scandal of Cambridge Analytica using

[1] The edge tier describes the physical layer where sensors and actors are placed to collect data from the real-world processes.

D. Burkhardt (✉) • P. Frey • S. Hiller • A. Neff • H. Lasi
Ferdinand-Steinbeis-Institute, Stuttgart, Germany
e-mail: daniel.burkhardt@steinbeis.de; patrick.frey@steinbeis.de; simon.hiller@steinbeis.de; alexander.neff@steinbeis.de; heiner.lasi@steinbeis.de

H. Treiblmaier, R. Beck (eds.), *Business Transformation through Blockchain*,
https://doi.org/10.1007/978-3-319-99058-3_4

millions of Facebook profiles to broadcast misinformation over the internet (Channel4 2018). This fact shows how an abuse of data and a power centralization in a social media platform can trigger misleading actions. In the IoT, such acts can have even worse consequences. Therefore, building blocks are required that guarantees data democracy and trust of the IoT.

Distributed Ledger (DL) concepts, such as Blockchain (BC), are intensely discussed topics in the world economy at present (Burgwinkel 2016). The reason is that this is the first time a consensus has been achieved without any centralized server (Tapscott 2016). Several enterprises, including McKinsey (Tapscott 2016) and SAP (Leukert 2016), see DL as having an enormous potential to revolutionize entire industries. The underlying data structures provide transparency, irreversibility, anonymity and distribution (Burkhardt et al. 2018). Especially in a connected and integrated world, where economic activities take place in business networks, the transformation of these characteristics could be of enormous importance (Brakeville and Perepa 2018).

DL generic platforms (DLgp), such as Ethereum or Hyperledger, are developed to make cross-industry collaboration possible (Hyperledger). Both ecosystems include the implementation of decentralized applications (DApps) on top of smart contracts. Large IT enterprises such as IBM (Raval 2016) and Microsoft (Microsoft 2018) recognized this potential and offer services that contain such generic platforms to develop DApps. Another factor that shows the vast interest and actual development of DL are the increasing Initial Coin Offerings (ICOs). In 2017, startups raised much more money through ICOs than venture capital (Kharpal 2017). But:

- How can DL leverage the business?
- Is it possible to replace existing components in established platforms with DL?
- Can DL be used to create new models of platform intermediation especially for the IoT?

Relation to Existing Theories and Work

In early 2017, the German Ministry for Economic Affairs and Energy (Bundesministerium für Wirtschaft und Energie 2017) released a white paper on digital platforms, which outlined a European way for further implementation of platforms in the manufacturing infrastructure of the European Union. The ministry is convinced that digital platforms will play a significant role in further economic growth and that they will also act as a driver for innovation, productivity and employment. This statement shows a definite need for research in platform technology.

The basis of defining the term DL and its related concepts is developed according to Burkhardt et al. (2018). The current usage of DL is manifold, with ongoing developments in different directions. A structure or framework for DL usage is necessary in order to abstract the diverse uses of DL and thus create interoperability and clarity of its usability.

In order to achieve the named research goals, it is important to close the research gaps. Thus, in this chapter work and theories related to the present discussion are shown in order to fill these gaps.

IoT Platforms: Existing Theories and Work

In order to classify IoT platforms, the term Internet of Things has to be defined. Although it has been around for several years, IoT has no uniform definition. First coined by Kevin Ashton in the context of RFID technology, IoT has become a growing phenomenon (Madakam et al. 2015).

In the context of this chapter, the definition of IoT from the Industrial Internet Consortium (IIC) is being followed. The IIC is one of the leading consortia in the field of industrial internet and IoT, with more than 250 enterprises throughout all sectors and domains. The IIC defines an Industrial-IoT (IIoT) system as a "system that connects and integrates industrial control systems with enterprise systems, business processes and analytics" (Karmarkar et al. 2017). Furthermore, the IIC provides four illustrated viewpoints on an IIoT system within the Industrial Internet Reference Architecture (IIRA) that are used to construct and analyze an IIoT system (Fig. 4.1). It is crucial to consider that the viewpoints have their focus on an ecosystem and not a single company to build such a system.

A digital platform can be classified in several different ways. Meier and Stormer (2012) divided it into five different classifications with different purposes and characteristics.

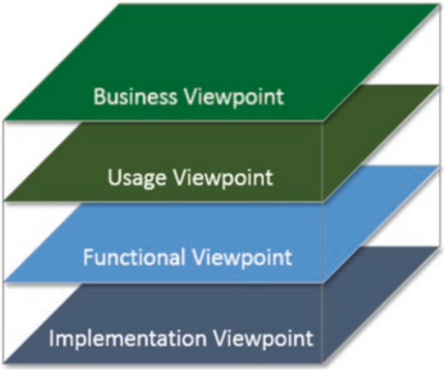


Fig. 4.1 Industrial internet reference architecture viewpoints. (Lin et al. 2017)

- **Agora**: The agora is a marketplace for goods. The characteristics of the agora are market information as well as a negotiation process and dynamic pricing. An example for this would be eBay.com.
- **Aggregator**: An aggregator is a digital supermarket with the purpose of presenting products with a fixed price. An obvious example would be amazon.com.
- **Integrator**: An integrator has the goal to optimize the value chain through targeted supplier selection, process optimization and product integration. Cisco and its services would be an example for an integrator.
- **Alliance**: An alliance is a self-organized, value-added space with the characteristics of innovation, building trust, and the abandonment of hierarchical control. Github.com as a developer community is an example of an alliance.
- **Distributor**: A distributor exchanges information, goods and services. The characteristics are network optimization, unlimited usage and logistical processes. UPS or AT&T and its services would be an example of a distributor.

From the combination of both given terms—IoT and platforms—originates the definition of IoT platforms that will be followed in this chapter. An IoT platform enables the connection of machines and devices, as well as the accumulation and analysis of machine and sensor data with the help of services (Zdravković et al. 2016).

Zdravković et al. (2016) also identify and array different categories of existing IoT platforms. These categories play an important role later in this chapter where comparison with DL comes into play. The categories are:

- **Domain-specific platforms**: These can be found within one domain where they enable domain-specific scenarios.
- **Technology-specific platforms**: These kinds of platforms only take into account one specific device or a set of devices. They are not limited to one sector or domain.
- **Machine to Machine (M2M) platforms**: Providers of M2M platforms have the purpose of offering connectivity as well as data analytics.
- **Generic platforms**: As the name indicates, this is this kind of platform is intended for a wide range of uses and not bound to one domain or set of technologies.

Two state-of-the-art examples of IoT platforms are:

- **Axoom IoT Platform**: A manufacturing-based platform which, for example, enables the connection of machines and sensors and the collection and analysis of data (www.axom-solutions.com).
- **ThingWorx**: A platform in the industrial sector which provides scalability, functionality and flexibility (https://www.ptc.com/en/products/iot/thingworx-platform).

Other examples of platforms were considered, such as by Köhler et al. (2014), Mineraud et al. (2015), Ray (2016), Sruthi and Kavitha (2016) and Zdravković et al. (2016).

Distributed Ledger: Existing Theories and Work

Qtum (2018b) defines technological platforms as possibilities to create and distribute games, tools and applications. As do Zdravković et al. (2016), it further categorizes platforms into those which are specific purpose driven and the more general (Qtum 2018b). Purkayastha (2017) defines Ethereum, Hyperledger, HydraChain, Multichain, Open Chain, IBM Blockchain, Chain and IOTA as platforms that support the prototyping of ideas with specified programming languages (Purkayastha 2017).

Qtum is an example of a DLgp (Qtum 2018b). Another example is Ethereum (Ethereum 2018), which provides the possibility to create DApps on top of its BC and smart contracts supported by the provision of an ERC20 token standard without a specific domain assignment (Braendgaard 2018). Following this, new business logic can be developed and connected up, which establishes potential for business model innovation but also disruption. An example of another DL generic platform is Hyperledger Fabric (Hyperledger 2018). Inter alia, it is used as a basis for the IBM Blockchain Platform (IBM 2018) which is utilized in the 'Car eWallet' solution of the partnership between ZF, UBS and IBM (Clark 2018).

On the other hand, there are DL platform components (DLpc), such as Bitcoin, Ripple, (Streamr 2018) or IOTA, that have been developed for a specific functionality (Beall 2017). Furthermore, projects or DApps like uPort, Aragon, Golem, Gnosis, Oracalize and so forth can be integrated into platforms with a specific scope of usage (Kasireddy 2017; Nagpal 2018).

In order to evaluate and compare BC solutions, Xu et al. (2017) define the four sections: level of decentralization, support for storage and computation, BC configuration and name other design decisions to be made when designing a system using BC. Going through the design process, the taxonomy created will support the analysis of a design option's capabilities and thus help to configure a system with the desired qualitative attributes (Xu et al. 2017). The section's criteria are relevant for a later categorization of DL features.

Criteria like usability, security, scalability, support and documentation, development, limitations and flexibility, currency, consensus and incentive mechanisms are defined by Macdonald, Liu-Thorrold and Julien (2017) to support the selection of existing DLgps. They evaluated the DL platforms Ethereum, IBM Open Blockchain, Intel Sawtooth Lake, Blockstream Sidechain Elements and Erisa. Their work found Ethereum to be the most suitable DLgp currently.

Further DL projects with additional specifications and relevance for this chapter are Nxt because of the use of proof-of-stake consensus algorithm (PoS) (Nxt 2018; Neo 2018) as an alternative to Ethereum and RSK (Lerner 2015). As a sidechain of Bitcoin, RSK enhances its functionality to a DLgp, which also leads to an enhancement of the Bitcoin's and RSK's capabilities.

The fusion of IoT and DL offers many new possibilities for both start-ups and tech companies. Pureswaran and Brody (2014) speak of an "Internet of Decentralized, Autonomous Things" that is created by this fusion. DL will govern the interacting devices that manage their own role and behavior in the described democratization of the digital world. The cooperation of IBM and Samsung created ADEPT, which should serve as a ledger for the billions of transactions generated by the billions of devices on the network (Barker 2015). Further organizations like IOTA (Popov 2017), Chain of Things (Chain of things 2018) or (Filament 2018) have the vision to build DLs suitable for the IoT and enable devices to behave autonomously in a secure and interoperable environment without requiring a central authority.

The developments discussed facilitate an integration of DL vertically as well as horizontally into existing domains and usage areas. Through analysis of related theories and work, we identified a major gap in platform categorization and its usage. Without such a categorization, a comparison on any layer would be akin to comparing "apples and pears". Therefore, definition and demarcation of DL platforms are key for the later development of features for DLgps and DLpcs in order to assess a profound usage of DL. The term 'platform' stands in this chapter for digital online platforms in manufacturing and IoT. According to Burkhardt et al. (2018), the evaluation is conducted on protocol layer with the objective to define general functions on the higher abstraction layer of 'concepts'.

Research Approach

This chapter contains a comparative study of two fairly new and still innovative technological fields. Concerning platforms, the scientific literature is advanced enough to allow a content analysis of their definitions, examples and most importantly their features. Recent and past research fits this approach for the necessary explanation of the focal concept here.

DL is an innovative field, barely discussed so far by the scientific community (Burkhardt et al. 2018). Thus, the scientific literature is not yet sufficient to arrive at a solid definition and to point out its key features for a comparative study. In light of this, an explorative approach with expert interviews based on the qualitative methodology of the social sciences (Atteslander 2010; Diekmann 2017; Kromrey 2006; Schnell et al. 2013) has been necessary. In this evaluation, we defined experts as early adopters of DL who have already collected experiences and hence a certain expertise in their day-to-day-business use of DL. Furthermore, developed DLgps and DLpcs were examined in order to form a deeper evaluation. For the use or implementation of DL in an existing system, a certain expertise and thorough analysis is necessary.

Based on our findings the characteristics of those two innovations were assigned to the four layers of the IIRA by the IIC: Business, Usage, Functional and Implementation. The IIC also defined the key characteristics (Privacy, Security, Safety, Resilience and Reliability) that were of concern in this research. The evaluation is based on a heuristic and not on a theoretical approach, due to lack of the latter in a fast-developing technological field like the industrial internet. This high velocity of development is also the reason why the analysis of characteristics was done without the claim of completeness.

Definitions and Demarcation

Before the evaluation of features and challenges, the terms 'platform', 'meta-platforms', 'marketplace', 'IoT', 'IoT platforms', 'DL' and 'DL platforms' need to be defined in order to set the basis for further discussions.

Digital platforms are mostly known for their use as market space distributors (e.g. Amazon or Alibaba). Therefore, their social and economic guidelines and routines are based on the rules for marketplaces, even going back to the days of the Agora in ancient Greece: sellers are allotted their specific space and sell their goods and services, with a certain fee for this opportunity paid to the marketplace owner. In addition, sellers have to follow the specific conditions of agreement of the market space distributor, the likes of presentation of the market space, shipment of the goods or providing what service. Otherwise, the marketplace owner can sanction the seller or even banish them from the marketplace. The buyers instead simply follow the specific rules of payment (Swedberg 2009).

Besides their distribution of market space and, with it, the bringing together and connecting of buyers and sellers in one place, digital platforms collect data from both user groups: corporate data of the selling companies and private data of the buyers, most importantly with concomitant analysis of purchasing behavior. Using the latter, digital platforms such as Amazon and Alibaba are able to improve their performance in logistics and allocation and their goods and even to anticipate future purchases (Iansiti and Lakhani 2017). With this in mind, we define digital platforms in general according to Zhu and Furr (2016) as an agent that connects two or more groups of users (human or technological) and enables their interaction directly.

Digital platforms can be found throughout all vertical sectors and domains. The advantages of data collection and distribution to different users can also be seen in the manufacturing sector. An open industry platform for IoT can be developed by one or more companies with the purpose of it being used for a product, service or technology. In its creation, it becomes useful for several other companies to complement their own innovations in order to create certain synergy or network effects (Gawer and Cusumano 2014). Zdravković et al. (2016) define an IoT platform "a software that enables connecting machines and devices and then acquisition, processing, transformation, organization and storing machine and sensor data" (Zdravković et al. 2016, p. 2).

In IoT, the convergence of OT and IT is essential to be productive, efficient and successful in business (Kienle 2017). To ensure convergence between both, domain-specific platforms on the OT side are needed, to connect partly to IT. In addition, you need meta-platforms accessing the underlying specific platforms to provide connectivity among different domains and to form horizontal integration. This convergence makes new business models possible. An example for such integration is the

Google Flights Search Engine simulating a meta-platform, whereby the third-party airlines are domain-specific platforms. In the area of such platforms, the traditional architectures exist of a centralized data structure. With the emergence of DL platforms, decentralized data structures are supported.

The main idea behind DL is a decentralized record-keeping of transactions, whereby transactions represents a basic function describing how an organization works. To validate such transactions without any centralized server, a consensus algorithm is necessary. Furthermore, for a permanent, immutable, transparent, anonymous and tamper-free data structure, methods of cryptography are applied.[2] BC as a concept of DL is designed by saving transactions in blocks and concatenating these blocks to a chain using cryptographic means. Protocols such as Ethereum and Bitcoin are built on this concept (Burkhardt et al. 2018).

To support horizontal integration, DLgps can be used. To get a better comprehension and a detailed line of development, DL platforms are divided into two categories. In DLgps all elements of a platform are fulfilled. In the definition of 'generic platforms' in the section entitled "IoT Platforms: Existing Theories and Work", the word 'generic' explains something that is generalized so it is interoperable among various systems or domains. In the IT context, 'generic' can refer to software and hardware as well as to business processes or practices. Generic translates as the ability of something to function without knowing the underlying details of a system that it is working within (Rouse 2018). The more generic the platform is, the broader the scope of use becomes. According to the IIRA, IoT systems can be broken down into functional domains. In contrast to the listed platform characteristics of the section "IoT Platforms: Existing Theories and Work", the functional domains illustrated here describe a complete IoT system from edge to business layer. DLgps cover functional domains such as operation, information and application which take

[2] Further principles, to define the term "Distributed Ledger", are explained in the paper from Burkhardt et al. (2018).

over properties of a platform in an IoT system. All of these domains have certain properties, listed in Fig. 4.2 (Lin et al. 2017). Examples of DLgps fulfilling the functional domains of a generic platform are Qtum, Ethereum and Hyperledger (Karthik 2018; Qtum 2018b). A further analysis of the described mapping is done in the rest of this chapter.

DLpcs implement a single type of property or a combination of properties listed in Fig. 4.2 (Lin et al. 2017). Components exhibit coherent functionalities. Through the enclosure of the implementation, components show a certain independence and thus they can be integrated into third-party technologies. The comprehensive use of components can have a positive impact on the economy as well as on applied development processes (IT Wissen.info 2012). Examples of DLpcs are BigchainDB or uPort. Through the integration of DLpcs, the functionality set of a DLgp or IoT platform can be expanded and thus a broader coverage of functionality is achieved.

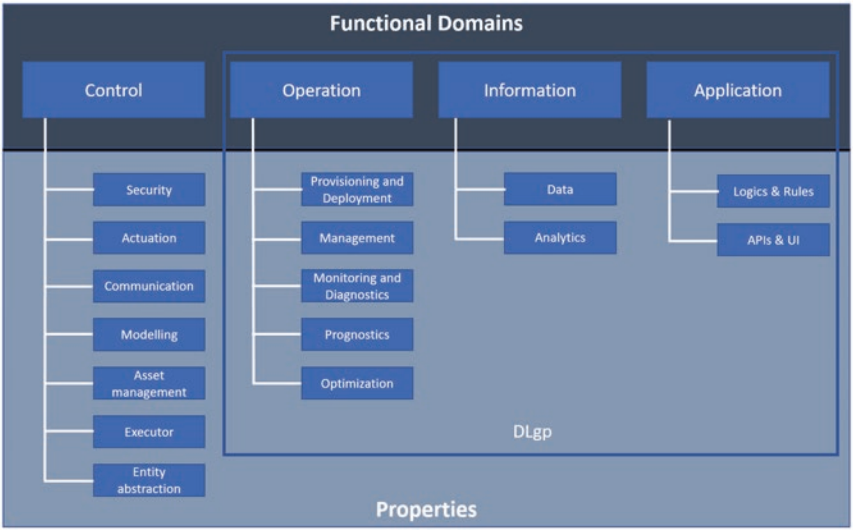


Fig. 4.2 Functional properties of an IoT system. (According to Lin et al. 2017)

Features and Challenges of IOT Platforms

From the existing literature, the following characteristics about IoT platforms are either derived or aggregated to enhance the content of the IIRA. The defined platform features are listed below the viewpoints Business, Usage, Functional and Infrastructure and are visualized in Figs. 4.6, 4.7 and 4.8.

- **Business Layer**: There are several forms of payment that the providers offer (Mazhelis and Tyrvainen 2014; Mineraud et al. 2015). The payment characteristics of platforms are differentiated in service and pricing models:
  - Service Models: One way of payment is through Publish-Subscribe (Mineraud et al. 2015). The allocation of applications is provided as a store (Mazhelis and Tyrvainen 2014; Mineraud et al. 2015) or by the platform providers themselves (Sruthi and Kavitha 2016). For the communication with other platforms interoperability as a service is sometimes a feature (Zdravković et al. 2016). Further mentioned features are the possibility to scale the platform—also as a service (Balamuralidhara et al. 2013; Ray 2016; Zdravković et al. 2016).
  - Pricing Models: Two features here are pay-as-you-go (Mineraud et al. 2015) and billing by inventory costs (Gawer and Cusumano 2014; Zdravković et al. 2016).
- **Usage Layer**: In order to operate devices via a platform, a well-functioning application environment is necessary. This includes a dashboard (Mineraud et al. 2015; Zdravković et al. 2016) or an interface (Sruthi and Kavitha 2016) as well as developer tools (Mineraud et al. 2015; Zdravković et al. 2016)—some of them with a drag-and-drop function (Zdravković et al. 2016). Such options also stimulate further network effects (Gawer and Cusumano 2014). For the usage layer, the product performance data is also of high importance (Zdravković et al. 2016). In the IIRA the analysis of stakeholders

that are involved in the specification of an IoT system are relevant in this layer (Lin et al. 2017).

- **Functional Layer:** As a main feature, communication plays an important role in the scientific literature (Zdravković et al. 2016). Concerning IoT, M2M is in the center of communication (Mineraud et al. 2015; Zdravković et al. 2016). Communication is mostly multi-sided (Mineraud et al. 2015) and as near to real time as possible (Zdravković et al. 2016). So, for its function the data is differentiated in terms of whether it is private or public use (Gawer and Cusumano 2014; Mineraud et al. 2015; Ray 2016). As applications, a general device management is often offered (Balamuralidhara et al. 2013; Dayarathna 2016; Zdravković et al. 2016) but also user management (Balamuralidhara et al. 2013), alerts and triggers, digital copies of devices, remote monitoring and mashups as the integration of new data (Zdravković et al. 2016). The most frequently mentioned functional features are data collection/accumulation (Dayarathna 2016; Mineraud et al. 2015; Ray 2016), data storage (Balamuralidhara et al. 2013; Mineraud et al. 2015; Sruthi and Kavitha 2016), data visualization (Balamuralidhara et al. 2013; Dayarathna 2016; Ray 2016; Sruthi and Kavitha 2016; Zdravković et al. 2016) and data analytics (Balamuralidhara et al. 2013; Dayarathna 2016; Mineraud et al. 2015; Ray 2016; Sruthi and Kavitha 2016; Zdravković et al. 2016). Zdravkovic et al. (2016) add features such as data exchange and streaming from which failure prediction can be derived.
- **Implementation Layer**: Concerning the infrastructure and hosting of IoT platforms, there are several differentiations. A platform can be hosted on a server or in the cloud (Mineraud et al. 2015; Ray 2016; Sruthi and Kavitha 2016) as well as an open or closed platform concerning access (Mineraud et al. 2015)—also referred to as internal or external platforms (Gawer and Cusumano 2014). There can be a support provided by the host (Balamuralidhara et al. 2013; Dayarathna 2016; Mazhelis and Tyrvainen 2014) and an integration in existing frameworks (Balamuralidhara et al. 2013; Sruthi and Kavitha 2016; Zdravković et al. 2016). Some platforms even offer

proprietary messaging (Mineraud et al. 2015) and/or an interconnection of several devices (Mineraud et al. 2015; Ray 2016).

The literature and research on IoT platforms point out a significant number of challenges. There is still no proper standardization in data format and processes (Implementation Layer) (Balamuralidhara et al. 2013; Ray 2016). In this heterogeneous network of platforms (Implementation Layer) (Ray 2016), the interoperability may suffer under certain exclusive ownership over a device (Usage Layer) (Zdravković et al. 2016). Mokhtar and Houshmand (2010) already highlighted this issue in 2010, while Ganzha et al. (2018) are offering a solution to the problem in 2018. Another challenge is the support for contextual data, (Functional Layer) (Dayarathna 2016) or for complex data structures (Functional Layer) and business logics (Business Layer) (Zdravković et al. 2016). In cloud-based systems as well as for the devices in centralized approaches, energy consumption and management are still an issue for platform providers and users (Implementation Layer) (Ray 2016; Zdravković et al. 2016). Platforms also play an important role for the product lifecycle (Menon et al. 2016). Yet, there are still certain issues in the reusability of devices concerning their use in different contexts or applications (Usage Layer) (Zdravković et al. 2016). Furthermore, the handling of millions of sensor data or even out-of-order processing are also an issue (Functional Layer) (Dayarathna 2016; Ray 2016). In addition, Ray (2017) identifies challenges in the middleware following vertical silos (Implementation Layer), unambiguous IoT node identity (Functional Layer) and fault tolerance (Implementation Layer), while Zdravković et al. (2016) points out that the only distinguishing feature IoT platforms have in comparison to other platforms is their M2M connectivity.

As far as it concerns the trustworthiness of the IIC Security Framework (IISF), security is a topic in the description of IoT platforms. (Sruthi and Kavitha 2016; Zdravković et al. 2016). Important issues are the security of information (Dayarathna 2016), secure access (Zdravković et al. 2016) and also protection from other users (Balamuralidhara et al. 2013). Besides security, the listed platform characteristics also support the other categories of trustworthiness, such as private or public data use in the category of privacy and integration framework in reliability.

Features and Challenges of Distributed Ledger Components and Platforms

In this section, the features of DLpcs and DLgps are defined. In the evolution of value creation from platforms to ecosystems, it is recognized that DL can play an important role in enhancing the two steps of evolution. Considering the three-tier architecture of the IIRA's implementation viewpoint, different functional operations of DL are identified (Lin et al. 2017). The three-tier architecture divides an IoT system into three layers. The edge tier comprises the assets surrounding and supporting the user in the physical environment conducting a specific use case. Figure 4.3 visualizes a smart locker use case, including a user's smartphone, a courier truck equipped with different sensors, a box system with smart locks and a package as assets on the edge. The platform tier—as the layer in the middle—gathers data coming from the edge tier, analyzes it and creates actions. Platforms on this tier receive commands from the enterprise tier, process them in order to manage services and functions provided to the assets on the edge tier. On this layer, depending on the use case DLpcs can be integrated to provide functionality to the platform implementation. For example, DL could take over data service, operation or governance services. On the enterprise tier, domain-specific business logic for

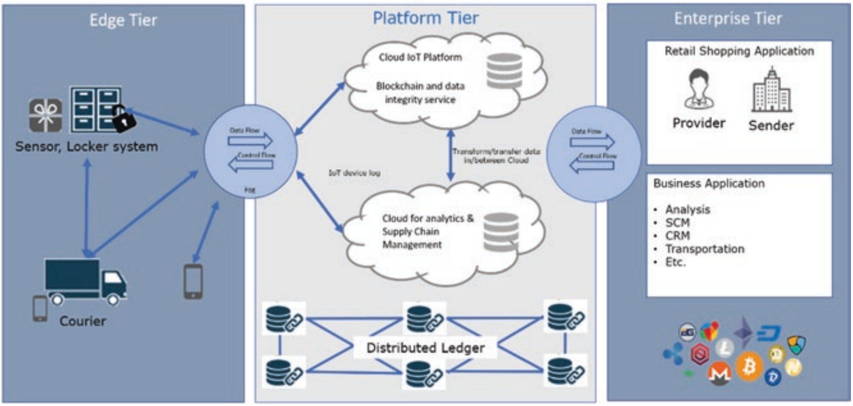


Fig. 4.3 Integration of DL platform component. (According to Lin et al. 2017)

end-users is implemented or operation specialists use platform and edge data. Digital tokens of the DLpc created by the chosen DL protocol can be used as a value counterpart for the usage of services provided on the platform tier. New economic possibilities arise out of this realized connection, increasing the lock-in effect of the business ecosystem.[3]

An example of a DLpc use is Uber creating the ECO token (ECO Foundation 2018) based on a permissioned public DL protocol under the ECO foundation. Thus, Uber enhances the value creation of its exclusive application as well as increasing indirect network effects of the evolving business ecosystem around Uber (Kasireddy 2017). The openness of DL guarantees interoperability of value exchange to other applications within the business ecosystem. This means that it is possible that a user possessing ECO tokens can pay for the services of partners that provide applications based on the ECO protocol (Johnston 2018). In contrast, the access of the user to the applications is still separate, as the applications are based on different technical platforms. Thus, the user needs to create separate accounts for each application.

On the next evolutionary step from platforms to ecosystems, DLgps play a major role. In Fig. 4.4 the assets on the edge tier are autonomously performing activities to realize use cases, that is, paying other assets for the use of services they provide by having their own identity. In the example shown, the box pays the truck for delivery of the package and charges the customer for storing the package. The functionality of the platform tier is divided into service, processing and analytics. The DLgp takes over the processing part and thus the platform management. It realizes the asset's unique identity. Furthermore, smart contracts can be implemented on a DLgp to add this behavior to the assets, enabling them to work autonomously. The analytics functional block implements the intelligence based on the data storage controlled as well through the DLgp. The user interface to the end-user is on the enterprise tier and implemented in DApps that are also based on the DLgp. This guarantees an interoperability between evolving ecosystems with a unified value exchange and

[3] According to Moore (1993), in a business ecosystem companies create capabilities around an innovation by working competitively and cooperatively to develop new solutions around it.

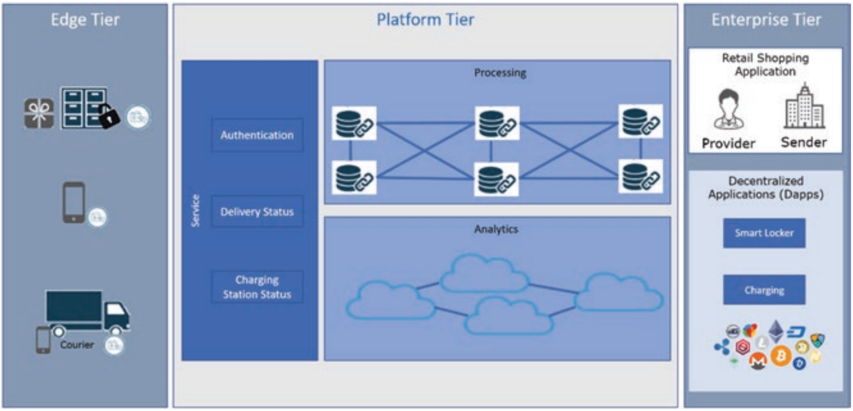


Fig. 4.4 DL generic platform-enabled ecosystem. (According to Lin et al. 2017)

free access enabled through a common DLgp,[4] creating indirect network effects. This will release new options for value creation from centralized platforms to decentralized and open IoT business ecosystems, with the potential to disrupt current business models.[5] The role of the cloud changes from controller to service provider, leading to a democracy of power in the IoT ecosystem (Pureswaran and Brody 2014). With this concept, assumptions are made which build the foundation for the further progress of the chapter:

- current IoT platform will be functionally enhanced by DLpcs to establish new value creation;
- DLgps will enable value creation in IoT business ecosystems with the consequence of disrupting current IoT platforms and solutions, making it more difficult to create lock-in effects.

[4] All DApps run on the same underlying structure, for example using the same virtual machine or language. Thus, no integration of proprietary APIs is needed. Following this, new DApps will create indirect network effects in other existing DApps as they can seamlessly be integrated into each other. Thus, new users of a DApp will increase the value of this DApp and indirectly the value of every other DApp on the DL generic platform Kasireddy (2017).

[5] The development of interoperability between ecosystems is in contrast to long-term subscription relationships that current manufacturers seek Dickson (2016).

Analysis of DL Platform Components and DL Generic Platforms

In this chapter, DLpcs and DLgps based on literature analysis are explained that exemplify the described classification and usage. This forms one part of the feature and challenge derivation of DL by analyzing the characteristics of the identified solutions.

DL Platform Components

Various solutions are relevant in this section, in which DL is used to fulfill a specific purpose. The identified DLpcs can be integrated into existing platforms to fulfill a specific platform function. One functional block of an IoT platform according to the IIRA is 'application' (Lin et al. 2017). DApps provide a service to an end-user to fulfill a specific purpose in its business. uPort, for instance, implements an open identity system based on the DLgp Ethereum; this allows users to save identity information (uport 2018). In the Ethereum ecosystem, a unique identification is thereby realized. Further identified DApps and their provided service are as follows (Aragon 2018; Gnosis Ltd. 2018; Golem 2016; Streamr 2018):

- Aragon: governance
- Golem: computing
- Gnosis: predictions
- Streamr: streaming

A further functional block is 'information' and one component thereof is 'data'. BigchainDB realizes big data storage with BC characteristics, such as decentralized control and immutability (BigchainDB GmbH 2018). Distributed storing of large files and media is enabled by the InterPlanetary File System (IPFS) taking over file system functionality (Protocol Labs 2018). High performance in data processing is a challenge of the IoT in order to, for example, realize M2M communication. IOTA provides a consensus algorithm based on a directed acyclic graph that aims to reach consensus in an IoT environment with a huge amount of data. Thus, it provides the functionality of 'data processing' (IOTA 2018). Bitcoin, as a first-generation BC, is classified as a further DLpc fulfilling the purpose of a 'value storage' of the functional block 'information'. This is due to the deflation of Bitcoin's cryptocurrency by dividing the mining rewards every 210,000 blocks and the currently low scalability (Bitcoinwiki 2018). To provide 'communication' with the edge or Web APIs outside of a DLgp, Oracalize can be used to realize this connection (Oraclize Limited 2018). The last prominent example of a DLpc is Ripple, which provides the functionality of 'Value Transfer' (Ripple 2018). This overview shows the current development of DLpcs to be used as alternatives or extensions to existing platform components.

DL Generic Platforms

Use cases or scenarios are relevant in this section in which DL is employed to fulfill functionalities of a general-purpose platform leading to a horizontal integration of domains. Furthermore, use cases or scenarios are described here that speak of DL without specific implementation details. One example is in Nannra in which it is argued that BC has the potential to provide security against attacks in the scenario of terrorists taking over self-driving cars (Nannra 2018). Additionally, the paper explains that by the interoperability created through the implementation of BC, safer and better critical infrastructure can be built (Nannra 2018).

The six platforms Qtum, Ethereum, Neo, Cardano, EOS and Hadera were identified as DLgps because all are Turing complete and provide the needed functionalities.[6] Next, the main features are explained and put into contrast. Qtum uses Bitcoin Core infrastructure combined with the Ethereum Virtual Machine, which thus provides modularity, stability and interoperability. Furthermore, through smart contracts processes can be automated.[7] Qtum, as well as other DLgp, provides the possibility to create custom tokens which enables the development of self-sufficient

[6] See Burkhardt and Werling for functional details of Ethereum Burkhardt et al. (2018).

[7] A program logic built to conduct virtual contract terms agreed upon by parties and autonomously runs on the DL.

ecosystems, as explained in the example of Uber. By building on the Bitcoin Unspent Transaction Output (UTXO) model, smart contracts can be deployed on lite wallets which can be installed on any mobile device. Thus, Qtum can be used in domains from IoT, supply chain management, telecommunications, social networking and so on—not having a specific domain usage (Qtum 2018a).

Ethereum and Neo contain similarities. Neo's focus is on creating a smart economy featuring digitized physical assets. To reach this goal it combines digital assets, digital identities and smart contract. Furthermore, Neo uses a Delegated Byzantine Fault Tolerant consensus algorithm which leads to a sacrifice in decentralization but improved scalability. With the infrastructure component 'NeoX', it implements cross-chain interoperability to enable cross-chain asset and transaction processing.[8] Another component, 'NeoFS', can be used to store large files over many different nodes with a configurable reliability (Szabo 1997). Ethereum, on the other hand, aims to offer a "trustful object messaging compute framework" (Szabo 1997) as a "transaction-based state machine" (Szabo 1997), providing a generic platform for the development of DApps with customized tokens. One difference to Neo lies in the consensus algorithm used. Ethereum currently uses PoW (proof of work) and it has planned to transfer with the next version to PoS. This difference has implications to scalability and finality of blocks.[9] Another difference lies in the programming language employed. Whereas Ethereum developed its own programming language—Solidity—and is working on further programming languages, called Serpent, LLL, Mutan and Viper, Neo adopts existing programming languages. This has implications for the safety of smart contracts (Fig. 4.5).[10]

Cardano is a DLgp developed by academics and engineers with a scientific philosophy. It consists of the following two layers, which increases flexibility in cases of maintenance and upgrades via soft forks. The

[8] Through cross-chain interoperability the exchange of assets or transactions between private and public Neo blockchains is implemented, Levenson (2017).

[9] An analysis of the implications is not part of this chapter.

[10] Again, an analysis of the implications is not part of this chapter.

Settlement Layer (SL) contains the value ledger after the UTXO model. The same as RSK is for Bitcoin the Computation Layer (CL) is for Cardano. Current developments in both layers include the IELE virtual machine, the Ouroboros PoS (proof of stake) consensus algorithm, programming language adoption of Solidity, the new programming language Plutus, Tartaglia library and integration of hardware security modules and Sealed Glass Proofs (Cardano 2018; Store of Value 2018). Cardano uses the delegated PoS (dPoS) consensus algorithm Ouroboros. Basically, the block producers are selected proportional to the amount of stake they hold or were delegated. The scheduling of the block producers is then done randomly from a source of provable randomness in order to avoid manipulation by block producers (dan on Steemit 2018).

EOS is another DLgp that uses a dPoS. Block producers are here selected through a continuous approval voting system and scheduled using a pseudorandom number created from the block time. EOS enables deterministic parallel execution of applications, which means that the parallel generated schedules are deterministically executed. This leads to different states of accounts in parallel threads,[11] which avoids an immediate execution of messages by scripts. Another benefit of EOS is the independence of bandwidth used by an application on the EOS BC and the current token price. A block producer, on the other hand, will increase bandwidth, computation and storage if the token value rises. Thus, network performance increases with a rising token value. Governance functions, like defective updates to applications or proposed hard forks, are done by elected block producers (EOSIO/Github 2018).

Hedera, the last and newest DLgp, identifies performance, security, governance and stability as challenges for public DLs and goals of the Hedera platform. From performance tests,[12] the Hedera team proved a throughput between less than 10,000 transactions per second (tps) to 500,000 tps and latency of under 11 seconds measured over different

[11] A block is divided into cycles, a cycle consists of threads, each thread contains transactions that contains a set of messages (EOSIO/Github 2018).

[12] Considering the performance of achieving consensus on transaction order and timestamps, not included is the processing of transactions (Baird et al. 2018).

number of computers and geographic distribution.[13] A finality could be reached between 0.75 seconds and 3 seconds, depending on the tradeoffs described. Hedera uses an asynchronous Byzantine Fault Tolerance (aBFT) consensus algorithm called Hashgraph, which secures the platform against, for example, distributed denial of service attacks, only if more than two-thirds of network participants follow the protocol correctly.[14] The Hedera governance is maintained by a council of up to 39 organizations to guarantee the integrity of codebase and prevent DL forking. This leads to a model of permissioned governance and open consensus over the order of transactions.[15] Concepts that are used to guarantee stability of the DL are cryptographic proofs and unique identifiers.[16] Hedera builds up on the internet using TCP/IP for communication. On the Hashgraph Consensus Layer, the gossip protocol and hashgraph consensus algorithm are used to reach consensus over the order of transactions in the network. Cryptocurrency is used to realize incentives and improve security, for example preventing Sybil attacks,[17] of the DL system. The file storage stores information with consensus in Merkle-directed acyclic graphs duplicated over the nodes in a shard.[18]

[13] Transactions are of 100 bytes.

[14] For more information, see Baird (2016) or Burkhardt et al. (2018).

[15] The codebase of Hedera is open for review but not opensource, whereas open innovation on top of the platform is enabled.

[16] Each round a node processes the hashgraph (shared/global state) by receiving all transactions of this round; it digitally signs the hashgraph and gossips it over the network. It collects all gossips from the other nodes and thus can construct a consensus hashgraph which can be used as a verifiable proof. Because the proof is organized as a Merkle tree, a proof can be given in an efficient way to a third party. Furthermore, the proof includes an address book which lists the public keys of all members together with their stake and the address book history that is a sequence of address books signed by members with more than two-thirds of the stake from the previous address book, going back to the genesis address book. In this way it serves as a unique identifier of the DL Baird (2016), Baird et al. (2018). (stake proof).

[17] Hedera uses PoS to weigh a node's vote in the hashgraph virtual voting algorithm. See Baird (2016), Burkhardt et al. (2018). Proxy staking is used to give a person the possibility to transfer its coins to another node using the person's stake. Baird et al. (2018).

[18] Sharding is used to gain performance when a network grows in number of nodes. It splits the nodes into separate shards containing a subset of the state of the entire ledger and communicating over messages. Consensus in a shard is reached by the hashgraph consensus algorithm leading to aBFT of the "multi-shared ledger" Baird et al. (2018).

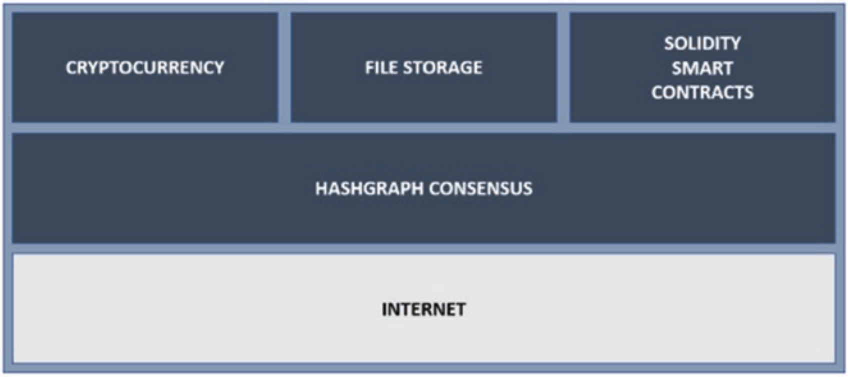


Fig. 4.5 Hedera architecture. (According to Baird et al. 2018)

Any Smart contracts written in Solidity can be deployed on Hedera (Fig. 4.5).[19]

Some challenges that Ethereum works on are privacy, consensus safety, smart contract safety and scalability. It is considered that the other mentioned DLgps face these challenges too and try to tackle them through different approaches. With Ethereum's byzantine hard fork at the end of 2017, support tools, such as zero-knowledge proof and ring signatures, were provided on which solutions to guarantee privacy can be created. The implementation of the PoS consensus algorithm is seen as a safe and efficient in comparison to PoW, which thus enables a greater security of consensus. Formal verifications and Viper (Ethereum/Github 2018a) as well as other activities aim to increase the safety of smart contracts in order to avoid costly bug removal. The last challenge—scalability—can easily be solved by a sacrifice in either safety or decentralization according to the trilemma of Vitalik Buterin (Ethereum/Github 2018a).[20] Further partial solutions of scalability are on second layer, such as interactive verification and state channels. TrueBit (2018) is a solution solely suitable for

[19] Formal proofs are in development to guarantee the stability of smart contracts. Swirlds and Baird (2018).

[20] Blockchain systems can only have at most two of the following features: decentralization, scalability and security Ethereum/Github (2018b).

specific applications and for state channels. Plasma (TrueBit 2018) is a way for improvement but limited to the main chain's ability of handling withdrawals, attacks and so forth. A promising solution of scalability on the base layer of Ethereum is sharding, which splits BC into shards of which each keeps its own state (Buterin Vitalik 2017; Ethereum/Github 2018b). In the current state of development, it is not possible to name a DLgp that is farther ahead in solving these challenges (Konstantopoulos 2018).

Analysis of Conducted Interviews

Between mid-February and the end of March 2018, seven oral interviews with DL experts from different business areas were conducted. Because of the aim to flexibly generate information, a semi-structured form of interview with the support of a questionnaire but the possibility to go deeper into any specific topics arising was held (Atteslander 2010; Diekmann 2013; Kromrey 2006; Schnell et al. 2017). The recorded interviews were analyzed according to a four-phase structure: transcription, individual analysis, general analysis and control (Lamnek and Krell 2010). The questionnaire was structured in two parts. The first part has its focus on general questions to the usage of DL and the second part targets the generation of features according to the viewpoints of business, usage, functional and implementation. In the interviews, the terms DL and BC were used interchangeably because no general definitions exist and the clarification of this was not part of interviews' focus. Thus, in the interview analyses DL also stands for BC.

Persona

The selected interviewees are global experts on infrastructure, protocol (DL), process, service and application layers as well as consultants in the area of DL. All the interviewees act in a business environment where partnerships and establishment of ecosystems are important. The expertise spans from DL development to business including the likes of cryptography, product and project management, business innovation, so that a breadth of knowledge on DL was available.

The Definition of DL

Despite the differences in expertise, the interviewees had a common understanding of DL. The definitions of DL included the following aspects:

- no central server required—an attacker does not know which server to attack because of the distributed network of DL;
- the Byzantine General's Problem is solved with DL;
- data is tamper resistant because it is redundant over the network nodes;
- the use of cryptography provides security;
- transactions get ordered through the DL protocol;
- a transaction is only valid if the total amount of held cryptocurrency stays the same;
- through the use of incentive mechanisms, DL is autonomous;
- a trustless interaction is enabled;
- smart contracts are used to implement the transfer of value.

Usage of DL

Some of the experts consider DL usage as relevant in the implementation of marketplaces or ecosystems, leading to a fusion of domains. Business areas in which a usage of DL is most significant overall at the moment are supply chains, energy, mobility, finance and certification. The IoT is also seen as a relevant field of DL adoption and therefore a further development of DL and IoT is required. One topic of development in the IoT is light and thin clients deployed on the edge assets of which first results are expected during a given year. Trusted chips that integrate cryptography curves are of further relevance. Another business area that was identified is healthcare.

The infrastructure experts argued that on the infrastructure layer, domain independence is preferred. From a development view they create their own roadmap as they hold the expertise, but on the other side close contact with their customers in an agile development mode is also necessary for prioritization. In relation to the state of DL, most of the developments are in PoC or prototype phase; some of them are already in testing and a few in the production phase. Most of the companies use prototyping to get to know the use of DL. This leads to developments of DL use cases in-house copying aspects from public, opensource projects. After involving several departments in the developments to erase silos, it is expected that the solutions will be enhanced to partnerships with other companies and industries. This will lead to new value creation released by DL. All the experts agree that DL usage is important in the formation of partnerships between different stakeholders for which the buildup of trust is effortful and costly. With DL a decentral storage of data, secure communication, trustful connections and digitalization of physical assets are realized. Furthermore, a development of specific DL solutions, like for the IoT, as well as DLgps are examined. Both directions lead to a vertical and horizontal integration of DL.

Functions of DL

DL establishes trust. In the IoT, there are challenges considering updates of devices, decisions to integrate devices in networks and the question of trust toward a device with which you would like to interact. DL realizes the management of devices through many parties, which establishes trust. Additionally, security and cost efficiency were named as further functional attributes by the experts. As DL involves several equal parties into the creation of consensus, the maintenance of the system is more efficient. Furthermore, DL enables the exchange of value in a secure and failure-resistant way, which opens new possibilities. Another expert adds the protection of customer information, process compliance and identity management as further important DL features. All the named functionalities could lead to a simplified creation of partnerships and sharing or selling of data. Thus, the creation of ecosystems is possible without a centralized party, which enables further entities to join in order to create value. This also establishes new opportunities for small businesses, making it easier to join ecosystems for which the creation of trust is not necessary.

Challenges of DL

Due to the state of development there are still challenges that need to be overcome. One major challenge is scalability. According to the experts this will be solved through vertical optimization including new tools, sharding and so on, and horizontal optimization including bridges to further BCs and such like. It is expected that a complex ecosystem with different but compatible DL solutions for specific usage areas will evolve. Another challenge is the discrepancy in speed of processing. If the speed is too high, forking will occur and the data cannot be trusted anymore. Thus, a balance between off-chain and on-chain data storage and processing is important. On the business level, one expert explains that currently it is important to show the customers where DL is not relevant. Before they define the infrastructure implementation it is therefore necessary to create a trust model in which the relevance of DL is evaluated. If a trust problem between the parties is not identified or a strong central player can force participants on its platform, then a DL operation might be possible but not for the entire industry. Furthermore, currently the experts work on increasing the acceptance of DL in their own company. Therefore, the educating of decisionmakers, especially through trainings, is essential. Support of DL solutions is another aspect that is relevant for its productive adoption, which at the moment is only rarely guaranteed by DL implementations. Ultimately, DL has an impact on current business models. This requires new business model methodologies which enable the evaluation of a company's capabilities in an ecosystem and a shift in culture. The generation of revenue decreases in importance in this case, whereas value creation gets more important.

Feature Analysis

For the development of DL features, the IIRA viewpoint model was used. The model shows four viewpoints that support the analysis of IoT systems. In the interviews, the experts assigned DL features to these viewpoints.

The Business Viewpoint

Trust is a high-level feature of DL. With DL, formulation of contracts between parties is not necessary anymore because with cryptographic mechanisms it is now possible to verify the identity of the other party and prevent double spending. This enables the digital transfer of value without a middleman. Thus, DL has an impact on economics, which forces companies to analyze or reshape their existing business models. Data that would have to be gathered centrally is now ubiquitously available in a verified manner, which pushes new business models, products and services, such as telematic insurances. Further barriers in the form of regulations and accounting have to be overcome in order to free the potential of DL. After this, partnerships, even with the customer, can be formed 'on the fly', which creates transparency of end-to-end processes and the formation of ecosystems without high interface development efforts. This will also lead to an improvement in operational speed and more efficiency in business processes. New incentives and mechanisms are created to invest in upcoming opportunities enabled through smart contracts, which is based on economic and game theoretical systems.

The Usage Viewpoint

With DL the user drifts into an active part of value generation by participating in the network. Currently, because of technical restrictions the user has to use central servers in order to participate in the network. With an improvement of technical possibilities, the user will shift further to being a direct network participant. The experts think that most users will not take up this role, which creates the need for new roles overseeing the user's tasks. A new economic niche is thus generated by this circumstance. Furthermore, the user can use innovations without losing privacy. Results based on data can be trusted without possessing the data itself. This enables the possibility to use an application without the need to trust the provider. As the user holds his or her own data (private key) the misuse of data by the provider or third parties is not possible. For some use cases, the data transparency can be also an obstacle that needs to be considered.

The Functional Viewpoint

Companies with a vertical integration focus on the development of specialized DL applications, whereas companies with a horizontal integration focus on the improvement of the DL usage. The first type of company is closer in terms of interaction with the end-user. Both types leverage each other by exchanging knowledge and developing compatibility. An integrative approach between the developments will lead to a higher stability and network effects for the whole ecosystem. For example, an asset's identity stays unique in different applications of the ecosystem or decisions that are made in a private BC can be transferred to a public BC, so realizing voting mechanisms. Additionally, another expert envisions the protection of customer data with DL as a further functional use. Thus, new models emerge that liberate the potential of DL. A current, general problem seen by the experts is missing standards for data, processes, protocols and so on, which do not exist in a domain or even an industry. According to their opinion, DL will not solve the problem of missing standards because some companies profit too much from their established standard. But in order to leverage the fusion of IoT and DL, this is a further challenge for both directions to be overcome.

The Implementation Viewpoint

Because of the interrelated developments of the two types of companies discussed, technical challenges need to be solved on both sides to improve developments. For example, scalability issues need to be solved by horizontal integration companies in order to enable vertical innovation. Due to the global reach of DL, a higher speed in developments can be achieved. Usually, the infrastructure has to be built before application development. With DL and opensource communities the infrastructure already exists. Furthermore, it became attractive for developers as the DL user base and link to business is available, which forces innovation. Additionally, for developers DL is seen to be appealing because opensource enables them to be more independent but also gives the opportunity to freely participate in impactful projects with other experienced developers. However, the form of developing has changed as concepts like trial and error are currently costly in the DL space. Developers have to make sure that their smart contract is bug free before deployment. This led to DLgps, such as Cardano, that have implemented programming languages with formal verifications, with the flipside that these languages are complicated and require specialists. Testing frameworks, such as Truffle, are also evolving that increase smart contract safety. Moreover, smart contracts need to be developed with a distributed execution in mind which forces the developer to consider dependencies in the code. The challenge for companies is to define a balance between smart contract safety, broad developer adoption and degree of integration of opensource. A high potential, especially for traditional industry companies, is discovered by the experts if DL is used to share data that is still captured in the systems of the companies. An openness to evolving communities is therefore required.

Results of Features and Challenges Evaluation

The results of the evaluation are shown in Figs. 4.6, 4.7 and 4.8.[21] The information gathered in the DL platform analysis and interviews was consolidated and transferred into the structure illustrated. It is divided into four sections that visualize the viewpoints of the IIRA. The summarized challenges of DL are listed in the upper part of each section and the features are shown on the lower part. For instance, from a business and usage viewpoint privacy and transparency need to be balanced depending on the use case, which led to the listing of 'privacy' and 'transparency' as challenges. The creation of use cases and transfer to business cases also includes the challenge of 'identification of usage' and 'impact on business model, business processes and culture' from a business perspective. A key challenge on the functional viewpoint is the 'dependencies of horizontal and vertical developments'. For example, current challenges on the implementation viewpoint, like 'scalability', need to be solved for DLgp in

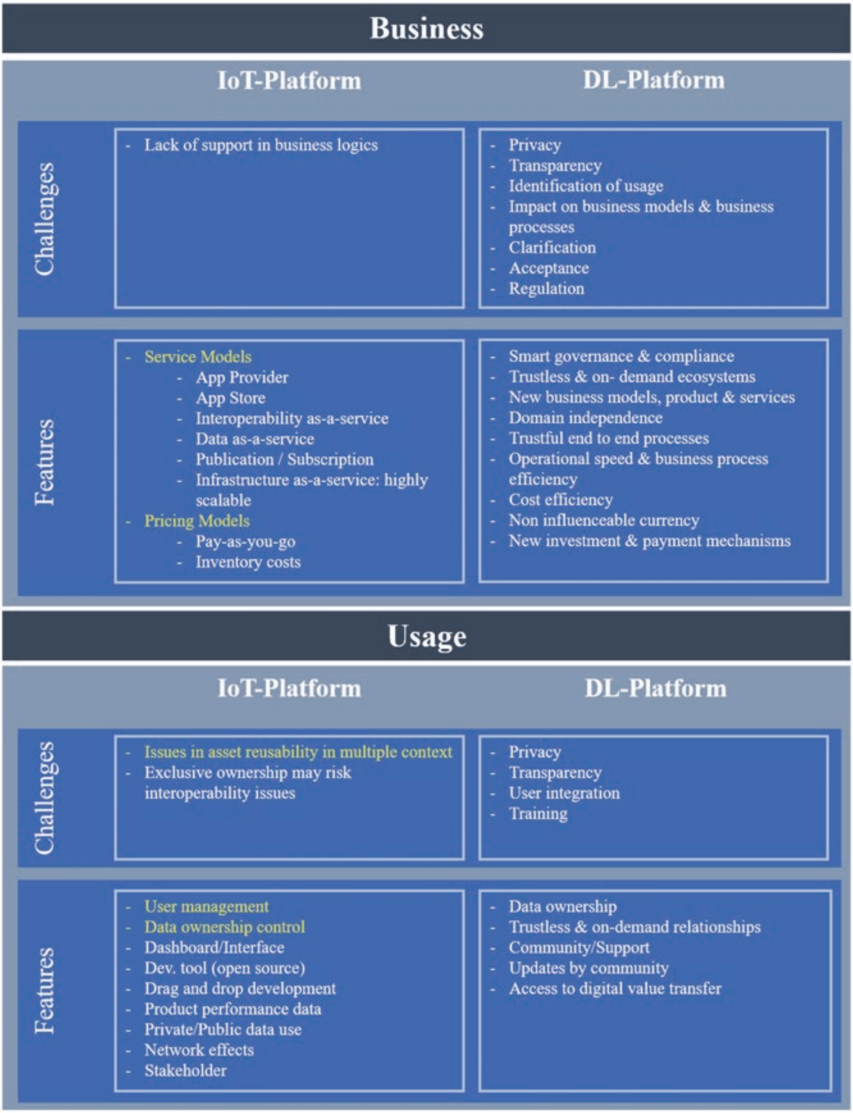
[21] Only key DL points from the Figs. 4.6, 4.7 and 4.8 are explained. For a detailed explanation of the features and challenges, please refer to the sections "Analysis of DL Platform Components and DL Generic Platforms" and "Analysis of Conducted Interviews".

order to run DLpcs and applications according to the defined conditions. Forks lead to partitions of DL protocols due to functional changes and different beliefs apropos the change necessity in the corresponding community. It requires an ecosystem of interrelated solutions, solving the functional and implementation challenges with a view on business and usage.

From a business viewpoint DL enables the features shown. 'Smart governance & compliance' is realized by 'smart contracts & DApps' on the implementation viewpoints. Furthermore, due to the characteristics of DLgps ecosystems, which can be built but do not require trust between the participants, no trust creation phase is necessary, which inclines to an 'on-demand' ecosystem creation. Additionally, because of the features of 'opensource', 'global reach', 'compatibility', 'existing and open infrastructure' and 'failure resistance' on the implementation viewpoint, 'operational speed' and 'cost efficiency' in the business viewpoint can be achieved. The user receives direct ownership over his or her own data. DL network participants decide themselves who accesses their data, which generates a 'transparent data ownership' in the functional viewpoint. Furthermore, any person with an internet connection gets the possibility to transfer value over the DL network, creating new possibilities in the business and usage viewpoint. In the functional viewpoint, a 'unique identity' can be realized because on a DLgp ('Common control layer') an identity of an asset or a person needs to be created once and can be used throughout the ecosystem. Due to the fact that data is validated by the respective consensus algorithm in a p2p network and data is owned by its creator, it concludes the information to be valid. This creates 'trusted applications' and new possibilities in the business viewpoint. To summarize, all the DL features from the various viewpoints form the foundations to foster 'privacy', 'security' and 'reliability' in order to enable 'trust' of a whole system.

Feature Mapping

In Figs. 4.6, 4.7 and 4.8, challenges and features of IoT platforms and DL according to the analysis of this chapter are arranged opposite each other. The yellow marking on IoT side indicate where a link can be formed to DL.



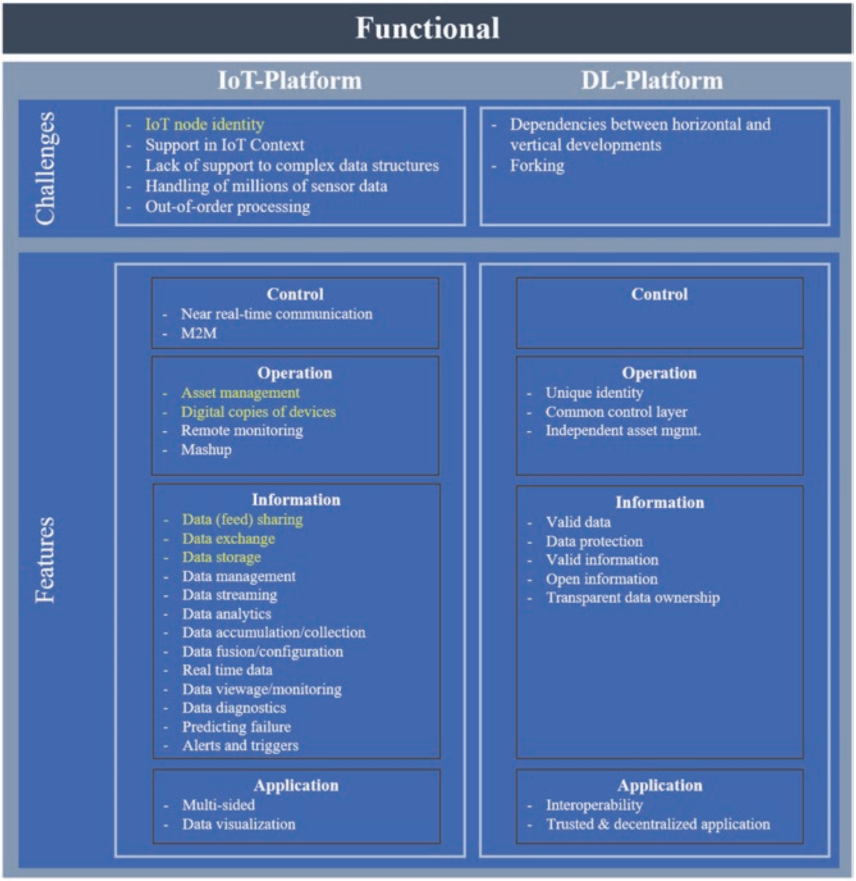
Business

	IoT-Platform	DL-Platform
Challenges	- Lack of support in business logics	- Privacy - Transparency - Identification of usage - Impact on business models & business processes - Clarification - Acceptance - Regulation
Features	- Service Models - App Provider - App Store - Interoperability as-a-service - Data as-a-service - Publication / Subscription - Infrastructure as-a-service: highly scalable - Pricing Models - Pay-as-you-go - Inventory costs	- Smart governance & compliance - Trustless & on- demand ecosystems - New business models, product & services - Domain independence - Trustful end to end processes - Operational speed & business process efficiency - Cost efficiency - Non influenceable currency - New investment & payment mechanisms

Usage

	IoT-Platform	DL-Platform
Challenges	- Issues in asset reusability in multiple context - Exclusive ownership may risk interoperability issues	- Privacy - Transparency - User integration - Training
Features	- User management - Data ownership control - Dashboard/Interface - Dev. tool (open source) - Drag and drop development - Product performance data - Private/Public data use - Network effects - Stakeholder	- Data ownership - Trustless & on-demand relationships - Community/Support - Updates by community - Access to digital value transfer

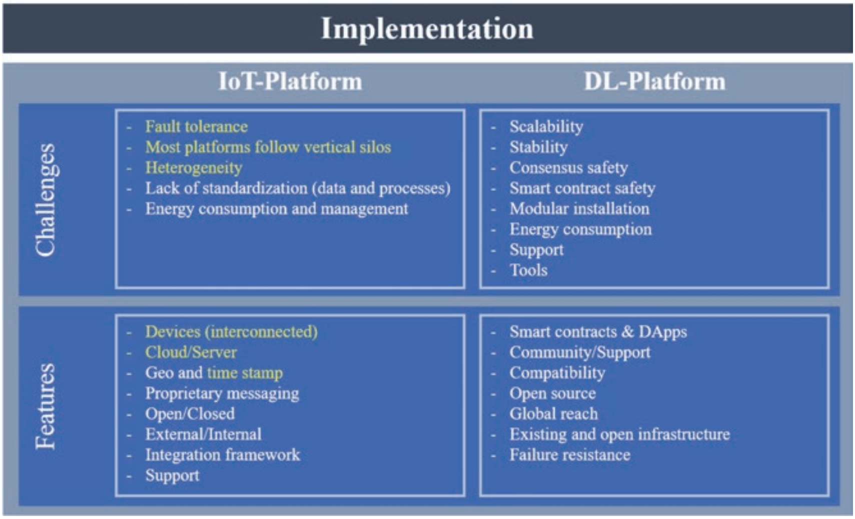
Fig. 4.6 Feature mapping IoT platforms and DL; business and usage viewpoint. (According to the IIRA business viewpoint Lin et al. 2017)



Functional	IoT-Platform	DL-Platform
Challenges	- IoT node identity - Support in IoT Context - Lack of support to complex data structures - Handling of millions of sensor data - Out-of-order processing	- Dependencies between horizontal and vertical developments - Forking
Features	**Control** - Near real-time communication - M2M	**Control**
	Operation - Asset management - Digital copies of devices - Remote monitoring - Mashup	**Operation** - Unique identity - Common control layer - Independent asset mgmt.
	Information - Data (feed) sharing - Data exchange - Data storage - Data management - Data streaming - Data analytics - Data accumulation/collection - Data fusion/configuration - Real time data - Data viewage/monitoring - Data diagnostics - Predicting failure - Alerts and triggers	**Information** - Valid data - Data protection - Valid information - Open information - Transparent data ownership
	Application - Multi-sided - Data visualization	**Application** - Interoperability - Trusted & decentralized application

Fig. 4.7 Feature mapping IoT platforms and DL; functional viewpoint. (According to the IIRA functional viewpoints Lin et al. 2017)

In the business viewpoint, DL will enable new 'service models' in addition to service subscription with an on-demand characteristic. Furthermore, through 'non-influenceable currency' and 'new investment and payment mechanisms', new 'pricing models' can be integrated which enable direct payments on the edge tier. With the implementation of DLgps and the integration of DLpcs into IoT systems, a reuse of assets in different contexts will be guaranteed as a horizontal integration facilitates



Implementation

	IoT-Platform	DL-Platform
Challenges	- Fault tolerance - Most platforms follow vertical silos - Heterogeneity - Lack of standardization (data and processes) - Energy consumption and management	- Scalability - Stability - Consensus safety - Smart contract safety - Modular installation - Energy consumption - Support - Tools
Features	- Devices (interconnected) - Cloud/Server - Geo and time stamp - Proprietary messaging - Open/Closed - External/Internal - Integration framework - Support	- Smart contracts & DApps - Community/Support - Compatibility - Open source - Global reach - Existing and open infrastructure - Failure resistance

Fig. 4.8 Feature mapping IoT platforms and DL; implementation viewpoint. (According to the IIRA implementation viewpoints Lin et al. 2017)

domain and context independence. Additionally, users of an IoT system receive a unique identity independent of context or application throughout the IoT ecosystem by the implementation of a DLgp as the ecosystem foundation. This also guarantees an independent ‘IoT node identity’, ‘user management’ and ‘asset management’. Furthermore, DL enables a valid data layer of an IoT system, which provides ‘data ownership control’, ‘data exchange’ and ‘data sharing’. The described connections support the development of valid ‘digital copies of devices’ and communication between devices on platform tier—‘devices (interconnected)’. Nannra (2018) advocates this link, saying that DL can support a secure communication between assets on the edge tier (Nannra 2018). IoT platform features described, such as ‘data storage’ and ‘cloud/server’, can be replaced by DLpcs. Because DL and IoT platforms comprise features that enable assets to act autonomously on the edge tier, M2M communication and value transfer is realized. Challenges on the implementation viewpoint, like ‘heterogeneity’, ‘fault tolerance’ and ‘vertical silos alignment’ can be tackled with the implementation of DLgps and DLpcs guaranteeing ‘interoperability’, ‘compatibility’ and ‘failure resistance’ in the functional and implementation viewpoint. DL guarantees a synchronized global state of the network which enables valid statements on the sequence of transactions—'timestamp'.

Conclusion

Trust, overarching an IoT system, can be enabled by emphasizing privacy, security, reliability, safety and resilience in all four viewpoints. Figure 4.9 indicates that the integration of DLpcs and DLgp facilitate the generation of 'privacy', 'security' and 'reliability' of an IoT system by establishing trustworthiness between the IoT stakeholders.

In this chapter, the analysis of IoT platforms and DL as a platform component and generic platform is conducted and the results are combined in feature mapping. The illustration supports the identification of IoT features and challenges that can be enhanced or replaced by DL's features in order to build a more trustful IoT system. This includes the prevention of data misuse, enabling of secure interconnectivity and interoperability as well as guaranteeing the promised behavior of the IoT system by implementing a decentralized control function. Additionally, challenges that have to be solved on the DL side can be identified. Moreover, it shows where DL does not provide functionalities in order to justify a more in-depth use of DL in the IoT. Thus, it is concluded that DL is the required pillar to enable democracy of power in the IoT. With DL, assets can build trustful relationships to create new value.

The DL challenges listed need to be solved to achieve the described scenario. It is further necessary to examine more DL and IoT solutions, conduct interviews and implement use cases to identify additional challenges and features in order to guarantee the completeness of the mapping visualization. This will be supported by a more detailed classification

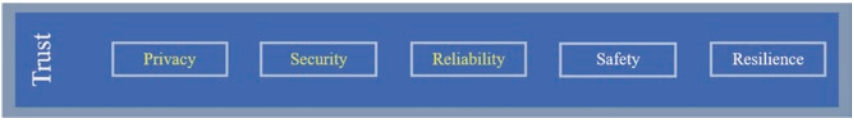


Fig. 4.9 Feature mapping IoT platforms and DL enabling trust

of DL and IoT platform types as well as its integration into the graphic structure. Through this detailing, an improved evaluation of the usage of DL in the IoT can be achieved. Furthermore, the use of DL in combination with other technological fields, such as artificial intelligence, is necessary to construct a substantial DL framework that supports its adoption and integration in the IoT.

References

Aragon. (2018). *Unstoppable Organizations*. Retrieved from https://aragon.one/

Atteslander, P. (2010). *Methoden der empirischen Sozialforschung* (13th ed.). Berlin: Erich Schmidt Verlag.

Baird, L. (2016). The SWIRLDS Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance: SWIRLDS Tech Report SWIRLDS-TR-2016-01. Retrieved from https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

Baird, L., Harmon, M., & Madsen, P. (2018). *Hedera: A Governing Council & Public Hashgraph Network: The Trust Layer of the Internet*. Hedera Hashgraph, LLC.

Balamuralidhara, P., Misra, P., & Pal, A. (2013). Software Platforms for Internet of Things and M2M. *Journal of the Indian Institute of Science, 93*(3), 487–498.

Barker, C. (2015). *Is Blockchain the Key to the Internet of Things? IBM and Samsung Think It Might Just Be*. Retrieved from http://www.zdnet.com/article/is-blockchain-the-key-to-the-internet-of-things-ibm-and-samsung-think-it-might-just-be/

Beall, G. (2017). *5 Blockchain Platforms to Keep Your Eye On In 2018*. Retrieved from https://www.business2community.com/finance/5-blockchain-platforms-keep-eye-2018-01979716

BigchainDB GmbH. (2018). *BigChainDB – Features*. Retrieved from https://www.bigchaindb.com/features/

Bitcoinwiki. (2018). *How Bitcoin Works*. Retrieved from https://en.bitcoin.it/wiki/How_bitcoin_works#See_also

Braendgaard, P. (2018). *A Personal Look at the Early Days of Internet vs Blockchain Today*. Retrieved from https://medium.com/@pelleb/personal-look-at-the-early-days-of-internet-vs-blockchain-today-590a98cb009f

Brakeville, S., & Perepa, B. (2018). *Blockchain Basics: Introduction to Distributed Ledgers: Get to Know This Game-Changing Technology and How to Start Using*

It. Retrieved from https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html

Bundesministerium für Wirtschaft und Energie (BMWi). (2017). *Weißbuch Digitale Plattformen: Digitale Ordnungspolitik für Wachstum, Innovation, Wettbewerb und Teilhabe*. BMWi: Berlin.

Burgwinkel, D. (Ed.). (2016). *Blockchain Technology: Einführung für Business- und IT Manager*. Berlin/Boston: De Gruyter Oldenbourg. Retrieved from http://www.degruyter.com/search?f_0=isbnissn&q_0=9783110487312&searchTitles=true

Burkhardt, D., Werling, M., & Lasi, H. (2018). Distributed Ledger: Definition & Demarcation. *IEEE Conference. Submitted at the IEEE Conference 2018*.

Buterin, V. (2017, November). *Vitalik Buterin: Ethereum 2.0 is EOS*. BeyondBlock, Taipei. Retrieved from https://www.reddit.com/r/eos/comments/7fnnxi/vitalik_buterin_ethereum_20_is_eos/

Cardano. (2018). *Why We Are Building Cardano*. Retrieved from https://whycardano.com/

Chain of Things. (2018). *Advancing Innovation in Blockchain & IoT*. Retrieved from https://www.chainofthings.com/

Channel4. (2018). *Revealed: Trump's Election Consultants Filmed Saying They Use Bribes and Sex Workers to Entrap Politicians*. Retrieved from https://www.channel4.com/news/cambridge-analytica-revealed-trumps-election-consultants-filmed-saying-they-use-bribes-and-sex-workers-to-entrap-politicians-investigation

Clark, J. (2018). *ZF, UBS and IBM Bring Blockchain to In-Vehicle Payments*. Retrieved from https://www.ibm.com/blogs/internet-of-things/zf-ubs-ibm-vehicle-payments/

dan on steemit. (2018). *Peer Review of Cardano's Ouroboros*. Retrieved from https://steemit.com/cardamon/@dan/peer-review-of-cardano-s-ouroboros

Dayarathna, M. (2016). Comparing 11 IoT Development Platforms. *DZone-IoT Zone*.

Dickson, B. (2016). *Decentralizing IoT Networks Through Blockchain*. Retrieved from https://techcrunch.com/2016/06/28/decentralizing-iot-networks-throughblockchain/?guccounter=1

Diekmann, A. (2017). *Empirische Sozialforschung: Grundlagen, Methoden, Anwendungen* (11th ed.). Hamburg: Rowohlt Taschenbuch Verlag.

ECO Foundation. (2018). *ECO: A Global Currency Protocol*. Retrieved from https://eco.com/eco-design-proposal-v1.pdf

EOSIO/Github. (2018). *EOS.IO Technical White Paper v2*. Retrieved from https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

Ethereum. (2018). *Ethereum: Blockchain App Platform*. Retrieved from https://www.ethereum.org/

Ethereum/Github. (2018a). *Principles and Goals*. Retrieved from https://github.com/ethereum/vyper

Ethereum/Github. (2018b). *Sharding FAQ: On Sharding Blockchains*. Retrieved from https://github.com/ethereum/wiki/wiki/Sharding-FAQ

Filament. (2018). *Filament v3.0: Thing Nirvana*. Advance Online Publication. https://doi.org/10.1787/651864166021

Ganzha, M., Paprzycki, M., Pawłowski, W., Szmeja, P., & Wasielewska, K. (2018). Towards Semantic Interoperability Between Internet of Things Platforms. In R. Gravina, C. E. Palau, M. Manso, A. Liotta, & G. Fortino (Eds.), *Internet of Things. Integration, Interconnection, and Interoperability of IoT Systems* (Vol. 42, pp. 103–127). Cham: Springer International Publishing https://doi.org/10.1007/978-3-319-61300-0_6.

Gawer, A., & Cusumano, M. A. (2014). Industry Platforms and Ecosystem Innovation. *Journal of Product Innovation Management, 31*(3), 417–433 https://doi.org/10.1111/jpim.12105.

Gnosis Ltd. (2018). *Meet the Future*. Retrieved from https://gnosis.pm/

Golem. (2016). *The Golem Project: Crowdfunding Whitepaper*. Retrieved from https://golem.network/doc/Golemwhitepaper.pdf

Hyperledger. *About Hyperledger*. Retrieved from https://www.hyperledger.org/about

Hyperledger. (2018). *Hyperledger: Fabric*. Retrieved from https://www.hyperledger.org/projects/fabric

Iansiti, M., & Lakhani, K. R. (2017). Managing Our Hub Economy. *Harvard Business Review, 95*(5), 84–92.

IBM. (2018). *IBM Blockchain Platform*. Retrieved from https://www.ibm.com/blockchain/platform/

IOTA. (2018). *The Backbone of IoT Is Here*. Retrieved from https://iota.org/

IT Wissen.info. (2012). *Komponentenmodell*. Retrieved from https://www.itwissen.info/Komponentenmodell-component-model.html

Johnston, A. (2018). *Uber Co-founder Launch New Global Cryptocurrency*. Retrieved from https://www.icoexaminer.com/ico-news/uber-co-founder-launch-new-global-cryptocurrency-airdrop-half/

Karmarkar, A., Hirsch, F., Simmon, E., Bournival, E., Buchheit, M., Joshi, R., et al. (2017). *The Industrial Internet of Things Volume G8: Vocabulary: IIC:PUB:G8:V2.00:PB:20170719.*

Karthik, K. (2018). *5 Advantages of Using Hyperledger Fabric for Your Enterprise Blockchain*. Retrieved from https://www.skcript.com/svr/5-advantages-of-using-hyperledger-fabric-for-your-enterprise-blockchain/

Kasireddy, P. (2017). *The Synergies Gained from Building on Ethereum's Decentralized App Ecosystem*. Retrieved from https://medium.com/swlh/the-synergies-gained-from-building-on-ethereums-decentralized-app-ecosystem-22a709a675d2

Kharpal, A. (2017). *Initial Coin Offerings Have Raised $1.2 Billion and Now Surpass Early Stage VC Funding*. Retrieved from https://www.cnbc.com/2017/08/09/initial-coin-offerings-surpass-early-stage-venture-capital-funding.html

Kienle, M. (2017). *Operational IT*. Retrieved from https://www.computerwoche.de/a/operational-it,3329464

Köhler, M., Wörner, D., & Wortmann, F. (2014). Platforms for the Internet of Things-an Analysis of Existing Solutions. In *5th Bosch Conference on Systems and Software Engineering (BoCSE).*

Konstantopoulos, G. (2018). *Scalability Tradeoffs: Why "The Ethereum Killer" Hasn't Arrived Yet*. Retrieved from https://medium.com/loom-network/scalability-tradeoffs-why-the-ethereum-killer-hasnt-arrived-yet-8f60a88e46c0

Kromrey, H. (2006). *Empirische Sozialforschung: Modelle und Methoden der standardisierten Datenerhebung und Datenauswertung* (11., überarb. Aufl., UTB für Wissenschaft Uni-Taschenbücher Soziologie: Vol. 1040). Stuttgart: Lucius & Lucius. Retrieved from http://www.socialnet.de/rezensionen/isbn.php?isbn=978-3-8252-1040-3

Lamnek, S., & Krell, C. (2010). *Qualitative Sozialforschung: Lehrbuch; [Online-Materialien]* (5., überarb. Aufl., Grundlagen Psychologie). Weinheim: Beltz. Retrieved from http://www.content-select.com/index.php?id=bib_view&ean=9783621278409

Lerner, S. D. (2015). RSK Rootstock Platform – Bitcoin Powered Smart Contracts: Whitepaper. Retrieved from https://bravenewcoin.com/assets/Whitepapers/RootstockWhitePaperv9-Overview.pdf

Leukert, B. (2016). *Blockchain: Vom Bitcoin zum Geschäftsmodell*. Retrieved from https://news.sap.com/germany/blockchain-revolution/

Levenson, N. (2017). *NEO Versus Ethereum: Why NEO Might Be 2018s Strongest Cryptocurrency*. Retrieved from https://hackernoon.com/neo-versus-ethereum-why-neo-might-be-2018s-strongest-cryptocurrency-79956138bea3

Lin, S.-W., Bradford, M., Durand, J., Bleakley, G., Chigani, A., Martin, R., et al. (2017). *The Industrial Internet of Things Volume G1: Reference Architecture*. IIC:PUB:G1:V1.80:20170131.

Macdonald, M., Liu-Thorrold, L., & Julien, R. (2017). *The Blockchain: A Comparison of Platforms and Their Uses Beyond Bitcoin*. The University of Queensland. https://doi.org/10.13140/RG.2.2.23274.52164

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications, 3*(5), 164.

Mazhelis, O., & Tyrvainen, P. (2014, March). A Framework for Evaluating Internet-of-Things Platforms: Application Provider Viewpoint. In *2014 IEEE World Forum on Internet of Things (WF-IoT)* (pp. 147–152). IEEE. https://doi.org/10.1109/WF-IoT.2014.6803137.

Meier, A., & Stormer, H. (2012). *eBusiness & eCommerce*. Berlin: Springer Berlin Heidelberg.

Menon, K., Kärkkäinen, H., & Gupta, J. P. (2016). Role of Industrial Internet Platforms in the Management of Product Lifecycle Related Information and Knowledge. In *IFIP International Conference on Product Lifecycle Management* (pp. 549–558). Cham: Springer.

Microsoft. (2018). *Single Member Consortium (Deprecated): Hyperledger Fabric on Azure*. Retrieved from https://azuremarketplace.microsoft.com/en-us/marketplace/apps/microsoft-azure-blockchain.azure-blockchain-service?tab=Overview

Mineraud, J., Mazhelis, O., Su, X., & Tarkoma, S. (2015). Contemporary Internet of Things Platforms. *ArXiv Preprint ArXiv:1501.07438*.

Mokhtar, A., & Houshmand, M. (2010). Introducing a Roadmap to Implement the Universal Manufacturing Platform Using Axiomatic Design Theory. *International Journal of Manufacturing Research, 5*(2), 252–269.

Moore, J. F. (1993). Predators and Prey: A New Ecology of Competition. *Harvard Business Review, 71*(3), 75–86.

Nagpal, R. (2018). *17 Blockchain Platforms – A Brief Introduction*. Retrieved from https://medium.com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b

Nannra, A. (2018). *Blockchain and a Safer Self-Driving Future*. Retrieved from https://blogs.cisco.com/innovation/blockchain-and-a-safer-self-driving-future

Neo. (2018). *Neo White Paper*. Retrieved from http://docs.neo.org/en-us/

Nxt. (2018). *Whitepaper:Nxt*. Retrieved from http://nxtwiki.org/wiki/Whitepaper:Nxt#Device_Portability

Oraclize Limited. (2018). *How It Works*. Retrieved from http://www.oraclize.it/

Popov, S. (2017). *The Tangle*. Retrieved from https://iota.org/IOTA_Whitepaper.pdf

Protocol Labs. (2018). *IPFS Is the Distributed Web*. Retrieved from https://ipfs.io/#how

Pureswaran, V., & Brody, P. (2014). Device Democracy: Saving the Future of the Internet of Things. *IBM Institute for Business Value*.

Purkayastha, S. (2017). *Have an Idea Around Blockchain? Here Are Eight Blockchain Platforms That You Can Choose from*. Retrieved from http://radiostud.io/eight-blockchain-platforms-comparison/

Qtum. (2018a). *Creating a Self Aware Blockchain*. Retrieved from https://briandcolwell.com/2017/08/qtum-creating-a-self-aware-blockchain/.html

Qtum. (2018b). *What's the Difference Between A Blockchain Currency and Platform*. Retrieved from https://blog.qtum.org/whats-the-difference-between-a-blockchain-currency-and-platform-dbd6a3d5a1c6

Raval, S. (2016). *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology* (1st ed.). Beijing/Boston/Farnham/Sebastopol/Tokyo: O'Reilly.

Ray, P. P. (2016). A Survey of IoT Cloud Platforms. *Future Computing and Informatics Journal, 1*(1–2), 35–46 https://doi.org/10.1016/j.fcij.2017.02.001.

Ripple. (2018). *Join RippleNet*. Retrieved from https://ripple.com/

Rouse, M. (2018). *agnostic*. Retrieved from http://whatis.techtarget.com/definition/agnostic

Schnell, R., Hill, P. B., & Esser, E. (2013). *Methoden der empirischen Sozialforschung* (10th ed.). München: Oldenbourg Verlag.

Sruthi, M., & Kavitha, B. R. (2016). A Survey on IoT Platform. *International Journal of Scientific Research and Modern Education (IJSRME), 1*(1), 468–473.

Store of Value. (2018). *Cardano*. Retrieved from http://storeofvalueblog.com/posts/a-deep-dive-into-cardano/

Streamr. (2018). *Unaufhaltsame Daten für Unaufhaltsame Apps*. Retrieved from https://www.streamr.com/

Swedberg, R. (2009). *Principles of Economic Sociology*. Princeton: Princeton University Press.

Swirlds, & Baird, L. (2018, March). *Hedera Hashgraph Live Event – 500.000 Transactions/Second.* Retrieved from https://www.youtube.com/watch?v=tNVmXTrEqCk

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*. (Volume 2). Retrieved from http://ojphi.org/ojs/index.php/fm/article/view/548/469

Tapscott, D. (2016). *How Blockchains Could Change the World*. Retrieved from https://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world

TrueBit. (2018). *TrueBit: Secure, Scalable, Decentralized Computation*. Retrieved from https://truebit.io/

uport. (2018). *Open Identity System for the Decentralized Web*. Retrieved from https://www.uport.me/

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., et al. (2017). *A Taxonomy of Blockchain-Based Systems for Architecture Design*. School of Computer Science and Engineering, UNSW, Sydney, Carnegie Mellon University, Pittsburgh, USI Lugano, Chalmers University of Technology, Gothenburg.

Zdravković, M., Trajanović, M., Sarraipa, J., Jardim-Gonçalves, R., Lezoche, M., Aubry, A., & Panetto, H. (2016). Survey of Internet-of-Things Platforms. In *6th International Conference on Information Society and Techology, ICIST 2016* (Vol. 1, pp. 216–220).

Zhu, F., & Furr, N. (2016). Products to Platforms: Making the Leap. *Harvard Business Review, 94*(4), 18.

5

Blockchain-Based Decentralized Accountability and Self-Sovereignty in Healthcare Systems

Sachin Shetty, Xueping Liang, Daniel Bowden, Juan Zhao, and Lingchen Zhang

Introduction

The recent influx of wearable medical devices promises to bring rich dividends to healthcare stakeholders. Wearable medical devices are networked computing devices equipped with sensors to track the patient's vital signs and physical activities. The data and the analytics can also be linked to Electronic Health Records (EHR), which can benefit patients to help

S. Shetty (✉) • X. Liang
Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Norfolk, VA, USA
e-mail: sshetty@odu.edu

D. Bowden
Sentara Healthcare, Norfolk, VA, USA

J. Zhao
Center for Precision Medicine, Vanderbilt University Medical Center, Nashville, TN, USA

L. Zhang
Information Engineering, Chinese Academy of Sciences, Beijing, China

H. Treiblmaier, R. Beck (eds.), *Business Transformation through Blockchain*,
https://doi.org/10.1007/978-3-319-99058-3_5

monitor their personal health and aid doctors in prescribing personalized medicine and insurance providers to gain insights into cost of providing medical care.

However, due to security and privacy concerns, it has been reported that medical device manufacturers have only instrumented 20–30% of their networked devices to be used in hospitals. There have been several vulnerabilities reported with medical devices. For instance, ICS-CERT reported that Hospira's Symbiq drug infusion pump (Matt 2015) used by medical facilities to automatically administer doses of medication to patients based on the amount specified by the caretaker was vulnerable. The vulnerability allows an attacker to change the doses of prescribed medicine and impact patient safety. In 2017, FDA has reported of vulnerabilities in St. Jude's Medical heart devices (Matt 2015). It is obvious that connected medical devices are here to stay and the likelihood for compromising medical devices grows exponentially. Current cybersecurity solutions for identity management are inefficient and lack the ability to track failure and accountability immediately.

In addition to compromise of medical devices, there are several privacy concerns with health data collected from both wearable devices and EHR systems. Patients are concerned about the lack of transparency in which healthcare stakeholder has access to their data and how is their data used. Current healthcare cybersecurity solutions focus on improving data providers' responsibilities to detect the data disclosure activities; however, it is equally important to protect data access and provide immediate notifications of improper data disclosure risks. In addition, over 300 EHR systems utilize centralized architecture which are prone to single point of failure and suffer from lack of interoperability that results in the lack of a holistic and thorough view of personal health. It is reported by Harris (2016) that 62% of insured adults rely on their doctors to manage their health records, which limits their ability to interact with other healthcare providers than their primary doctor. Moreover, even though many health providers are supposed to follow rules or laws, such as HIPAA (Health Insurance Portability and Accountability Act of 1996), there are still many entities that are not covered by any laws. Therefore, it is crucial that any entity that has access to the data should be accountable for their operations on the data and any operations on the data need to be audited.

Blockchain's capability to capture data provenance will facilitate secure tracking of medical devices from production to ongoing use. The provenance information encoded in the blockchain provides immutable and reliable workflow with a trusted ground truth. The ground truth can be used for transparent, traceability and accountability when any device malfunctions accidentally or as a result of a security attack. The capability will also be useful for autonomous monitoring and preventive maintenance of medical devices. As compared to existing cyber defense solutions, Blockchain's distributed consensus protocols and cryptography techniques, decentralized control will reduce cyber threat risks for medical devices. The other benefits include streamlining the secure tracking of medical devices, cost savings, improving patient privacy by secure and targeted access to patient data.

Blockchain relies on pseudoanonymity (replacing names with identifiers) and public key infrastructure, keeping the privacy of the users. The workshop co-held by the Office of the National Coordinator for Health IT (ONC) and the National Institute for Standards and Technology (NIST) (2016) focused on the blockchain usage in healthcare and research, aiming to clarify the implications of blockchain as an infrastructure for healthcare use cases including privacy preservation for predictive modeling, increasing interoperability between institutions at a large scale, immutability of health records, health insurance claim process improvement, health information exchange, healthcare delivery models with artificial intelligence, identity management, monetization strategies and data provenance requirements.

With the above mentioned issues of data ownership, data isolation and lack of accountability, as well as high privacy risks existing in current EHR systems, patients have little control over their personal health data (Kish and Topol 2015), the notion of Self-Sovereignty by Clippinger (2017) gains great popularity for dealing with healthcare data issues. To better bring this concept into reality, we adopt two novel technologies, Intel SGX and blockchain, to implement a patient-centric PHDM system with accountability and decentralization. Intel SGX offers an anonymous key system (AKS) (Sarangdhar et al. 2016) that can generate an anonymous certificate which will then be transmitted to a certification platform for validation. Blockchain technology, where data are stored in a public, distributed and immutable ledger, maintained by a decentralized network of computing nodes, provides a decentralized and permanent record-keeping capability, which is critical to data provenance (Liang et al. 2017a, b, c; Ekblaw et al. 2016; Peterson et al. 2016; Thierer 2014; Yue et al. 2016; Zhang et al. 2016; Angela 2018) and access control (Hardjono and Pentland 2016) in cloud data protection.

In this chapter, we present a complete patient-centric PHDM system, allowing patients to collect and manage their health data with compliance. In the development of the system, we take the user ownership of data into consideration and the contribution is as follows.

- Self-Sovereign Data Ownership. We adopt the idea of user-centric architecture to control data access and issue permissions. It is the data owner that decides who can access the data and whether to make the data public or private, as well as how to validate the data. Token-based verification is utilized to grant one-time access to data requested by third parties.
- Permanent Data Record with Integrity. We collect data records and submit an abstract of each record to the blockchain network. The records are included in a block and the integrity of the record is guaranteed by the consensus mechanism used in the block mining process.
- Scalable Data Processing. The volume of health data collected from wearable devices and user input scales greatly so we propose a high-speed algorithm to improve the efficiency of data processing.
- Decentralized and Distributed Privacy and Access Control. We propose a decentralized permission management protocol to deal with each personal health data request. The data access records are stored to provide traceable logs, using blockchain to preserve immutability.
- Trusted Accountability. The trusted execution environment provisioned by Intel SGX is utilized to generate a fingerprint for each data access. For medical treatment and insurance enforcement, every action is traceable. Once data leakage is detected, the malicious entity can be identified for investigation.

System Architecture

A three-layer architecture for accountability and privacy preservation is designed for the PHDM system. The data sharing layer provides users with entire control over their personal health data and handles data requests from third parties. The SGX enabled hardware layer provisions a trusted execution environment in the cloud, generates data access tokens and is responsible for reliable data storage and process. The blockchain network layer, which is distributed and untrusted, records data operations and various data access requests for immutability and integrity protection. Figure 5.1 is a general scenario for the patient-centric PHDM system. Personal wearable devices collect original health data, such as walking distance, sleeping conditions and heartbeat, which may be synchronized by the user with their online account associated with the cloud server and cloud database. Every piece of health data could be hashed and uploaded to the blockchain network for record-keeping and integrity protection. The original data is maintained in the cloud database hosted on trusted platform enabled by SGX. The user owns personal health data, maintains access tokens, and is responsible for granting, denying, and revoking data access from any other parties requesting data access. For example, a user seeking medical treatment would grant the doctor a one-time data access token. Same scenario applies to user-insurance company interactions. Besides, user can also manually record everyday activities according to a particular medical treatment such as medicine usage and share the information frequently with the doctor.

Healthcare providers such as doctors can perform medical test, give suggestions or provide medical treatment, and request access to previous medical treatment from the patient. The data request and the corresponding data access is recorded on the blockchain for distributed validation. Besides, user may request a health insurance quote from insurance companies to choose health insurance plans. Insurance companies can also request access to user health data from wearable devices and medical treatment history. The blockchain network is used for three purposes. For health data collected from wearable devices and from healthcare providers, each of the hashed data entry is uploaded to the blockchain network

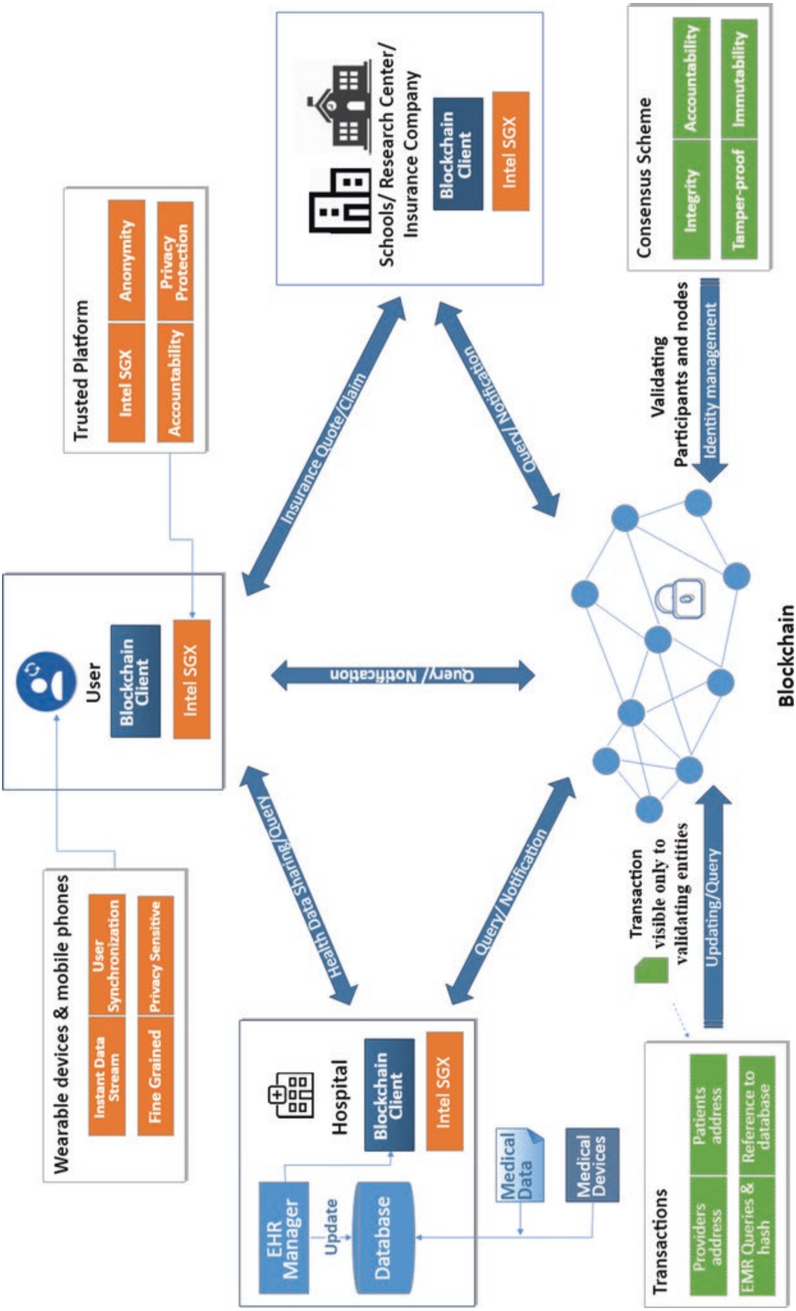


Fig. 5.1 Patient-centric PHDM system

for integrity protection. For personal health data access request from healthcare provider and health insurance company, a permission from the data owner is needed with a decentralized permission management scheme. Besides, each of the access request and access activity should be recorded on the blockchain for further auditing or investigation. Each of the data access request should be processed to get a permission from the data owner with a decentralized permission management protocol. The access control policies should be stored in a distributed manner on the blockchain which ensures stability. Besides, each of the access request and access activity should be recorded on the blockchain for further auditing or investigation.

System Entities

User System users collect data from wearable devices that monitor users' health data such as walking distance, sleeping conditions, and heartbeat. Those data are then uploaded to the cloud database hosted on trusted platform via the mobile application. User is the owner of personal health data and is responsible for granting, denying, and revoking data access from any other parties, such as healthcare providers and insurance companies. If the user is seeking medical treatment, the user would share the health data with the desired doctors. If the treatment is finished, the data access is revoked to deny further access from the doctors. Same scenario applies to user-insurance company relations. Besides, user can also record everyday activities according to a particular medical treatment such as medicine usage to share with the treatment provider for adjustment and better improvement.

Wearable Device Wearable devices serve to transform original health information into human readable format and then the data is synchronized by the user to their online account. Each account is associated with a set of wearable devices and possible medical devices. When a piece of health data generated, it will be uploaded to the blockchain network for record-keeping and integrity protection.

Healthcare Provider Healthcare providers such as doctors are appointed by a certain user to perform medical test, give some suggestions or provide medical treatment. Meanwhile, the medical treatment data can be uploaded to the blockchain network for data sharing with other healthcare providers under the user's permission. And the current healthcare provider can request access to previous health data and medical treatment from the user. Every data request and the corresponding data access is recorded on the blockchain.

Health Insurance Company User may request a health insurance quote from health insurance companies or agents to choose a proper health insurance plan. To provide better insurance policies, insurance companies request data access from users including user health data from wearable devices and medical treatment history. Users with previous medical treatment(s) may need to pay a higher rate and the history cannot be denied by users to prevent insurance fraud. Users can choose not to share exercise information due to privacy issues but mostly they would desire to share because regular exercise can bring down the insurance pay rate. However, users cannot hide or modify medical treatment history data since those data are permanently recorded on the blockchain network and the integrity and trustworthiness is ensured. Moreover, the insurance claims can also be recorded on the blockchain.

Blockchain Network The blockchain network is used for three purposes. For health data collected from both wearable devices and healthcare providers, each of the hashed data entry is uploaded to the blockchain network for integrity protection. For personal health data access from healthcare provider and health insurance company, a permission from the data owner is needed with a decentralized permission management scheme.

Cloud Database The cloud database stores user health related data, data requests from the healthcare provider and insurance companies, data access record and data access control policy. Data access is accountable and traceable. Once data leakage is detected, the malicious entity can be identified.

Key Establishment

In the patient-centric data management system, users are required to register an online account to be involved in the system and generate data encryption key pairs to encrypt their cloud data for confidentiality. For key management, we assume the system developers adopt a secure wallet service. The description of each key established is as follows.

User Registration Key K_{UR} The user needs to create an online account to store health data collected from wearable devices and other sources in the cloud database. We denote the user registration key as K_{UR}. Every time user wants to operate on their cloud health data, the registration key is needed. This key is generated from the platform identity key using Intel SGX AKS and is thus bounded to the user. Even if the user's registration key is stolen or compromised, it could not be used elsewhere without the user authentication. Similarly, the registration key for healthcare provider and healthcare insurance company is K_{HR} and K_{IR}, respectively.

Data Encryption Key K_{DE} After registration, the user generates an encryption key K_{DE} to encrypt all the health data stored in the cloud database. When a health data entry is created, user has the option to encrypt the data entry, which limits the data access only to the key owners, and the hashed data entry will be uploaded instantly to the blockchain.

Data Sharing Public/Private Key Pair (PK_{DS}, PR_{DS}) For health data sharing, a public/private key pair will be generated, denoted as (PK_{DS}, PR_{DS}). In some cases that the data sharing activity is to be recorded on the blockchain, the private key is used to generate a signature from the user to indicate the health data ownership, while the public key is used by others to verify the ownership. When users want to share their health data with healthcare providers or insurance companies, they share the private key for data access and the corresponding tokens generated with this private key.

Platform Identification Key K_{PID} Each trusted platform owns a platform identification key K_{PID}, also generated from the platform identity key using Intel SGX AKS. Every health data request and data access on a certain platform will generate an activity record signed by K_{PID} for accountability while still with anonymity preserved. Different entity keys are noted as K_{PIDu} for users, K_{PIDp} for healthcare providers, and K_{PIDi} for insurance companies.

PHDM Procedures

In the system, there are five phases for PHDM: user registration, health data generation and synchronization (data generated from user, healthcare provider, and insurance company), health data access management, health data access record uploading, and health data access auditing.

User Registration In the system, user needs to create an online account to store health data collected from wearable devices and other sources in the cloud database by way of establishing an online ID. Other entities in the system cannot correlate the online ID with their real identity, preserving user privacy in the registration phase. Personal health data comes from wearable devices such as activity trackers or smart watches, and medical devices such as pacemakers or defibrillation, as well as manual user input for treatment tracking such as medicine usage and training. To synchronize the personal data to the cloud for convenient access and further process, the user first can register to the cloud service provider for an online account with enough storage capability. Figure 5.2 shows the data collection and synchronization architecture.

Health Data Generation and Synchronization Health data contains four categories: data collected from wearable devices, data collected from medical test, data collected by patient indicating their treatment details, and data recorded by healthcare providers and insurance companies. After registration, the user can collect health data from wearable devices, which monitor their everyday activities, such as walking, bicycling, and sleeping, and choose to synchronize those data with their online account. The collected data is encrypted using K_{DE} and stored in the cloud database. This preserves user privacy in the data generation and storage phase.

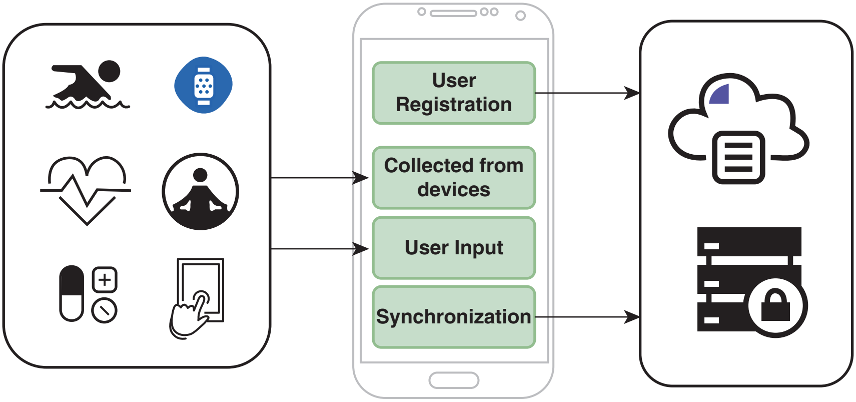


Fig. 5.2 Personal health data collection

The synchronization step triggers an event in the system which transforms the event into a transaction on the blockchain. Every time a health data entry is created, user has the option to encrypt the data entry and upload the record on the blockchain.

Health Data Access Management User can share data with healthcare providers to seek healthcare services, and with insurance companies to get a quote for the insurance policy and to be insured. A token-based access control mechanism is adopted to control personal health data access and exposure. The health data are stored in the cloud database and the access control policies are stored on the blockchain in a decentralized way to ensure integrity and remove the necessity of a trusted third party. Both healthcare providers and insurance companies can request data access to the data owner, that is, the registered user in the system. User can grant, deny, and revoke access from both parties. Each time there is a data request, the user will generate an access token to the requester. The access token is bound to a trusted platform for accountability.

Health Data Access Record Uploading As mentioned above, once a data request or data access event is monitored in the system, the event will be captured as a data access record which will serve as a system log for future validation and regulation. The record is hashed and eventually transformed into a Merkle tree node (Merkle 1980) using Tierion API (Tierion 2016). The Merkle tree root node will be anchored in a blockchain transaction following the Chainpoint 2.0 protocol, proposed by Wayne et al. (2016). For the blockchain nodes, both healthcare providers and insurance companies can join the blockchain mining process in exchange for the large-scale dataset retrieved from personal health database as mining rewards. For privacy concerns, the dataset removes sensitive information such as name and location and is anonymous. Insurance companies can learn more information from medical history and health data so that they can make specific policies according to the characteristics of customers. Healthcare providers can learn from previous medical treatment and gain experiences which will benefit future medical cases and improve medical levels.

Health Data Access Auditing When it is necessary for legal regulators to investigate the system security, user can grant the system auditor access to the data records on blockchain network. Each data record is verifiable by checking the record signatures. It is also accountable against the trusted platform by identifying the platform key used in the signature.

Token-Based Access Control

For anonymity and verification purposes, we adopt the token-based access control mechanism to handle the data management process. As is shown in Fig. 5.2, the cloud server is responsible for issuing and verifying tokens, and also maintaining both the data record database and data access log database. Users can request and share the access tokens to data requestors. Potential data requestors include healthcare providers, insurance companies, and even system auditors. Each data and token operation is recorded in the blockchain and thus validated. After user registration, the cloud server can issue tokens based on the personal information provided by users. To access data, the required token will be presented to the cloud server and verified. The server issuance operation, the user token presentation, and verification omit system logs, which will be stored in the log database, as well as data requests and access from third parties.

U-Prove Based Token Generation

User registration is based on U-Prove (Paquin and Zaverucha 2011), which is proved capable to be integrated into Trusted Platform Module 2.0 by Chen and Li (2013). U-Prove (Paquin 2013) includes three entities, namely, issuer, prover, and verifier. In our system, the issuer and the verifier are the same entity, that is, the cloud server. The user in our PHDM system is the prover entity in U-Prove model. During user registration phase, there are some parameter definitions for both prover and issuer.

- The value of the token information field ($T\,I$): $T\,I \in (0, 1)^*$
- The value of the prover information field ($P\,I$): $P\,I \in (0, 1)^*$
- Application Attributes (AA): $(A1, \ldots, An), T\,I$

  $(A1, \ldots, An)$ indicates n attributes from the application itself.

- Issuer Parameters (IP): U IDp, desc(Gp), U IDH, (g0, g1, …, gn, gt), (e1, …, en), S

U IDp is an application-specific identifier for this particular *IP*, which is unique across the PHDM system and *desc*(*Gp*) specifies the group (*Gp*) with an order of *p*, which is used for discrete logarithm computation in the following verification steps.

U IDH is the identifier for the secure hash algorithm. $(g0, g1, \ldots, gn, gt)$ is the issuer's public key. $(e1, \ldots, en)$ is generated from *AA*, indicating the format of each application attribute.

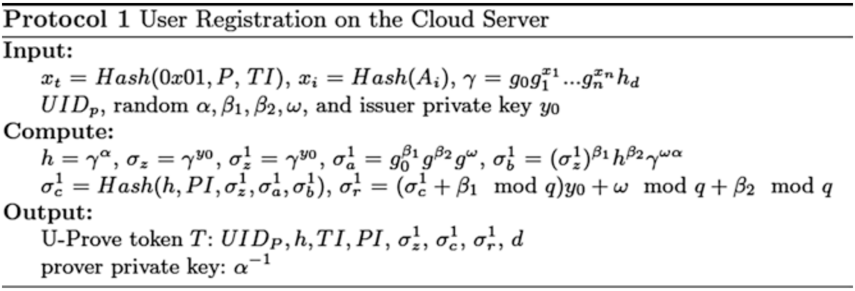
- The hash of the *IP* (*P*): $P = H(IP)$
- Device-protected Boolean (*DB*): *d*

This indicates whether the protocol is device-protected. PHDM adopts trusted execution environment so the value by default is *true*.

- Device Parameters: *gd, xd, hd*

The device generator *gd* satisfies *gd* ∈ *Gq*. *xd* is device private key and *hd* is the public key.

With the above information provided, we choose the issuance protocol version number 0*x*01. The user platform identification key K_{PIDu}, is used to generate the device private key. The token generation protocol is as follows.



```
Protocol 1 User Registration on the Cloud Server
Input:
    $x_t = Hash(0x01, P, TI)$, $x_i = Hash(A_i)$, $\gamma = g_0 g_1^{x_1} ... g_n^{x_n} h_d$
    $UID_p$, random $\alpha, \beta_1, \beta_2, \omega$, and issuer private key $y_0$
Compute:
    $h = \gamma^{\alpha}$, $\sigma_z = \gamma^{y_0}$, $\sigma_z^1 = \gamma^{y_0}$, $\sigma_a^1 = g_0^{\beta_1} g^{\beta_2} g^{\omega}$, $\sigma_b^1 = (\sigma_z^1)^{\beta_1} h^{\beta_2} \gamma^{\omega\alpha}$
    $\sigma_c^1 = Hash(h, PI, \sigma_z^1, \sigma_a^1, \sigma_b^1)$, $\sigma_r^1 = (\sigma_c^1 + \beta_1 \mod q) y_0 + \omega \mod q + \beta_2 \mod q$
Output:
    U-Prove token $T$: $UID_P, h, TI, PI, \sigma_z^1, \sigma_c^1, \sigma_r^1, d$
    prover private key: $\alpha^{-1}$
```

The cloud server issues tokens to users with the signature ($\sigma_z{}^1$, $\sigma_c{}^1$, $\sigma_r{}^1$). For privacy concerns, the AA are hashed for the generation of U-Prove based token. During some circumstances, the issuer is able to generate multiple tokens at one time for better performance.

Token Presentation Protocol

A presentation proof of ownership of certain messages or attributes contained in the token is generated using the token private key and is required to access user data in the cloud database. Before accessing data, the data requestor needs to attest itself and convince the user that it is running on top of SGX enabled environment in an isolated enclave. The SGX attestation is launched by the data requestor, which will send a signed quote to the data owner for verification using the platform dependent key. The remote attestation between the two platforms is performed with the assistance of the Intel Attestation Service (Anati et al. 2013). After the verification, the user will request a one-time U-Prove token with a newly generated private key PRDS and share it with the data requestor. The data requestor forwards the token to the verifier of the cloud database and will be granted access after the verification. Different decisions can be made by the user, such as to grant, deny and revoke access. The presentation proof serves two purposes. For one thing, it proves the integrity and the authenticity of the attribute values and for another, it establishes the confirmation of the ownership of the private key associated with the token itself, which will further prevent token replay attack.

Decentralized Accountability and Integrity Protection

As is shown in Fig. 5.2, each data and token operation is recorded in the blockchain and thus validated in a decentralized and permanent manner, ensuring data integrity. Besides, every operation is launched on a trusted platform enabled by Intel SGX, making the operation record trustworthy and nonframeable. The event record can be described using a tuple as <*datahash, owner, receiver, time, location, expirydate, signature*> where the signature comes with platform dependency for accountability. Then the tuple is submitted to the blockchain network, which is followed by several steps to transform a list of records into a transaction. A list of transactions will be used to form a block, and the block will be validated by nodes in the blockchain network by consensus algorithms. After a series of processes, the integrity of the record can be preserved, and future validation on the block and the transaction related to this record is accessible. Each time there is an operation on the personal health data, a record will be created and anchored to the blockchain. This ensures that every action on personal health data is accountable. There are different types of operations from different parties, as listed in Table 5.1. The SGX platform identification key KPID is used to generate the signature thus making each record platform dependent and ensuring that every action on personal health data is accountable. The token generation and issuance are also recorded in the same way so as to track the data requests and authorizations.

For scalability considerations, we adopt a Merkle tree-based architecture (Merkle 1980) to handle large number of data records. Each

Table 5.1 Types of operations in the healthcare collaboration system

Health data	Operator	Operation
Personal health data	User	Update, query
	Healthcare provider	Query
	Insurance company	Query
Medical history	Healthcare provider	Update, query
	User	Query
	Insurance company	Query
Insurance information	Insurance company	Update, query
	User	Query
	Healthcare provider	Query

leaf node represents a record and the intermediate node is computed as the hash of the two leaf nodes. The Merkle root, along with the tree path from the current node to the root, serves as the proof of integrity and validation, that is, the Merkle proof. The basic Merkle proof is shown in Fig. 5.3. First, we need to identify the record location, the targetHashB. The target hash and the path to the Merkle root, that is, nodes in green, constitute the Merkle proof of the hashed data record,

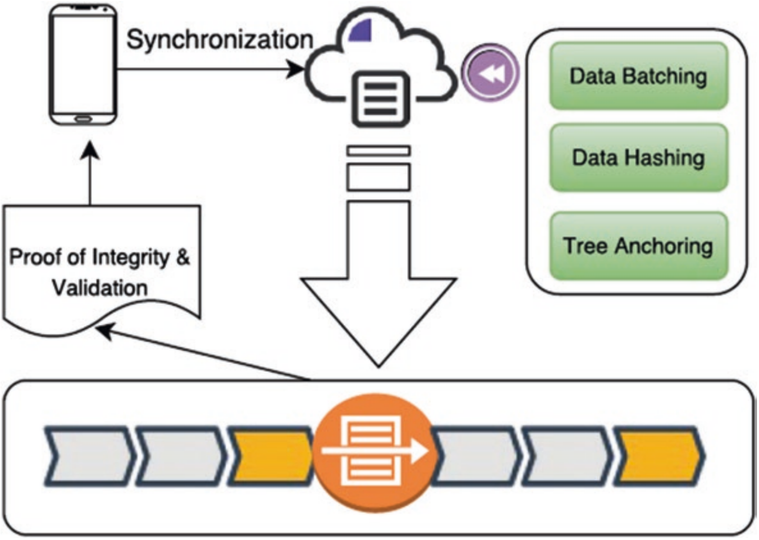


Fig. 5.3 Personal health data integrity protection

which is stored in a JSON-LD document that contains the information to cryptographically verify that the record is anchored to a blockchain. By calculating the hashes in different tree levels, it is easy and fast to obtain the root hash, which is anchored in the blockchain transaction, witnessed, and maintained by some distributed nodes. It proves the data was created as it was at the time anchored. The Merkle root for each Merkle tree is related to one transaction in the blockchain network, which means a blockchain transaction represents a list of data records the Merkle hosts, enabling the scalability and effectiveness of data integrity protection and validation. The tree-based architecture protects the integrity of each operation record itself which can be validated by traversing the tree nodes. Meanwhile, it implicitly indicates the integrity of all the nodes in that any single node modification could lead to the modification of the root, thus protecting the integrity of the whole tree structure at trivial costs (Figs. 5.4 and 5.5).

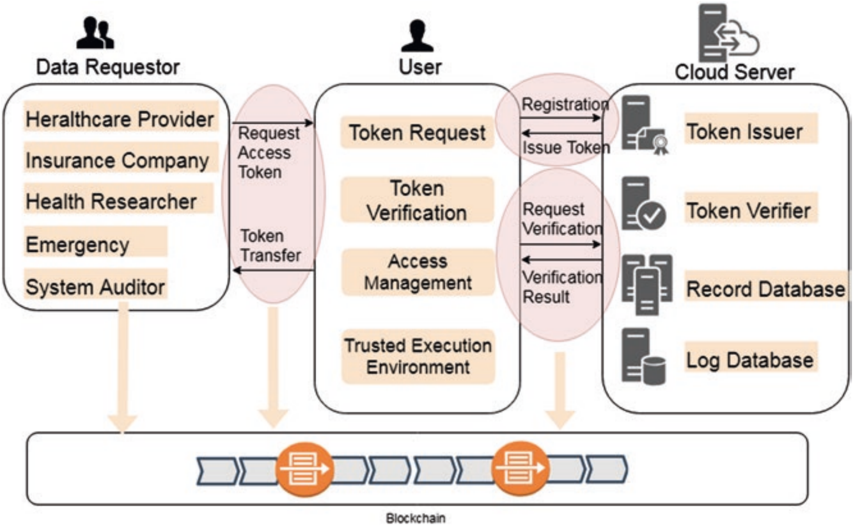


Fig. 5.4 PHDM system interaction

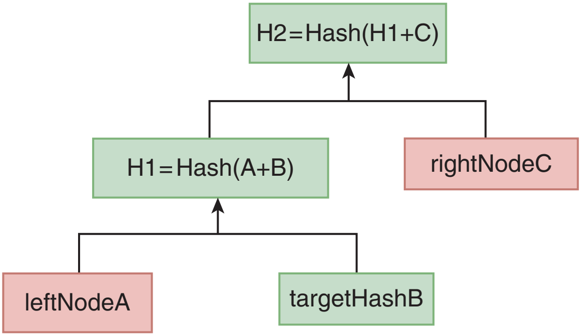
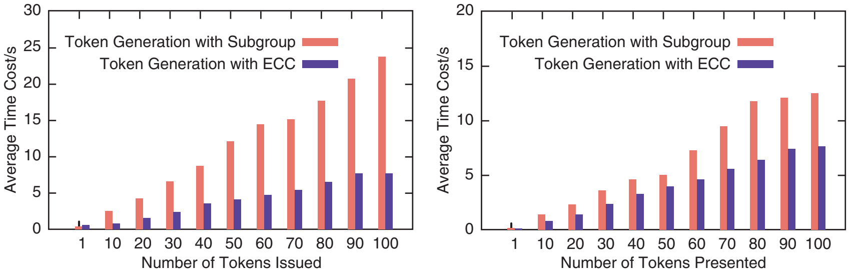


Fig. 5.5 Merkle tree-based data integrity protection

System Evaluation

Our system adopts a user-centric model for processing personal health data using blockchain network, ensuring the data ownership of individuals, as well as data integrity. The operations on the data records are highly inter-operable and compatible with current systems. By enforcing access control policies, users can handle their personal data without worrying about the privacy issues. Meanwhile, each request and update from healthcare providers and health insurance companies are recorded and anchored to the blockchain network, making actions toward personal health data accountable. With all the security objectives proposed in Section I achieved, it is crucial to evaluate the system performance, regarding to the scalability and efficiency of the data integrity proof generation and data validation process. We test different numbers of concurrent records with a range from 1 to 10,000. Figures 5.6 and 5.7 show the average time cost. From these two figures, we can conclude that the system can handle a large dataset at low latency, which indicates the scalability and efficiency of the data process. By adopting Merkle tree method to batch data, we implement an algorithm with the computation complexity of $O(\log_2 n)$. This is an important advantage when the data records are collected at a high frequency. In the future, we will take a deeper vision into the delay tolerance for healthcare data processing and improve the data collaboration procedures accordingly.



(a) Average Time for Token Issuance (b) Average Time for Token Presentation

Fig. 5.6 Average time cost for token issuance and presentation

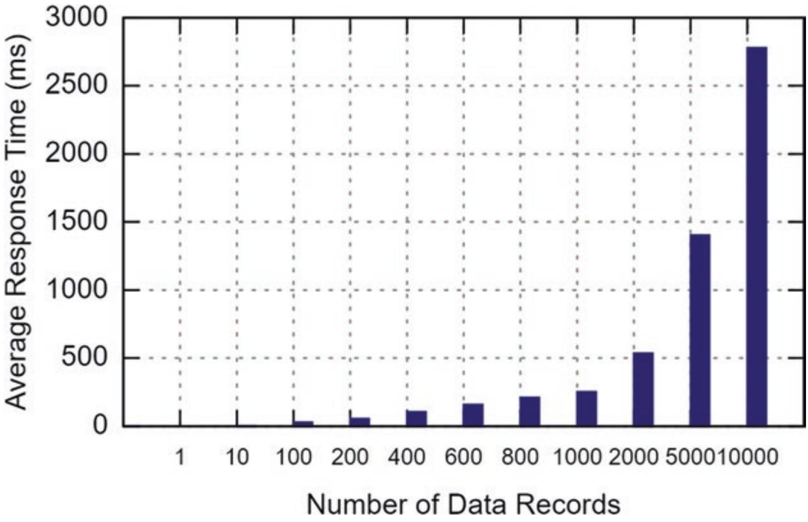


Fig. 5.7 Average time for proof generation

For U-Prove based token generation, we select five attributes predefined and involved in each token and two of them are required to obtain a data access token. During the token issuance, there are basically two cryptographic methods for digital signature including Subgroup and ECC. The evaluation results for token issuance and presentation with these two methods are shown in Fig. 5.4a, b. It can be concluded that ECC-based token generation is more efficient than the subgroup-based method. This can be explained that ECC utilizes shorter key length for the elliptic curve than subgroups of equivalent security levels and com-

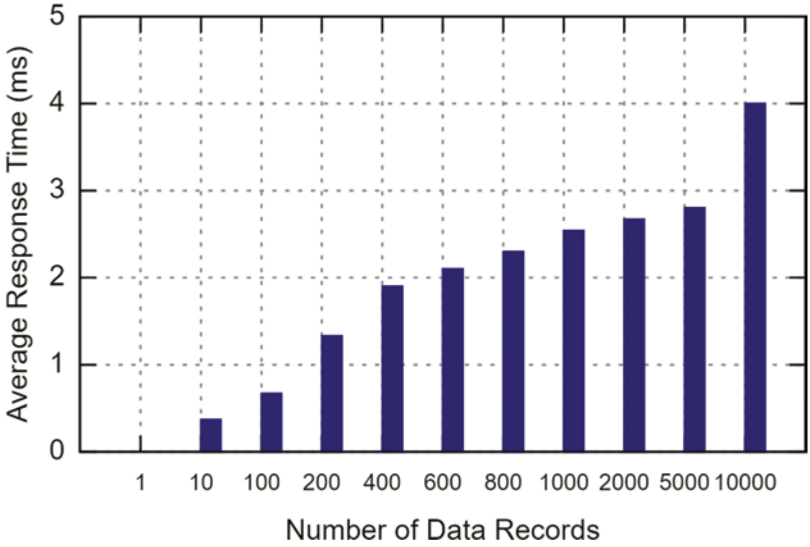


Fig. 5.8 Average time for proof validation

putes faster with a small field. Adopting the ECC-based U-Prove protocols for both token issuance and presentation, the average overhead brought to the system is 8.1% and 9.4%, respectively (Fig. 5.8).

Mitigation of Attack Surfaces in Blockchain Using Intel SGX

The proposed PHDM system will be deployed in a permissioned blockchain platform within a healthcare organization's cyber infrastructure. However, the permissioned blockchain platform are susceptible to attacks. In this section, we provide information on INTEL SGX mitigates attack surfaces in the proposed PHDM system.

Blockchain Vulnerabilities and Attacks

Due to the P2P communication model and the trustless node involvement, most blockchain services and blockchain-based applications could be vulnerable to certain attacks that are difficult to detect or prevent. It is possible that the network node is compromised and thus negatively impact the mining process or consensus process. In this section, we present and analyze the vulnerabilities that are possible for distributed ledgers.

Block Withholding Attack (A1)

Blockchain nodes usually join a pool to mine blocks with other nodes. Once a new block is mined, the rewards is shared among all the pool members. However, some malicious nodes intend to join the pool but never publish the block that has been mined, which decreases the overall rewards of the pool (Rosenfeld 2011). Such attack is hard to detect because the mining process is controlled by the owner of the mining platform. Even when the platform finds a solution to a new block, other nodes are not aware of the fact. Analysis (Courtois and Bahack 2014) shows that block withholding attack makes it possible for a rogue miner to gain profit without effort.

Block Discarding Attack (A2)

Block discarding attack (Bahack 2013) happens when a node controls the majority of network connections with other nodes. A mined block needs to be confirmed by most of the nodes and added to the blockchain. If the network is controlled by a single party that intends to discard a certain block mined by a normal node, the attack will discourage the nodes in the controlled network from confirming this block. In this way, the newly mined block by the normal node will be set invalid if a block from other nodes is confirmed earlier than itself.

Replay Attack (A3)

Replay attack often happens in P2P networks where there are frequent message exchange and propagation. Attackers may try to repeat or delay an intercepted data transmission, thus preventing the honest party from communicating normally with the party where the message comes from

(Dua et al. 2013). Replay attack in blockchain network is discussed in several scenarios, such as smart grid (Kim et al. 2016) and IoT environment (Lee and Lee 2017), as well as blockchain-based big data authentication protocols (Abdullah et al. 2017). Replay attack also serves as a way to launch block withholding attack when the malicious node eavesdrops the block confirmation message and delays the message from immediate propagation. For blockchain applications where there are quantities of distributed nodes, it is challenging to mitigate such attacks using the traditional timestamping services since most message exchange is transferred in a simultaneous session and a concurrent manner.

Man in the Middle Attack (A4)

Man in the Middle Attack (Callegati et al. 2009) is similar to replay attack in that attackers try to intercept the message between two honest parties, possibly alter the message and then deliver the false message. Usually, the attacker tries to insert himself in-between the information flow of the client and server, inject a forged message to both sides so that he can impersonate either side. Both the client and server could leak sensitive information since they believe they are interacting with the authenticated parties. In blockchain network, this could happen when a node joins the block mining process and steal the mining result, that is, the solution to a puzzle in a proof of work blockchain, from another node and then pass it to other participants for confirmation. Even though there are methods to detect such attacks, but the timing is critical. When the solution finder realizes that the solution is stolen, it may be too late since the rewards are already distributed.

Potential Privacy Risks (A5)

One major concern of blockchain is the privacy issue due to the distributed nature of node connection. Each node participates in the network actively to broadcast messages and receive rewards. Transactions made by each node is traceable by other nodes. This is also concerned with the anonymity issue which is acknowledged in Bitcoin transactions since the transactions are permanently recorded in the public ledger while everyone can see the detailed transaction balance and public addresses. Some scenarios such as financial institutes and military communications require isolated transactions built on top of tamper-proof blockchains. If the privacy issue is solved, users can communicate in a secure way without exposure of sensitive information and still make use of blockchain benefits for integrity protection.

Majority Hash Rate Attack (A6)

In order to gain a large quantity of profit, some miners use special mining equipment to control a great source of mining power. When an attacker controls more than 50% of the entire mining power, he can reverse transactions he sent while he is in control and even prevent some transactions from being confirmed with high possibility. This is why majority hash rate attack is also called 51% attack. This attack could also lose the decentralized nature of blockchain since the majority of the network is controlled by a powerful entity. A two-phase proof of work (Bastiaan 2015) is proposed to prevent such attack but the hardware is not seriously considered in the model.

SGX Capabilities

Intel SGX provides enclaves, which is an isolated zone for trusted program running, to reduce the attack surface and minimize the trusted computing base. We illustrate three key notions adopted by SGX, namely, Enclave, Attestation, and Sealing, as follows.

Enclave

When an enclave is created, the sensitive code and data will be stored inside a protected memory region called Enclave Page Cache (EPC). The EPC region is encrypted which ensures strong confidentiality. The code inside the enclave is not authorized to access memory beyond the enclave boundaries. If code inside one enclave accesses content in another enclave, there would be an error of aborted page access. Enclave Page Cache Map is a hardware structure which stores security and access control information for every page in the EPC. After the enclave is provisioned with appropriate memory content, there will be an enclave measurement stored in two registers, MRENCLAVE and MRSIGNER. MRENCLAVE provides an identity of enclave code called enclave identity, which is a SHA-256 digest of enclave log by ECREATE instruction. The enclave log contains the content and relative position of the enclave pages as well as some security flags (Intel 2013). MRSIGNER identifies an enclave signer's identity called sealing identity, which signs an enclave when the enclave is created. Inside the MRSIGNER, the hash of the signer's public key is stored. After enclave is initialized, the enclave identity and sealing identity will be available by calling.

EGETKEY and EREPORT instructions. Each enclave has a certificate issued by the enclave author in the format of SIGSTRUCT. Three metadata fields in SIGSTRUCT is used to determine an enclave's identity: the modulus of the RSA key used to sign the certificate (MODULUS), the enclave's product ID (ISVPRODID), and the security version number (ISVSVN). An enclave author can issue several enclave certificates using the same RSA key to indicate different modules of the same software.

Attestation

Attestation is a process that one entity proves that it is running on top of a trusted platform to another. Intel SGX provides two types of attestation, including local attestation (two enclaves running on the same platform) and remote attestation (extending local attestation to outside of the platform). Local attestation can be performed between two enclaves: target enclave and challenger enclave. First of all, challenger enclave sends attestation request to target enclave for verification as well as challenger enclave's MRENCLAVE value. Then target enclave uses EREPORT instruction as well as the received MRENCLAVE value to create a signed REPORT for challenger enclave and sends it back. Challenger enclave receives the REPORT and extracts the REPORT key to compute the MAC. If the MAC matches the value on the target enclave's REPORT, then challenger enclave can confirm that target enclave is running on the same trusted platform. Then challenger enclave can create a REPORT for target enclave and sends it to target enclave so that target enclave can confirm that challenger enclave is on the same platform in a similar way. In some cases, two enclaves on different platforms need to verify each other. Intel SGX enables a third enclave called quoting enclave to help launch a remote attestation. Quoting enclave adopts Intel Enhanced Privacy ID (EPID) (Brickell and Li 2011) as a key to sign the REPORT from the target enclave on the same platform and generate a QUOTE which will be sent to the remote enclave for verification. Similar to local attestation, there is a challenger enclave requesting to verify the target enclave. Here, the target enclave exists on a different platform from the challenger enclave. The target enclave will create a REPORT and send it to the quoting enclave. The quoting enclave signs the REPORT using the EPID key to generate a QUOTE and sends the QUOTE back to the target enclave. The target enclave forwards the QUOTE to challenger enclave as well as some other user data for authentication. Challenger enclave uses an EPID public key to verify the QUOTE. In this way, the target platform is verified and further communication can be established.

Sealing

When enclave program finishes running, the code and data inside the enclave will be gone. In order to store the data for future use, Intel SGX provides a sealing key to encrypt data and ensure data integrity. The sealed data can only be unsealed when the trusted environment is restored locally (Anati et al. 2013). By calling EGETKEY instruction, current enclave can access the sealing key, seal the data, and export the data to a memory region outside the enclave. There are two sealing policies designed by Intel, including sealing to the enclave identity and sealing to the sealing identity. Depending on the access control policies of the enclave applications, different sealing policies can be adopted. Sealing to the enclave identity can produce a key only available to the exact enclave instance. If a key available to different enclave instances under the same sealing identity is needed, the policy of sealing to the sealing identity (Sealing Authority) can make it. With the security notions described above, the security capabilities of SGX can be summarized as follows.

Enclave Execution (C1) is tamper-resistant against software attacks outside the enclave (McKeen et al. 2013). **Hardware-rooted Randomness (C2)** provides a valuable source for cryptographic key generation and protection. A true random function is provided in the tRTS (Trusted Run-Time System) library available in Intel CPUs (Aumasson 2016). **Remote Attestation (C3)** allows a client platform to attest itself to a remote party proving that the client is running in a trusted environment. This ensures the integrity of code execution in both the client and server side. **Trusted Elapsed time (C4)** provides a hardware-assisted measure for trusted timestamping service, which is critical for scenarios where it is time sensitive. **Confidentiality Assurance (C5)** prevents sensitive transactions and business contracts from leakage. The enclave identity key and provisioning key can be involved for secret protection and attestation. **Sealing and Unsealing (C6)** helps to store confidential information outside the enclave for future access after system shutdown. **Monotonic Counter (C7)** is supported to serve as a measure to defend against the replay attack.

Considering the attacks mentioned, we utilize Intel SGX to establish a trusted execution environment which will greatly reduce the attack surface and minimize the trusted computing base. At the same time, most SGX capabilities can be chosen to effectively defend all of the six attack as illustrated in Table 5.2, to achieve a reliable distributed ledger.

Trusted execution could be established in an enclave zone (C1) which provides an isolated environment and thus the reduced attack surface, playing an important role in defending against all five attacks. The code and data inside the enclave are integrity-protected. SGX enabled blockchain mining ensures that the mining process will be isolated inside the enclave. Even when the platform and the Operating System is controlled by a malicious entity, the mining is still protected from compromise. This guarantees that once a block is mined, the block will be immediately submitted to the blockchain network without delay, making block withholding attack impossible. Hardware-rooted Randomness (C2) helps with

Table 5.2 Design rationale for SGX enabled blockchain

Potential attacks	Intel SGX capabilities
Block withholding attack (A1)	Enclave execution (C1)
Block discarding attack (A2)	Enclave execution (C1), remote attestation (C3), monotonic counter(C7)
Replay attack (A3)	Hardware-rooted randomness (C2), remote attestation (C3), trusted elapsed time (C4)
MITM attack (A4)	Hardware-rooted randomness (C2), remote attestation (C3), confidentiality assurance (C5)
Potential privacy risks (A5)	Enclave execution (C1), confidentiality assurance (C5), sealing and unsealing (C6)
Majority hash rate attack (A6)	Enclave execution (C1)

random number generation used in key management protocols, benefiting the message exchange in transactions between blockchain nodes and is capable of resisting replay attack. The function *sgx read rand*() calls the hardware-based pseudorandom generator (PRNG) available in Intel CPUs through the RDRAND instruction. Remote Attestation.

(C3) is employed during communications between client and server for the purpose of key negotiation and exchanging shared secrets which will be used in the following interaction. The shared secrets established using remote attestation may become platform dependent, making it an effective countermeasure for resisting the man in the middle attack since the secret is bound to the platform dependent identity that cannot be forged by a middle man. To provide a message with a trusted timestamping, the SGX capability of trusted elapsed time (C4) can be adopted by calling *sgx get trusted time* from the architecture enclave service. This trusted time can effectively prevent replay attack where a given expire time is set. Confidentiality Assurance (C5) protects peer to peer communication in the transaction process and preserve the confidentiality of both identity and transaction. Enclaves can seal and unseal the secret (C6) shared by two parties, especially the secret is used multiple times. Monotonic Counter (C7) provides a trusted counter by calling *sgx create monotonic counter* function, which is utilized to preserve message authenticity during communications, thus enhancing resistance against replay attack and man in the middle attack.

Conclusion

In this chapter, we design and implement a mobile healthcare system for personal health data collection, sharing and collaboration between individuals and healthcare providers, as well as insurance companies. The system can also be extended to accommodate the usage of health data for research purposes. By adopting block chain and SGX technology, the system is implemented in a distributed and trustless way so that personal health data is stored and shared with robustness. The algorithm to handle data records can preserve both integrity and privacy at the same time.

By utilizing blockchain technology in the self-sovereign healthcare systems, we manage to distribute the responsibility of maintaining trusted records for data operation as well as token generations.

Meanwhile, benefiting from the blockchain consensus scheme and the decentralized architecture, along with the trusted execution environment and the platform dependency provisioned by Intel SGX, the records are anchored with trusted timestamping and redundancy, preserving both availability and accountability of the healthcare data and operations. We also propose U-Prove based protocols for the permission management. We implement a prototype of the PHDM system and the evaluation shows that the performance is acceptable.

For future work, we will integrate the PHDM system with the enhancement of a blockchain-based access control scheme to provide better data protection and user privacy. We will explore how to combine both personal health data and medical data together and provide a better solution to address healthcare uses in identity management and electronic health record management.

References

Abdullah, N., Hakansson, A., & Moradian, E. (2017). Blockchain Based Approach to Enhance Big Data Authentication in Distributed Environment. In *Ubiquitous and Future Networks (ICUFN), 2017 Ninth International Conference on* (pp. 887–892). IEEE.

Anati, I., Gueron, S., Johnson, S., & Scarlata, V. (2013). Innovative Technology for CPU Based Attestation and Sealing. In *Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy* (Vol. 13).

Angela, S. (2018). *FDA Issues Safety Communication on Availability of Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (Formerly St. Jude Medical's) Implantable Cardiac Pacemakers*. https://www.fda.gov/NewsEvents/Newsroom/FDAInBrief/ucm573853.htm

Aumasson, L. (2016). *Sgx Secure Enclaves in Practice: Security and Crypto Review – Kudelski Security*. Black Hat USA.

Bahack, L. (2013). *Theoretical Bitcoin Attacks with Less Than Half of the Computational Power (Draft)*. arXiv preprint arXiv:1312.7013.

Bastiaan, M. (2015). *Preventing the 51%-Attack: A Stochastic Analysis of Two Phase Proof of Work in Bitcoin*. Available at http://fmttools.ewi.utwente.nl/files/sprojects/268.pdf

Brickell, E., & Li, J. (2011). Enhanced Privacy ID from Bilinear Pairing for Hardware Authentication and Attestation. *International Journal of Information Privacy, Security and Integrity 2, 1*(1), 3–33.

Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-Middle Attack to the https Protocol. *IEEE Security Privacy, 7*(1), 78–81.

Chen, L., & Li, J. (2013). Flexible and Scalable Digital Signatures in tpm 2.0. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security* (pp. 37–48). CCS' 13. New York: ACM.

Clippinger, J. H. (2017). *Why Self-Sovereignty Matters*. https://idcubed.org/

Courtois, N. T., & Bahack, L. (2014). *On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency*. arXiv preprint arXiv:1402.1718.

Dua, G., Gautam, N., Sharma, D., & Arora, A. (2013). *Replay Attack Prevention in Kerberos Authentication Protocol Using Triple Password*. CoRR abs/1304.3550.

Ekblaw A, Azaria A, Halamka JD. Lippman A. A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. White Paper. 2016. http://dci.mit.edu/assets/papers/eckblaw.pdf

Hardjono, T., & Pentland, A. S. (2016). *Verifiable Anonymous Identities and Access Control in Permissioned Blockchains*. http://www.venturecanvas.com/wp-content/uploads/2016/04/506b6-chainanchor-identities-04172016.pdf

Harris, P. (2016). *Connected Patient Report*. Salesforce Research.

Intel. (2013). *Intel Software Guard Extensions Programming Reference*. https://software.intel.com/sites/default/files/managed/48/88/329298-002.pdf

Kim, M., Song, S., & Jun, M.-S. (2016). A Study of Block Chain-Based Peer-to-Peer Energy Loan Service in Smart Grid Environments. *Advanced Science Letters, 22*(9), 2543–2546.

Kish, L. J., & Topol, E. J. (2015). Unpatients-Why Patients Should Own Their Medical Data. *Nature Biotechnology, 33*(9), 921–924.

Lee, B., & Lee, J.-H. (2017). Blockchain-Based Secure Firmware Update for Embedded Devices in an Internet of Things Environment. *The Journal of Supercomputing, 73*(3), 1152–1167.

Liang, X., Zhao, J., Shetty, S., & Li, D. (2017a). Towards Data Assurance and Resilience in IoT Using Blockchain. In *IEEE Military Communications Conference (MILCOM)*. Baltimore, pp. 261–266.

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017b). Provchain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. In *International Symposium on Cluster, Cloud and Grid Computing*. IEEE/ACM Baltimore, MD.

Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017c). Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications. In *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)* (pp. 1–5), Montreal, QC.

Matt, M. (2015). *Tip of the Iceberg: FDA's Alert to Unplug Hospira's Drug Infusion Pumps from Clinical Networks*. https://researchcenter.paloaltonetworks.com/2015/08/tip-of-the-iceberg-fdas-alert-to-unplug-hospiras-drug-infusion-pumps-from-clinical-networks/

McKeen, F., Alexandrovich, I., Berenzon, A., Rozas, C. V., Shafi, H., Shanbhogue, V., & Savagaonkar, U. R. (2013). Innovative Instructions and Software Model for Isolated Execution. In *Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy (HASP '13)*. New York: ACM.

Merkle, R. C. (1980). Protocols for Public Key Cryptosystems. In *Security and Privacy, 1980 IEEE Symposium on* (pp. 122–122). IEEE.

National Institute for Standards and Technology (NIST) and Office of the National Coordinator for Health IT. (2016). *Use of Blockchain in Healthcare and Research Workshop*. https://oncprojectracking.healthit.gov/wiki/display/TechLabI/Use+of+Blockchain+in+Healthcare+and+Research+Workshop

Paquin, C. (2013). *U-prove Technology Overview v1.1 (Revision 2)*. https://www.microsoft.com/en-us/research/publication/u-prove-technology-overview-v1-1-revision-2/

Paquin, C., & Zaverucha, G. (2011). *U-prove Cryptographic Specification v1. 1*. Technical Report, Microsoft Corporation.

Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016). *A Blockchain-Based Approach to Health Information Exchange Networks*. https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf

Rosenfeld, M. (2011). *Analysis of Bitcoin Pooled Mining Reward Systems*. arXiv preprint arXiv:1112.4980.

Sarangdhar, N., Nemiroff, D., Smith, N., Brickell, E., & Li, J. (2016). *Trusted Platform Module Certification and Attestation Utilizing an Anonymous Key System*. https://www.google.com/patents/US20160142212. uS Patent App. 14/542,491.

Thierer, A. D. (2014). The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation. *Richmond Journal of Law & Technology, 21*, 1.

Tierion. (2016). *Tierion Api*. https://tierion.com/app/api

Wayne, V., Jason, B., & Shawn, W. (2016). *Chainpoint: A Scalable Protocol for Anchoring Data in the Blockchain and Generating Blockchain Receipts*. http://www.chainpoint.org/

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *Journal of Medical Systems, 40*(10), 218. https://doi.org/10.1007/s10916-016-0574-6.

Zhang, J., Xue, N., & Huang, X. (2016). A Secure System for Pervasive Social Network-Based Healthcare. *IEEE Access, 4*, 9239–9250.

Part II

Sustainability

6

Toward a Sustainable Circular Economy Powered by Community-Based Incentive Systems

Marcus M. Dapp

Interdependent Crises, Complexity, and a New Approach

The term digital revolution refers to the profound changes brought about by digital information and communication technologies (ICT) in the twentieth century and their gradual convergence at the beginning of the twenty-first century. Digitization has brought a steep increase in the connectivity of our societies and economies through massively reduced transaction costs. This connectivity has enabled large corporations to gradually develop into networks with global reach—internally, with transnational subsidiaries, and externally, with supply chains spanning the globe. This increased interdependence between businesses has led to the mega trend we call "globalization".

The author acknowledges funding by the Swiss National Foundation for EU FLAG ERA project *FuturICT2.eu* under grant number 170226.

M. M. Dapp (✉)
Computational Social Science, ETH Zürich, Zürich, Switzerland
e-mail: marcus.dapp@gess.ethz.ch

H. Treiblmaier, R. Beck (eds.), *Business Transformation through Blockchain*,
https://doi.org/10.1007/978-3-319-99058-3_6

Globalization, deregulation, and ICT have brought much progress and better standards of living to many people and countries. However, this development seems to come at a price that becomes increasingly palpable. Non-sustainability is the biggest global challenge humanity is facing at the beginning of the twenty-first century. In a global survey among business and governmental leaders, *environmental risks*—extreme weather events, natural disasters, failure to mitigate and adapt to climate change, biodiversity loss and ecosystem collapse, as well as man-made natural disasters—have been identified as the risk cluster which would have the largest impact as well as the highest likelihood (World Economic Forum 2018).

Today, our societies and economies are much more interconnected than any previous time in history. This high degree of connectedness within and between corporations and institutions has created a large web of complex systems. These networks are much harder to control than the societies and economies of the twentieth century, which were smaller, more isolated, and often confined to the nation state. While the economy went global without much restriction, a concerted global effort to regulate it is nearly non-existent. The unrestricted operation of globalized industries has created a series of ecological crises that have the potential to remove the very foundations the global economy continues to rely on.

Since 2008, we also are fully aware that the dominant economic system is not invulnerable to turbulence and crashes. The survey mentioned above identified a variety of *economic risks*—fiscal crises, un-/underemployment, asset bubbles in a major economy, failure of critical infrastructure, failure of a financial mechanism or institution, energy price shocks, illicit trade, deflation, and unmanaged inflation—that are considered to be likely and have a lower, but still significant impact (World Economic Forum 2018).

The interdependence and thus complexity of these challenges is unprecedented. The "too big to fail" debate has shown that the economic power and reach of large corporations and banks are exceeding the capacity of many nation states to contain economic mishaps. Joint efforts by policy makers, regulators and governments are underway:

- The United Nations has developed the "Sustainable Development Goals" framework that covers a broad range of social and economic development issues, including poverty, hunger, health, education, climate change, gender equality, water, sanitation, energy, environment and social justice (United Nations 2015).

- European nations implemented a series of financial support measures (European Financial Stability Facility and European Stability Mechanism) to counter the European debt crisis. The European Central Bank is repurchasing bonds at a large scale, also known as quantitative easing ("European Debt Crisis" 2018)
- The Basel Committee on Banking Supervision is implementing the third installment of the Basel Accord ("Basel III"), after several extensions, in 2019. The accord is a global, voluntary regulatory framework on bank capital adequacy, stress testing, and market liquidity risk, developed in response to the deficiencies in financial regulation revealed by the financial crisis of 2007–08 ("Basel III" 2018).

The failure of regulators to keep up and create effective global frameworks to which all nations and actors are accountable is leading to social tensions and even crises in some parts of the world. *Societal risks*—such as water crises, food crises, large-scale involuntary migration, spread of infectious diseases, and profound social instability—are thought to have a similar impact as environmental risks (World Economic Forum 2018).

As a consequence, general public trust in business and political leaders is eroding in many countries. We can find a variety of examples of the *geopolitical risks* identified by the World Economic Forum (2018) such as interstate conflict, failure of national governance, terrorist attacks, failure of regional or global governance, and state collapse or crisis in a variety of countries on all continents.

The question is: Against this backdrop, how should we tackle this web of interdependent complex crises and address some of the fundamental challenges humanity faces—such as climate change? The sustainability challenges we are witnessing are rooted in a misaligned incentive system that does not take into account the ecological and human capital which the economic system depends upon and needs for its very existence.

In order to think of new solutions, some of the key assumptions of standard economics need to be scrutinized because they insufficiently describe and model the complex reality we live in. Conventional economics makes several assumptions that seem to be overly simplistic (Ball and Helbing 2012, chap. 7; Helbing 2013):

- Interpreting the economy as an equilibrium system that, through supply and demand, would always find a perfect price balance, as long as no outside influences interfere. As a consequence, forecasts underrate the potential for major fluctuations such as bubbles and crashes. The underlying assumption of a closed, linear model does not quite reflect our world as an open, non-linear system.
- The orthodox model imagines economic agents as independent, endowed with all necessary information at all times, and always acting rationally to maximize their own "utility". This conceptualization has been relaxed, using concepts such as bounded rationality and information asymmetry. However, this new branch of behavioral economics only illustrates the stark contrast between old and new economic models.
- By assuming agents interact solely on the basis of price information, feedback loops and interdependent behavior are ignored. While the press often speculates that herd behavior may create fluctuations, bubbles, or crashes, they are not part of conventional economic models.

One of the core problems is that today's economic system is creating systemic market failures in the form of so-called market externalities. They are considered external precisely because they are not contained in the models of conventional economics (see above). As a consequence, today's economy always needs external checks and safeguards; a role traditionally carried out by policymakers and regulators. Classic governmental instruments include subsidies to foster positive externalities and taxation to curb negative externalities.

However, while the economy went global without much restraint in recent decades, governments have been largely uneffective in guiding and framing the globalized economies. One of the reasons is that policymaking is still mainly confined to national preferences and boundaries. Recent leaks demonstrate that corporations play on legal gaps and tax haven constructs around the world, which indicates that it is a challenge for competing nations to agree on consistent, global policy.

One solution would be to harmonize regulation globally in important domains like environmental protection, CO_2 emissions, and so on. This has been attempted through initiatives like CO_2 emission trading (Kyoto and Paris Agreements), although the results clearly lag behind the expectations. One of the core reasons is that the social, cultural and economic realities of nations vary significantly, leading to a broad spectrum of national interests and motives. Diplomatic efforts to align these interests are time-consuming and prone to failure. In many ways, the Paris Agreement is an example that can be considered a huge success—although the stability of strong commitments and backing is not self-evident (e.g., the position of the US administration).

It is safe to assume that any approach relying on globally harmonized regulation to tackle the interconnected challenges described above will take a long time (which we may not have) and often lead to agreements of the lowest common denominator. The second reason to be skeptical lies in the nature of the approach: financial (dis)incentives like taxes and subsidies only affect one parameter of the complex system—national currency. We suggest a more robust system of finer granularity is better suited to steer our economies and societies.

In order to move toward such an alternative system, we start from a few key questions:

- *What if we could measure externalities much more broadly and deeply—and automatically using ICT?*
- *What if we could price externalities that have not been priced before and make them visible?*
- *What if we could expose such priced externalities to new (dis)incentive systems (i.e. markets)?*

Our proposed approach is to extend the economic system itself by systematically including externalities and making them tradable on markets. We are proposing to address societal challenges using a new governance paradigm made possible by innovative technology. Using insights from complexity science, we propose a new system which would motivate people to act more sustainably, while remaining decentralized, self-organizing, multi-layered, and circular. With the advent of recent breakthroughs in digital technology—mainly blockchain technology, but also the “Internet of Things”, and artificial intelligence—it is possible to create such decentralized incentive systems (Kleineberg and Helbing 2016).

Blockchain (BC) technology allows data streams that quantify externalities to be recorded and tracked in a trustworthy manner. It also allows these data streams to be valued and traded (“priced externalities”). This would allow to create decentralized markets for externalities which currently do not exist. In addition, these data streams and markets would not need a governance structure controlled by institutions like central banks. That is because BC technology allows anyone to create monetary systems accessible by anyone on the Internet. In contrast to fiat currencies, anyone on the Internet can obtain and use Bitcoin, for example. “Economic and monetary management will be overhauled by new systems anchored in digital currencies and the blockchain, making traditional pricing mechanisms and exchange rate systems less relevant” (World Economic Forum 2015, p. 35).

The sensory networks of the Internet of Things (IoT) allow measuring real-life phenomena representing externalities. These phenomena could be tracked by public machine sensor networks like those used to measure emissions, noise, traffic, etc. run by city administrations in combination with human sensor networks based on mobile phones and other devices (e.g. hardware kits like Raspberry Pi. At a later stage, personal artificial intelligence (AI) tools could help to analyze the various streams of data on externalities and represent them as cryptocurrency. The tools could create behavioral recommendations for users on how to manage their wallets in the best way.

Cryptoeconomic designs will power incentive systems on a variety of platforms that focus on different externalities. These platforms will gradually connect to create new “token economies”, whereby tokens circulate within and between the platforms. This will create new sources of income and new ways of mitigating unsustainable activities on a large scale. Moreover, these token economies will have their own built-in governance systems.

In the following section, we describe the core concepts and processes of such a design and discuss some architectural considerations.

Core Concepts

We propose a decentralized economic system that combines a series of distinct concepts and processes. The broad strokes are presented here as an overview while the details will be left for later stages of research.

Blockchain technology makes it possible to design and create digital currencies to allow local communities to create and design their own money. That is significant for two reasons. Firstly, it allows communities to create currencies and design economic policies ("cryptoeconomics") that are tailored to their local needs. A centrally issued single currency following a single economic policy cannot provide such a level of adaptiveness. Therefore, the European Central Bank continues to struggle to develop a single economic policy which is adequate for the heterogeneous EU market: its instruments are essentially limited to money supply, interest rates, and bonds. Secondly, bottom-up cryptocurrencies will over time democratize money supply and money governance. Traditionally, a small group of managers in central banks (that are often privately owned and not democratically legitimized) decide on the entirety of the monetary system, from money supply, to fractional-reserve standards, to interest rates. The consequences of its decisions affect very large populations (e.g. 330 m US citizens in case of the FED, 510 m EU28 citizens in case of the ECB).

Bearing in mind the complexity challenges discussed in the previous section, it is fair to ask whether a small group of people facing bounded rationality, information asymmetries, and a limited arsenal of instruments is in fact able to steer such large complex economies—or whether new, more participatory, self-organizing systems would bring more benefit to a larger number. This section makes a proposal based on the latter contention.

Incentive System

One of the core concepts is to create an incentive (and feedback) system that is multi-dimensional, multi-layered and based on cryptocurrencies designed to promote sustainable behavior.

Table 6.1 Examples for market externalities

Positive externalities	Negative externalities
Education, cooperation, health, community service, reuse, recycling, biodiversity, care-taking, CO_2 capture, etc.	CO_2 and other emissions, pollution, disease spread, waste of food/energy, deforestation, garbage, noise, etc.

Cryptocurrencies The basis of the design is that agents in the system receive money for sustainable behavior when they create positive and/or reduce negative externalities in their area of influence. Externalities, i.e. effects on actors who have not been part of the original transaction, cover a broad spectrum (c.f. Table 6.1). If the side effects of a market transaction are beneficial to a group of bystanders, the externality is called positive; whereas if they are harmful, it is called negative. For example: polluting the environment while producing oil is a negative externality if nobody in the transaction (neither the oil-producing corporation nor its clients) covers the cost of cleaning up the environment (c.f. oilspillmonitor.ng for empirical data about this problem).

Externalities are positive if a transaction creates beneficial spillover effects for others. For example, reducing CO_2 emissions anywhere on the globe helps everybody on the globe—no matter who actively contributed to the reduction. This lack of incentive to contribute is known as a collective action or free-rider problem and is one of the reasons why global climate agreements are so hard to accomplish.

Terminology: Blockchain, Cryptocurrency, Altcoins, Smart Contracts, DApps, DAO

A blockchain is a distributed data structure that is collectively written and maintained by a network through a distributed consensus mechanism. In 2008, Bitcoin was the first application—offering digital cash or "cryptocurrency" to its users—using blockchain technology and an economic consensus mechanism called proof-of-work. Copycat projects have created a myriad of alternative cryptocurrencies ("altcoins") and several new exchanges started to allow users to trade cryptocurrencies (see coinmarketcap.com for an overview). Regulation across the world is patchy, ranging from innovative, supportive approaches in some jurisdictions to flat out bans in others.

The introduction of smart contracts by the Ethereum project in 2013 led to the second phase of evolution. Smart contracts are code that is deployed to a blockchain to be immutable and self-executing. Smart contracts can interact with other smart contracts, websites and humans allowing for the emergence of programmable value transfer networks ("Internet of Value"). Such decentralized applications ("DApps") sit one layer above the blockchain and make use of its features. Many DApps explore this new space to create domain specific applications ranging from insurance to social networks, supply chain provenance, prediction markets or voting.

Moving up the stack, the third phase of evolution has started with "TheDAO" project in 2016. A Decentralized Autonomous Organization is a network based on a set of interacting smart contracts that not only perform functions of a certain application domain but that also incorporate functionality to mimic an organizational structure and its governance—in a distributed way. The key problems to be solved are decision-making/voting, dispute resolution, joint funding schemes, and so on.

Across all phases, technology and governance pose the key challenges at the current stage of development. Fully decentralized approaches to technology are severely limited in scaling and throughput performance while the ambition to create democratic structures on top of the DApps poses a design challenge in its own right.

As of writing there are hundreds of distributed ledger projects actively exploring the space to experiment with different data structures (e.g. blockchains, directed acyclic graphs, hashgraphs), consensus algorithms (e.g. proof-of-work, proof-of-stake, Byzantine Fault Tolerance (BFT), etc.), different application domains (see above), and last but not least technical challenges ranging from closing security loopholes to experimenting with new approaches to increase performance.

Just like central banks or local currency schemes, the designers of this new money need to answer two key questions: How/For what will people receive cryptocurrencies, and how/for what will they be able to spend them? Generally, new coins are *received* for positive actions that strengthen the network and address externalities specific to that token. Instead of a debt-based IOU issuing scheme—as most fiat currencies use since the abandonment of the Bretton Woods gold standard in 1971—the currency will be based on the real-life "good" work of tackling an unsustainable externality (we may call this "proof-of-good-work"). Thus, it derives its value from the community that issues the currency—and accepts it in return. Two aspects are crucial: Firstly, the local community needs to create closed-loop systems in which the tokens issued can also be spent on things that users value. At the beginning, when there are only a few currencies, this will be harder than when numerous currencies are already established. Successful existing local currency projects offer a great deal of insight here. Secondly, issuing money for good work also means that agents are not required to exchange their own fiat currency into a cryptocurrency to participate in the system. Newly minted tokens will not be distributed to banks but directly to people for activity deemed beneficial to the community. Therefore, it is crucial that the community controls the supply and policy of the token and not banks. In this way, the new token economy can self-organize, develop in parallel to the existing financial systems, and function independently of them. An area we can learn much from, is game reward systems research.

The question of how people will *spend* their cryptocurrencies is closely related to the design of feedback mechanisms and closed loops in the system. The more closed circles the designers manage to create when devising the mechanisms of a new currency ("circular" economy), the easier it will circulate, and the easier it will be for people to not only earn but also spend tokens. As the system runs in parallel to existing fiat currencies, there is no immediate need to buy food and shelter with the new cryptocurrency. At the same time, people will spend tokens because they want other positive externalities like clean water, healthy food, education, etc.

Multiple Dimensions Contrary to today's economic system, agents will make use of a variety of currencies that represent classes or types of externalities. People do not use one single currency, but many: each currency represents a type of externality and acts as a signal on the market for externalities. These signals will make preferences and priorities in the demand and supply of externalities to a greater extent visible than in today's markets. In addition, agents will be able to actively participate by trading the different currencies/externalities. Although not quite the same because it is not created from the bottom up, the closest existing analogy the markets for CO_2 emission certificates.

Multiple Layers In most cases, local communities (e.g. a city) will issue a currency according to the type and scope of the externality they want to address. However, others like international bodies (e.g. the United Nations or the European Union) can do the same. For example, instead of today's distribution scheme, the United Nations could issue tokens equivalent to the budget allocated to climate mitigation and distribute them to communities in return for credible (cryptographic) proof that a certain amount of CO_2 was permanently captured. The support would be direct, transparent, accountable, and more effective than today's processes as the success metric would already be built-in. As long as a token is addressing an externality, any group should be able to create and use it. However, not being a local community, the United Nations would also offer a compelling way for people to use the tokens they receive. At the beginning, it would be possible to exchange them for fiat currency. In the long run, however, the tokens would need to have intrinsic value.

Valuation How is the value of such cryptocurrencies determined or influenced? The "mudflation" phenomenon in computer games (the unintended inflation, i.e. devaluation, of virtual tokens issued in-game without any limits) shows that simply creating and issuing tokens will not work. The challenge is to get the economic policy right. At the same time, programmable money allows a much more fine-grained control of a monetary system: token supply can be capped or non-capped leading to deflationary or inflationary currency; tokens can be destroyed ("burnt") and removed from the supply; demurrage, expiration, and many more characteristics can be made inherent properties of a token. However, as these possibilities did not exist before, it is hard to predict the potential of large-scale, bottom-up, open cryptocurrency systems, that are democratically governed and accessible to anyone.

Convertibility A second aspect is the convertibility of cryptocurrencies. Generally, people should be able to exchange from any currency to any currency to make the most use of their tokens. This can either be accomplished by a mechanism that allows direct conversions or by using a "meta currency" that allows the exchange between different currencies. In a 2010 policy paper analyzing the imperfections of the existing international monetary system (e.g. over-representation of the USD), the International Monetary Fund presented several options to increase stability (Moghadam 2010).

One option was *to create a sui generis global currency*—called Bancor in honor of economist John Maynard Keynes—to replace today's system of Special Drawing Rights, as either a common or a parallel currency. A similar conceivable approach would be to devise a system of externality-based coins in which conversions are done automatically through smart contracts. In fact, some blockchain projects are working on such conversion mechanisms (e.g. Bancor and Interledger, c.f. section on architecture).

Some conversions, however, may be detrimental to the overall goal of sustainability. Take the following hypothetical example: a project proposal involves burning down 10 km^2 of rain forest to build schools. If the cost-benefit estimates are done in one single currency, a result of both estimates being close may lead to a favorable judgment of the project. This approach presumes that the costs and benefits of having trees versus having schools are of comparable quality and can be balanced. This presumption ignores the fact that the rain forest will be gone, no matter how many schools are built. On the other side, if two different externality tokens representing CO_2 emissions and education were used, it would become transparent that building schools does not balance out the diminished capacity of the rain forest to capture CO_2 - the tokens represent two different dimensions. To discourage such transactions, they would need to cost more—not unlike the tax proposed by James Tobin to curb excessive foreign-exchange transactions.

Reputation Using programmable tokens in incentive systems enables the creation of metrics akin to reputation. For example, maintaining a consistently above-average balance of "CO_2 coins" would indicate that an individual has made a credible effort to keep his/her ecological footprint low (if the user decides to make this information public). Several externality measurements combined would gradually form a rich user profile with some degree of reliability and accuracy. Under the control of the user, such profiles could be used for job interviews, political campaigns, insurance policies, etc.

Token Economy

Token and Tokenization A token is a quantified unit of value, generic and fungible. Most blockchain projects use a token for implementing their own cryptoeconomics. In the simplest case, the token is the cryptocurrency itself, like bitcoins on the Bitcoin network. On Ethereum, ether is used as "gas" to execute smart contracts on the platform. Ethereum-based decentralized applications (so-called DApps) typically create their own tokens specific to the functionality. Standards are emerging to define common characteristics to make these tokens interoperable (e.g. ERC20, ERC777).

Typically, new tokens are created in one of two ways. Either, the whole token supply is created in advance ("pre-mined") with the option to sell to future users via a token-sale mechanism like an initial coin offering (ICO). Or, the tokens are created regularly while the platform is being used. Sometimes, these two approaches are combined. In addition, tokens can operate in different ways, some examples include: payments (like normal currency), stakes (for users to get "skin in the game"), or creation/destruction schemes ("burning" tokens usually renders them unusable, at least temporarily).

A related concept is tokenization. Tokenization is the act of creating a set of tokens to digitally represent an asset or a right. For example, a physical object like a house, car, or a natural resource (such as a forest or a field) can be tokenized to render a fine-grained digital representation of the physical object's value. This enables the resource to be managed multilaterally and maintained collectively.

There are different ways to conceptualize and tokenize an externality on a blockchain: as a currency, asset or something else entirely. In the first case, the logic of a *currency* is straightforward: users receive tokens by doing something valuable and spend tokens (pay) for something they value. If a currency logic is adopted, it creates a market where externalities are traded. Another way to model externalities is as an asset. For instance, the community selects a user to take care of a piece of forest with the aim to gradually grow the forest or limit deforestation. In this way, the person acts as a custodian of the forest. One form of compensation would involve rewarding the user for maintaining or expanding the forest over time. The financial logic is different to a currency: The person has a stake in the forest and could not as easily switch to another externality as would be the case if the user possessed a currency convertible on markets. An even more sophisticated approach would be to integrate this logic into a decentralized autonomous organization (DAO) such that the foresst would own itself and manage its own tokens through smart contracts (c.f. the art project "terra0"). Such a technocratic governance framework could be designed to directly reflect community rules to collectively manage externalities (Ostrom 2015), rules that are hard to implement using only currency or asset concepts.

What Is Cryptoeconomics?

No commonly agreed definitions exist yet but following Vitalik Buterin one can say that cryptoeconomics is the combination of cryptographic proofs of past events and economic incentives to encourage future events inside a blockchain system. On the cryptography side, components used center mainly around consensus algorithms, digital signatures, and hash functions, plus more recently, zero-knowledge proofs, multi-party computation and homomorphic encryption. On the economy side, things are more complex and an active area of research involving game theory, mechanism design, and network economics.

Cryptoeconomics Cryptoeconomic designs will power the incentive systems established around local externalities. Gradually, as more of these currencies come into existence, they will connect to create token economies, whereby tokens will circulate in and between the currencies. Such currency networks, technically accessible by anyone (including "the unbanked"), can represent new sources of income and new ways of mitigating unsustainable activities on a larger scale. Moreover, these token economies will have their own built-in systems of governance.

Two notable blockchain projects that are actively experimenting with a variety of complex, multi-coin cryptoeconomic mechanisms may serve as illustrative examples. *Steemit* is a blogging platform similar to Medium or Wordpress that rewards users for writing and curating content. No central entity monitors what is published and once published, the history of posts is immutable. The sophisticated incentive mechanism uses three different tokens that model a checking account, a savings account, and a currency account (to USD). New tokens are issued daily to reward contributors who post new content, and vote and comment on existing content. *Akasha*, the second example, is a social network "dedicated to freedom of expression, access to information, and privacy". The incentive mechanism enables the base currency to be exchanged for self-regenerating

“Mana” used to publish, vote, comment, etc. Voting burns Mana, which the authors can collect and reconvert to the base currency. Whereas the savings account in Steemit serves as a form of reputation, Akasha uses a fourth currency called Karma that builds based on the burning on Mana. Both these examples show that the power of blockchain technology goes beyond mimicking fiat currencies in a secure digital way; *its real power lies in the ability to define complex rules governing how a currency should operate*—an ability that fiat currencies are unable to provide.

The key to the success of such initiatives is that local communities can design and create currencies and incentives according to their local needs, tokenize what is agreed to be relevant, and collectively track the parameters in question. A key question is how to fairly distribute tokens at the beginning of the process. One interesting idea in that context is that individuals could issue their *own* personal currency which would gain value through a network of mutual acceptance, an idea pursued for example by the Circles project (https://joincircles.net/).

Finally, such a system creates decentralized markets for externalities and thus contributes to solving the problem of externalities being “outside the economy”. It also constitutes a new source of income and could potentially constitute a contribution to a universal basic income scheme.

Token Economy and Interoperability Today, many blockchain projects create numerous DApps, each with their own tokens, cryptoeconomics, etc. This creates a heterogeneous landscape of DApps. The pressure to connect these DApps is already apparent and will increase over time. While the term “cryptoeconomics” describes incentive systems designed for and within a DApp, the term “token economy” describes the wider economy between different DApps. Although crypto investors can trade many cryptocurrencies and tokens today, a full-fledged token economy in which direct flows of tokens between different DApps creates more complex networks does not yet exist.

However, in order to usefully discuss token economies, a more fundamental problem needs to be solved first: Despite many public and private blockchains in existence today, inter-blockchain interoperability remains elusive. Assets on one blockchain generally cannot be moved to other chains and exchanging assets on different blockchains requires a centralized intermediary. Two projects that may serve as examples of how to address this challenge can be found in the technology section (Cøsmøs and Polkadot).

The goal would be to scale DApps to address different externalities in different regions of the world and then trade the externalities in order to cater to the various needs of people—that is, create a token economy.

Sensing Network

The function of the sensing network is to translate real world objects and actions into their digital representations. Several questions need to be addressed here: How is the validity of a digital representation ensured and then verified? How can users stay in control of their data and more concretely, how can they gain reputation from their data (and tokens) without compromising anonymity? Who controls the sensor networks?

Proof of Good Work We use the term "good work" to describe activity an agent does to create a positive or reduce a negative externality. The challenge is to translate this real-life event into a trusted digital representation in the form of a certain amount of tokens which measures the scope of externality.

To rightfully reward tokens, the community needs a guarantee that the good work has indeed taken place and that the data once collected is protected from manipulation before it enters the immutable blockchain. Two types of proof are possible: (a) "oracles" are trusted data sources outside of blockchains and constitute one of the key challenges for existing blockchain projects. The current solutions range from trusted hardware in sensors, to encrypted transmissions between sensors and the blockchain. (b) What can be done in cases where no adequate hardware exists? For example, it would be quite easy for an actor to fake a "selfie" with ten trees which he/she ostensibly planted (to increase CO_2 capture). Here, a concept of "social proof" or "human oracles" may be helpful: members of the community mutually verify and attest that a certain activity took place. Aside from the question of scalability, it is crucial to devise a cryptoeconomic design that gives incentives to the verifiers to participate and be honest (no collusion, etc.). Blockchain projects on voting and dispute resolution are working on such mechanisms.

Identity and Privacy In order to create an independent system that works globally without external infrastructure or governance, the question of identity also needs to be addressed. One interesting concept discussed in this context is self-sovereign identity. Instead of a government issuing a state-owned ID card, citizens use a decentralized identity service which they control. Users would make claims and provide proof of their identity (name, age, place of birth) that other users would corroborate (attest). Just as people keep passports, birth certificates, bank records, and important bills on paper in their private homes, self-sovereign identity would replicate this approach digitally. Suitable cryptoeconomic designs are needed to keep everyone honest and interested in strengthening each other's identity (Abraham 2017).

A related question is how an incentive system which will invariably make use of reputational metrics can be reconciled with the desire to keep users' personal and externality data private (or anonymous). This is an active area of research. One interesting concept is that of zero-knowledge proofs and multi-party computation which allow one party to prove their knowledge of something to another party without actually revealing this knowledge. For example, a user would be able to show that they own a piece of externality data without the need to reveal the content of that data (e.g. their CO_2 footprint).

Mesh Networks Over time, the Internet became strongly dependent on centralized industries (ranging from Internet service and domain names to social networks and search engines) mainly because of the client-server logic embedded in its design. In order for the IoT to be less dependent on industry, communities could run mesh networks of sensors alongside the existing infrastructure (e.g., https://www.thethingsnetwork.org/).

Community-run decentralized networks are desirable for various reasons: firstly, they prevent misaligned incentive systems whereby personal data is sold between corporations as a business model; secondly, they make the network more resilient as data is not concentrated in a few nodes driven by a data-collection business model; and, thirdly, they enable diverse data sources that may not have a viable business model (e.g. data curation projects like Wikipedia or Open Street Map).

This approach can be gradually expanded from local communities, to regions, and finally to continents and the entire globe, incrementally building a “digital nervous network” to benefit all citizens, with fewer dependencies and more democratic oversight (Helbing and Pournaras 2015).

Governance

Reijers et al. (2016) provide a comparative analysis of the new governance models enabled by blockchain technology which draw on the social contract theories of Hobbes, Rousseau, and Rawls. A system as decentralized as the one proposed needs a similar governance approach based on direct democratic and participatory principles like community decision-making, majority rule, voting, dispute resolution, etc. The core design principles, decentralization and subsidiarity, are complementary.

Subsidiarity Subsidiarity is a principle of social organization that holds that social and political issues should be dealt with at the most immediate (local) level. Being an opt-in system, communities cannot give unfair advantage to those who join first.

Decentralization As control at local level affects people greatly in their daily lives, it is important to prevent single actors or stakeholders from dominating. In other words, the system needs to have balanced democratic legitimation from the bottom up.

Transparent Technology The democratic control paradigm needs to extend to the technical realm: changing the parameters of the incentive system, controlling the IoT networks, designing the AI, and so on need to be transparent processes subject to democratic oversight. This requires inter alia that all technical artifacts, software, algorithms, and APIs need to be open source for public review.

Glocalization There are two key governance processes: creating and/or modifying local token designs and managing the registry of all tokens and setting parameters on a global level. The proposed approach acknowledges the concurrence of the growing importance of the continental and global realm on the one hand (c.f. discussion on globalization at the beginning) and the salience of local and regional governance (cities, communities) on the other. Governance at the local level, although not necessarily democratic at all times, has a long tradition in many cities around the world. Personal relationships supported by incentive systems as described above should make it possible to establish externality markets with local/regional scope if adequate mechanisms are in place to settle disputes to ensure that "good work" is correctly recorded.

In order to ensure that local needs are indeed addressed and the interests of the community safeguarded, it is important that the community collectively has an influence on the pricing mechanism. That is not to say that prices are defined by committee, but that priorities for certain types of externality can be democratically determined and influence the pricing mechanism. While both halves of a city separated by a river share a common interest in a clean river, they may have different priorities regarding noise or littering and thus, they may derive different pricing mechanisms (or even tokens).

While the pressure to coordinate globally may be lessened in a decentralized system built on community self-organization, global coordination remains the more difficult governance task. We argue that any global mechanism must be democratically legitimized to be inclusive, accepted, and hence effective. Monbiot (2004) presents several ideas concerning how a democratic world parliament could be devised that are compatible with the presented approach. In addition, we argue for multi-stakeholder representation in global governance: besides local and regional governments, and business, science and civil society also need to be represented. Representatives of all four groups would be elected by their constituencies and would share decision-making power equally. Their deliberations are public and they should strive for consensus on most questions (with no veto power to block important decisions).

Evaluating such novel governance proposals is challenging, but today's technologies allow us to experiment with massive online deliberation spaces (Helbing and Klauser 2016) and liquid democracy/delegated voting (Helbing and Pournaras 2015) in order to bring enriched expertise to bear on governance and make the decision-making process more transparent and resistant to manipulation.

Architecture and Technologies

To be able to implement the concepts presented above, a conceptual understanding of the core processes and an overview of the technological landscape is needed in order to devise a technological architecture. Figure 6.1 depicts the core process architecture on a high level. From right to left, the externality data is sensed and stored. The first stage of the cryptoeconomic design involves verifying the correctness of data (oracles/social proofs) and generating digital tokens to represent the data. They are kept in the user's wallet until he/she decides to use them. The token-economy design encompasses the pricing process and trading on decentralized markets.

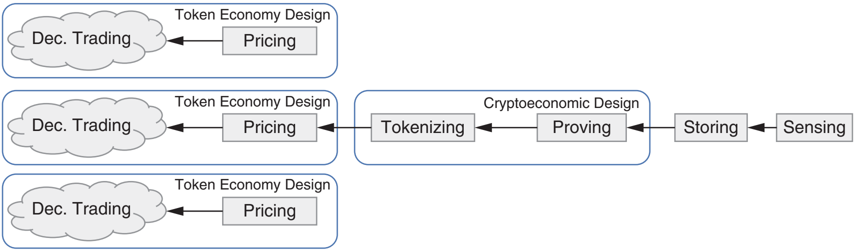


Fig. 6.1 Overview of core processes from data sensing to token trading

This overview cannot go into a detailed technological discussion. However, to illustrate the diversity of blockchain projects, we provide a brief overview of selected blockchain projects that support one or more of the core process requirements. In addition to the core processes described in Fig. 6.1, we add two more aspects—governance and interoperability—as crucial elements of a working system.

All project information in the table is summarized from the respective project website and/or white paper (Table 6.2).

Table 6.2 Example projects addressing the requirements of individual core processes

Core process	Description and example projects
Sensing	*During sensing, users can collect/crowd-source data on externalities using sensor infrastructure or their own hardware sensors, for example their mobile devices.* **IOTA** (https://iota.org/) is a blockless distributed ledger ("Tangle") that makes feeless value transfers possible. The Tangle makes consensus an intrinsic part of the system, leading to a decentralized and self-regulating peer-to-peer network that is lightweight with instant consensus on new transactions. **Streamr** (https://www.streamr.com/) tokenizes streaming data to enable machines and humans to trade it on a decentralized market. Streamr offers a visual programming environment to create data-driven DApps. **AIRA** (https://aira.life/) is working on a standard to facilitate human–robot and robot–robot economic interactions using liability smart contracts. AIRA makes it possible to connect a variety of different robots, and trade sensor data between them, etc. with the final goal of establishing fully automated enterprises in a "robot economy"

(*continued*)

Table 6.2 (continued)

Core process	Description and example projects
Storing	*Users can decide to store the sensor data locally, or with a trusted decentralized cloud storage provider of their choice, or register the data as streaming data (no storage). In addition, users can decide on the (non)encryption of the raw data.* **Datum** (https://datum.org/) is a decentralized and distributed high performance NoSQL database backed by a blockchain ledger. This technology allows anyone to securely and anonymously backup structured data from social networks, wearables, smart homes, and other IoT devices. **SIA** (https://sia.tech/) and **Filecoin** (https://filecoin.io/) make the free hard drive capacity of users available to create a storage network powered by cryptocurrency (and smart contracts). Participants are incentivized to store other user's files and users pay to store their files. **BigChainDB** (https://www.bigchaindb.com) is a Big Data distributed database augmented with blockchain characteristics to enable decentralized control, immutability, rich permissioning, transfer of digital assets, and control via a federation of voting nodes
Proving	*Users can declare what quantity of externality* (e.g. *10 trees planted) a piece of data represents. Users then register their data on the blockchain after passing the "proof-of-good-work" verification. This can be achieved either by proving that trusted hardware was used, or by using a social proof mechanism offered by the system.* **Oraclize** (http://www.oraclize.it/) acts as a data carrier, a reliable connection between Web APIs and a DApp. Oraclize's own "good behavior" is enforced by cryptographic proofs. **Gnosis** (https://gnosis.pm/) and **Augur** (http://www.augur.net/) are decentralized, peer-to-peer oracle and prediction market platforms. They allow users to create prediction markets on the outcome of any future event, or viewed differently, to establish decentralized oracles powered by humans

(*continued*)

Table 6.2 (continued)

Core process	Description and example projects
Tokenizing	*The system translates the quantified data into a tokenized representation based on the economic policy devised by the community. Users receive the tokens into their wallets and can start using them.* **District0x** (https://district0x.io/). Districts are marketplaces and communities that exist as DAOs (with their own token) on the district0x network. All districts possess some core functionalities like posting/listing, searching, ranking/reputation, and invoicing and can be extended with plugins. The creation of a district establishes an accompanying Aragon entity (see below), where all of the district's governance and decision-making processes are executed. Comparable projects are **Colony** (https://colony.io/), where districts are called colonies, and **Giveth** (https://giveth.io/), which targets altruistic, non-profit organizations. In addition, **Bancor** (https://about.bancor.network/) allows users to convert between any two tokens, with no counterparty, at an automatically calculated price, thanks to built-in liquidity. The Bancor protocol is a standard for ERC20 tokens that allows smart contracts to connect to a liquidity network, enabling continuous on-chain liquidity throughout the network, without needing to match buyers and sellers

(*continued*)

Table 6.2 (continued)

Core process	Description and example projects
Pricing/trading	*When users decide they want to actively spend/use their tokens, they join a decentralized market. A price is determined based on the community's economic policy for this externality and its current collective pricing preferences as well as the demand/supply on the respective market.* **Swarm.city** (https://swarm.city/) is a decentralized marketplace with a built-in contextual reputation system. It allows people to communicate and transact value using context-specific marketplaces ("hashtags"), and form communities ("hives") to benefit from economies of scale and earn reputation collectively through marketplace transactions. **DEX** (https://www.dex.sg/) is a decentralized data exchange where people can monetize and share data. It offers data discovery, curation, verification, and an incentive system to provide better data as well as transactions. **Enigma** (https://enigma.co/) is a privacy protocol that enables encrypted, secret (smart) contracts that are able to handle sensitive data without moving off-chain, thus enabling privacy-preserving DApps
Governance	*The system requires governance mechanisms that work in decentralized, trust-less environments to provide mechanisms for dispute resolution and voting.* **Aragon** (https://aragon.one/) enables users to create and manage decentralized organizational structures to democratize governance and allow for borderless, permissionless and efficient value creation. **Kleros** (https://kleros.io/) is a decentralized arbitration protocol that uses game theory and crowd-sourcing to adjudicate claims in a fast, transparent and inexpensive way. It aims to help users resolve disputes quickly, securely, and affordably

(*continued*)

Table 6.2 (continued)

Core process	Description and example projects
Interoperability	*In order for the system to be extensible and scalable in the future, it requires mechanisms to connect different distributed ledger technologies in a coherent way to allow for cross-chain transactions.* **Cøsmøs** (https://cosmos.network/) is a permissionless decentralized network of independent parallel blockchains ("zones"), each powered by classical BFT consensus algorithms. The Inter-Blockchain Communication protocol keeps track of the number of tokens in each connected chain and manages inter-blockchain transfers. The end goal is to allow many sovereign and easy-to-develop blockchains to scale and interoperate with each other, creating an Internet of Blockchains. (The architecture is a more general application of the Bitcoin sidechains concept, using classic BFT and Proof-of-Stake algorithms, instead of proof-of-work.). **Polkadot** (https://polkadot.network/) is a heterogeneous multi-chain technology that follows a different approach. It is an inter-chain blockchain protocol which also enforces the order and the validity of the messages between the chains. It enables independent blockchains to exchange information and trust-free transactions via the Polkadot relay chain. **Interledger** (https://interledger.org/) is a protocol suite for sending payments across different chains in different currencies using connectors (like Internet routers), to route packets of money across independent payment networks. The open architecture and minimal protocol enable interoperability for any value transfer system

Implications

In this chapter, we argued for a new economic approach that has sustainability built into its core design by using cryptoeconomics based on blockchain technology to create incentive systems which encourage sustainable behavior. We presented in detail the core concepts and discussed some architectural and technological aspects. What are the implications of such a system?

Challenging Implications Firstly, the primary challenge is to develop a design framework/template which communities can easily use without being experts. A multidisciplinary approach is required to correctly design the initial parameters and incentives so that people will opt-in and start using the system. Relevant disciplines include behavioral economics, game theory, mechanism design, psychology, and sciences related to individual externalities (earth and life sciences). The parameters for the bootstrap phase may differ considerably to those of later phases when the system has stabilized and matured.

A related challenge is how to handle negative externalities. It is intuitive to design incentive systems to foster positive feedback loops to encourage users to engage in an activity deemed to be favorable by the community: "Do more good, get more tokens!" However, how can negative externalities that nobody wants to have in the first place be addressed without compromising the opt-in system? It is not attractive for a new user to start off with a negative balance of something like CO_2 or food waste. One approach to avoid negative balances could be to systematically find a positive externality to reward and counteract the negative one, but more research is needed here.

Secondly, the system needs to be as easy to use as possible for anyone. Receiving and using cryptocurrency today is very difficult for a layperson. Today's crypto wallets require users to take care of abstract things like private keys which are hard to understand and if they are lost, all funds will be inaccessible. This environment is not inviting for new users who wish to try the system out. Gamification, UX design and receiving new cryptocurrency without the need to exchange your own money can help, but a lot of experimentation is needed.

Thirdly, even if the first and second challenges are resolved, incentive systems rely on the assumption that humans will act because they receive tokens, and act more if they receive more tokens. However, this is not a given: the danger is that the existing intrinsic motivation to do good is not reduced by introducing tokens (extrinsic incentives) but magnified. People might only become active if they receive tokens for it. This problem already exists, but in a system where everybody participates, the effects may be much larger. Concepts based on reputation or charity may offer solutions, but more research in the context of cryptocurrencies is needed.

Beneficial Implications Firstly, the largest implications are for the economic system: open money—accessible to anyone, which can be earned by anyone, self-governed, and with potentially global reach—allows us to rethink the role of money and its governance in a much wider sense than hitherto. In addition, it allows us to run (public and transparent) experiments on economic policy at scale—something that was previously impossible. If successful, we should see a higher quality of life with less resource usage for more people. The possibility to earn income from positive externalities could contribute to a universal basic income scheme and thus tackle the anticipated unemployment caused by automation (Frey and Osborne 2017).

Secondly, from a complexity science perspective, such a bottom-up self-organized system provides many more control variables (in the form of tokens). This helps to make the overall economic system more robust and stable compared to a centrally defined economic policy based on a single currency. The policy implications could be that less policy control is needed to keep the economy in check, but this hypothesis needs testing.

Thirdly, if there were a fully digital system of currencies and underlying economic policies codified in software, it would make it much easier than today to run simulations of new policies before initiating real-life experiments. However even real-life experiments are conceivable: from A/B testing of the same currency exhibiting two different sets of characteristics and measuring the acceptance in the community, to releasing entire test currencies.

Fourthly, in addition to the potential of additional income sources for individuals, entire new business models for mission-driven non-profit organizations dedicated to sustainability are possible. Instead of donor-based models to finance projects which solve problems without a business model, such organizations could devise incentive systems and issue their own currency to address the issue.

In a distant future, when such a system may be fully deployed and matured and billions of people may earn and trade a multitude of externality tokens on a daily basis, using wallets with so many different tokens that personal digital assistants (run by AI) would need to suggest the optimal use of them. In such a future, as complex human interactions are matched by complex, multi-dimensional digital transactions optimized by personal AI systems, the actual notion of "money" as the (single) medium of exchange may slowly move into the background. A society with so many currencies that the individual cannot manage them manually anymore, might also be viewed as an essentially moneyless society.

References

Abraham, A. (2017). *Self-Sovereign Identity Whitepaper About the Concept of Self-Sovereign Identity Including Its Potential*. White Paper. E-Government Innovationszentrum Österreich. https://www.egiz.gv.at/files/download/Self-Sovereign-Identity-Whitepaper.pdf

Ball, P., & Helbing, D. (2012). *Why Society Is a Complex Matter: Meeting Twenty-First Century Challenges with a New Kind of Science*. Berlin: Springer.

Basel III. (2018). *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Basel_III&oldid=836576024

European Debt Crisis. (2018). *Wikipedia*. https://en.wikipedia.org/w/index.php?title=European_debt_crisis&oldid=833996513

Frey, C. B., & Osborne, M. A. (2017, January). The Future of Employment: How Susceptible Are Jobs to Computerisation? *Technological Forecasting and Social Change, 114*, 254–280. https://doi.org/10.1016/j.techfore.2016.08.019.

Helbing, D. (2013). Globally Networked Risks and How to Respond. *Nature, 497*(7447), 51–59. https://doi.org/10.1038/nature12047.

Helbing, D., & Klauser, S. (2016, August 4). How to Make Democracy Work in the Digital Age. *Huffington Post* (blog). https://www.huffingtonpost.com/entry/how-to-make-democracy-work-in-the-digital-age_us_57a2f488e4b0456cb7e17e0f

Helbing, D., & Pournaras, E. (2015). Society: Build Digital Democracy. *Nature News, 527*(7576), 33.

Kleineberg, K.-K., & Helbing, D. (2016). A 'Social Bitcoin' Could Sustain a Democratic Digital World. *The European Physical Journal Special Topics, 225*(17–18), 3231–3241.

Moghadam, R. (2010). *Reserve Accumulation and International Monetary Stability (Policy Papers)* (pp. 20–28). International Monetary Fund.

Monbiot, G. (2004). *The Age of Consent: A Manifesto for a New World Order*. London: Harper Perennial.

Ostrom, E. (2015). *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge: Cambridge University Press.

Reijers, W., O'Brolcháin, F., & Haynes, P. (2016). Governance in Blockchain Technologies & Social Contract Theories. *Ledger, 1*, 134–151. https://doi.org/10.5195/ledger.2016.62.

United Nations. (2015). *Transforming Our World: The 2030 Agenda for Sustainable Development A/RES/70/1*. https://sustainabledevelopment.un.org/post2015/transformingourworld/publication

World Economic Forum. (2015). *Deep Shift: Technology Tipping Points and Societal Impact*. World Economic Forum. http://weforum.org/reports/deep-shift-technology-tipping-points-and-societal-impact

World Economic Forum. (2018). Global Risks Landscape 2018. *The Global Risks Report 2018* (blog). http://wef.ch/2m7gWWx

7

Can Cryptocurrencies Help to Pave the Way to a More Sustainable Economy? Questioning the Economic Growth Paradigm

David Leonard and Horst Treiblmaier

The emergence of blockchain technology entails myriad implications for actors across a diverse set of industry sectors. Focusing on the blockchain as the data structure underlying cryptocurrencies, this chapter explores the potential of this technology to contribute to the broader societal goals of inter- and intra-generational equity commonly convened under the banner of sustainability. In particular, we examine how cryptocurrencies may alleviate a fundamental institutional driver for economic growth and facilitate the maintenance of a sustainable steady-state economy by displacing demand for debt-based money as a medium of exchange. In building this case, the chapter begins by considering the inexorable limits to economic growth implied by the bio-physical realities of our planet,

D. Leonard (✉)
Department of Sustainability, Governance, and Methods, MODUL University Vienna, Vienna, Austria
e-mail: david.leonard@modul.ac.at

H. Treiblmaier
Department of International Management, MODUL University Vienna, Vienna, Austria
e-mail: horst.treiblmaier@modul.ac.at

H. Treiblmaier, R. Beck (eds.), *Business Transformation through Blockchain*,
https://doi.org/10.1007/978-3-319-99058-3_7

and the inability of our current monetary systems to function effectively within these limits. The discussion then turns to the ways in which political reforms and alternative currencies could overcome this problem, before exploring the various advantages of cryptocurrencies over many of the alternative options. This line of argumentation amounts to a strong case for the further development of blockchain technologies and especially cryptocurrencies, and one which may appeal to individuals far beyond the spheres of IT, business, and finance.

The Bio-physical World and Its Natural Limits

The first law of thermodynamics informs us that the stock of materials on our finite planet is manifestly limited, but also that we may use the same materials repeatedly. The speed with which we cycle this limited stock of materials through our economic systems—the material flow—is inescapably limited by the availability of energy. The second law of thermodynamics informs us that entropy, which denotes the degree of randomness in a system and the unavailability of thermal energy to be converted into mechanical work, constantly increases. This implies that accelerating the flow of materials through our economic systems requires an ever increasing input of energy. However, the availability of energy to humankind is itself limited by our capacity to harness solar radiation from the sun in the form of solar, wind, and hydropower, as well as the orbital kinetic energy of the sun which manifests as tidal energy. It is not just our capacity to harness these sources which is limited, but the energy flows from these sources are inherently limited themselves. The fact that the economy deals with limited resources and follows the law of physics rather than the so-called economic cycles and mechanical equilibrium states has been laid out decades ago in the work of Georgescu-Roegen (1971, 1975), but has thus far failed to transcend into a new logic of reasoning in economics (Cojanu 2009).

While the ongoing debate about the magnitude of the limits imposed by these physical realities could fill many books (see e.g. Rockstrom et al. 2009; Meadows et al. 2004; Hardin 1995), and is therefore beyond the scope of this contribution, the case made here relies only on acceptance of the fact that the availability of matter and energy for human economic activity is necessarily limited. Increasing technological efficiency enables the maximization of economic output given these limited sources, but as economic activity can never be completely decoupled from environmental impacts, planetary boundaries impose an inescapable absolute limit to the scale of human economic activity.

Societal factors impose even more restrictive limits on the scale of human economic activity than these absolute limits imposed by the biosphere: namely the desirability of the increasingly throwaway society which is implied by continuously accelerating the flow rate of a limited stock of materials. Increasing production and consumption implies not only diminishing marginal benefits from these activities, but also increasing marginal costs—as the provisioning role of ecosystem services is displaced by economic activity (Daly 2005). The 'weak sustainability' perspective endorsed by most nation states and international organizations deems 'sustainable' any increase in aggregate wealth, regardless if this is achieved through further substitution of natural capital by man-made capital. This viewpoint is reflected in the Adjusted Net Savings approach to national accounting (Stiglitz et al. 2009), which subtracts from GDP costs associated with capital depreciation and resource depletion, and therefore treats all factors of production as substitutable. The

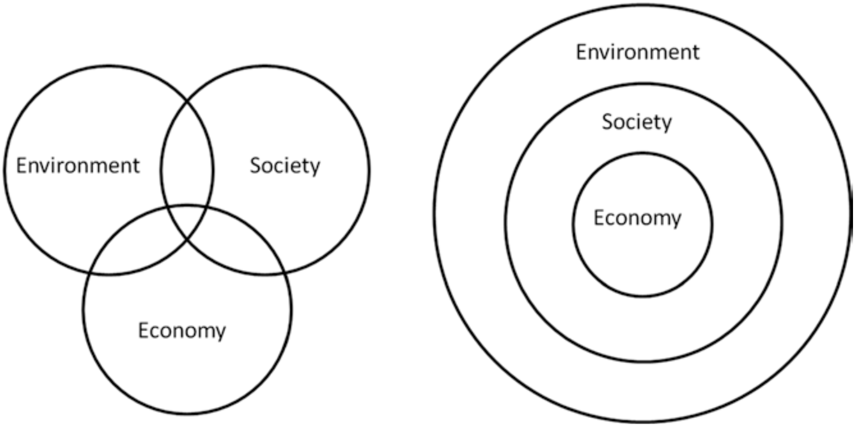


Fig. 7.1 Weak sustainability (left) vs. strong sustainability (right)

independence of the ecological, social, and economic spheres supposed by weak sustainability approaches is depicted in the left side of Fig. 7.1.

The 'strong sustainability' perspective typically endorsed by ecological economists, on the other hand, recognizes the inescapable dependence of both society and the economy on a functioning biosphere, and therefore rejects the linear substitutability of these different types of capital. The right side of Fig. 7.1 depicts these dependencies by representing society as a subset of the environment, and the economy as a subset of the society. Differences between weak and strong conceptions of sustainability lead to dramatically divergent conclusions: the former typically leads to endorsement of 'sustainable' economic growth, while the latter leads to conclusions that a steady-state economy represents the most desirable of all possible outcomes (Daly 1991). Irrespective of differing opinions about which approach will best maintain the wealth of our societies at this point in time, it is clear that beyond a given level of production economic growth will become uneconomic in that the costs of further economic expansion to humanity will outweigh the benefits (Daly 2005). It can be concluded from these bio-physical and societal factors, taken together, that perpetual economic growth is not only impossible, but also undesirable. The so-called growth paradigm, which postulates that economic growth is good, imperative, limitless, and a remedy for many social problems is therefore nothing more than an ideology (Dale 2012).

As a species we are destined for a no-growth future. The open question for society is whether we will reach this inevitable outcome by design, or whether it will be forced upon us by resource scarcity. The consequences for human wellbeing under these two scenarios are wildly different. A controlled transition to a steady-state economy (Daly 1991) will necessitate significant reforms to many of our most deeply entrenched societal institutions which were designed prior to 1970, before the planet's carrying capacity was breached, and therefore reflect an empty world paradigm which assumes an eternal growth in production (Farina et al. 2003). Prominent examples include state administered pension schemes and our debt-based money supply. Awareness has since grown that this Ponzi development path is not viable in the context of planetary limits (Madhavan and Barrass 2011), yet the nature of these societal institutions also precludes the cessation of economic growth, as economic stagnation implies the failure of social security systems (Busch 2010), constriction of the monetary supply, and recession (Nicolini 2015). Nevertheless, the goals of inter- and intra-generational equity will be best served by the development of a steady-state economy, where a fixed stock of resources flows through our economic systems at a constant and non-increasing rate to meet the needs of a stable population (Daly 1991). This version of the no-growth future does not imply the stagnation of a system designed to grow, but rather includes a number of institutional reforms to create a system which is designed to maintain a non-declining level of material throughput per capita (Kerschner 2010). Reaching this state will require significant reforms to several societal institutions: the focus here is on our monetary systems.

The Money Supply

Currently, the vast majority of all money in existence is created in the form of debt and is brought into existence by the creation of loans by private banks through fractional reserve banking (Dyson et al. 2016). In many states, banks are required to retain a certain percentage of demand deposits as reserves and are entitled according to regulation to loan out the remainder at interest. Reserve ratios are determined by central banks and therefore differ by jurisdiction: some states like Australia require no minimum reserves (Reserve Bank of Australia 1991), while Brazil requires 40% of demand deposits to be retained by banks (Banco Central do Brasil 2018). For the sake of demonstration, we will assume a reserve ratio of 10%, which is the ratio applied in the US (Federal Reserve 2017), and is a common figure worldwide. This reservation process repeats when the loaned money is later deposited in the same or another bank, with 10% being retained and the remainder lent at interest: this process continues indefinitely with ever decreasing sums. To provide an example (shown in Table 7.1), an initial deposit of $10 of high-powered money by a commercial bank at a central bank facilitates an initial loan by the commercial bank of $100, which is recorded by the commercial bank as an asset. This high-powered money equals the bank's accounts with the central bank, plus the amount of cash held in its vaults plus the circulating

Table 7.1 Creation of money under fractional reserve banking

	Deposits		Required reserves (10%)		Loans		Transactions		Cum. money
Step	Creditor	Amount ($)	Amount ($)	Cum. res. ($)	Debtor	Amount ($)	Entities	Amount ($)	supply ($)
1	Comm. Bank	10.00	10.00	10.00	Person A	100.00	A to B	100.00	110.00
2	Person B	100.00	10.00	20.00	Person C	90.00	C to D	90.00	200.00
3	Person D	90.00	9.00	29.00	Person E	81.00	E to F	81.00	281.00
4	Person F	81.00	8.10	37.10	Person G	72.90	G to H	72.90	353.90
5	Person H	72.90	7.29	44.39	Person I	65.61	I to J	65.61	419.51
…	…	…	…	…	…	…	…	…	…
44	Person X	1.08	0.11	**109.03**	Person Y	0.97	Y to Z	0.97	**1001.27**

currency. The total money supply is now $110. Following some transaction by the debtor, the recipient of the $100 deposits the money at the same or another institution. This demand deposit facilitates the granting of a further loan in the amount of $90. The total money supply now stands at $200. Repetition of this process enables subsequent loans in the amount of $81, then $73, then $66, and so on, with the total money supply increasing by these amounts at each stage. After 44 iterations, the value of new loans which can be granted has dropped to around $1. Meanwhile, the initial $10 deposit has given rise to loans totaling $990, thereby increasing the total money supply to around $1000, with around $100 of this retained by banks as reserves. Through this eminently simple yet little understood mechanism, banks are able to literally create money out of nothing and then charge interest on that money. Of course, the potential to create money in this way is not always fully realized: banks may voluntarily elect to hold reserves in excess of the minimum legal requirements, while the hoarding of money by citizens outside of deposit accounts (under the mattress for instance) represents a leakage to this system, which stops the money creation process. Nevertheless, currently, around 97% of the global monetary supply has been created in this way, with the remainder consisting of notes and coins (Dyson et al. 2016).

Society needs money as a medium of exchange. The current system is one in which we, as a society, effectively rent our money from private banks who create this money out of nothing but the debtor's pledge of repayment, with interest representing the rental costs. An economy based on debt-based money is able to grow only by placing ever more people into ever greater debt through the granting of credit. This process insidiously concedes power to the few while the many are subjected to a sublimated form of slavery known as 'debt peonage' (Hudson 2012), which is ultimately enforced by state violence. The purpose here is not to address the ethical questions about whether banks should be able to siphon wealth and power from society by charging interest on money they have created out of nothing. These questions have been addressed by other authors, who frequently conclude that the decentralized nature of cryptocurrencies based on the blockchain exemplifies a democratization of the money supply to address these power imbalances, and therefore represents the defining characteristic of these emerging technologies

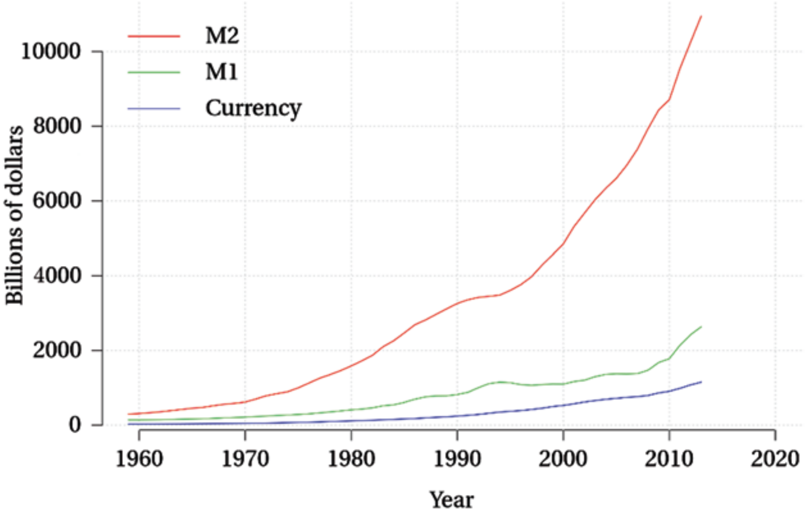


Fig. 7.2 Components of the US monetary supply. (Wikimedia 2018)

(Antonopoulos 2016). Rather, the purpose of this section is to explore the suitability of the current system for non-growing economies and the transition to a steady-state economy, as well as the merits of alternative monetary systems.

Given that the majority of our money has been issued as credit, the first question to be addressed is where the additional money is to come from in order to service the interest payments on our existing stock. At the aggregate level there can be only one answer: new loans must be issued continuously (Douthwaite 2006). That is, our monetary supply must perpetually increase in order to avoid defaults on existing loans. It is important to note that this imperative is not a function of the human condition or our economic systems, but is an inherent characteristic of the monetary system itself (Douthwaite 2006). And the monetary supply is increasing very rapidly indeed: 3.8% growth in ‘broad money’ in the United States during 2016 being somewhat below the average growth rate of around 5% pa over the past 50 years (WorldBank 2017), see Fig. 7.2. The flip-side of this increasing liquidity is the spiraling levels of public and private debt around the world. The debt-based nature of this new money implies a drive for increased productivity at the micro level, as those entities which have taken on debt must realize sufficient returns on their investments to service the interest repayments. This is the first way in which our current monetary system necessitates an ever expanding economy and an ever increasing throughput of materials and energy.

Growth of the monetary supply at a more-or-less constant rate leads to an exponential expansion, which appears benign in times of sufficient economic growth. When the production and consumption of goods and services increases in line with the monetary supply, price levels remain constant. The necessity of continually increasing aggregate production to keep pace with the expanding monetary supply, and thereby avoid excessive inflation, is the second driver for economic growth, and perhaps the most important institutional factor at play: despite the fact that this imperative is pushing us further away from a sustainable scale for the macro-economy from a 'strong sustainability' perspective. From a 'weak' sustainability perspective, however, economists, politicians, and business leaders are entirely correct when they state—to the exasperation of many environmental actors—that the economy, and therefore the flow of materials and energy, must constantly increase in magnitude. The general inflationary trend that characterizes developed economies (Monnin 2014) indicates that recent economic growth rates have been insufficient to maintain price stability, and the situation does not look like changing. Many governments openly embrace inflation, even setting inflation targets, as the expectation of higher future prices discourages saving in favor of present-day spending, and thereby spurs short-term economic growth (Kremer et al. 2013). But it seems that governments may have little choice but to accept inflation, as no developed economy is bold enough to forecast economic growth rates at anywhere near the rate at which the money supply is increasing (OECD 2017). Looking further toward the future, and bearing in mind the increasingly limited availability of resources, it is clear that the increase in production levels must slow even further and, in the best-case-scenario, will eventually stabilize as we move into the steady-state economy: the only alternative being a resource-driven economic collapse (Daly 1991). As this transpires, inflation will inevitably increase further as the autonomously growing money supply outpaces production by an ever growing margin.

The conclusions which can be drawn from this preceding discussion are (1) that our current monetary systems are inappropriate for the impending reality of non-growing economies and (2) that our current monetary systems actively drive society away from the goal of establishing a sustainable scale for the macro-economy. Advocates of 'weak sustainability', which seeks an increase in the wealth of societies by allowing for further substitution of natural capital by man-made capital, may not be alarmed by this narrative. In contrast, advocates of 'strong sustainability', who recognize that future wellbeing is dependent on maintaining stocks of natural capital, are likely to come to the conclusion that reforming our monetary systems is the most pressing institutional challenge in progressing toward a society which accords sufficient respect to the notion of inter-generational equity. Fortunately, there are several avenues by which such reforms could be implemented.

Alternative Money Systems

The most important feature of any alternative system from a 'strong sustainability' perspective is that money should exist independent of debt—commonly referred to as 'positive money' (Dyson 2014). On the one hand, positive money fosters intra-generational equity by diminishing the power imbalances inherent to the current system (Dyson et al. 2016). On the other hand, positive money supports inter-generational equity by reducing the burden of debt which will be inherited by future generations, as well as enabling environmental conservation by alleviating the drive for unsustainable growth implicit to debt-based money (Douthwaite 2006).

Such a system could theoretically result from incremental reforms to the current system, as outlined by Fisher (1935) and updated by Huber and Robertson (2000): governments need simply demand that central banks gradually raise the reserve rate to 100% over time. At that point, commercial banks would no longer have the power to create money and would be restricted to loaning that money which they had previously accepted as deposits: their income would comprise only the difference between the interest collected on loans and that paid on deposits, as well as fees for the provision of financial services. When injections of additional money were deemed necessary according to economic conditions, this could be printed by the treasury or central banks at the government's behest and spent into existence—for example in paying the salaries of public servants. Central banks, if retained at all, would then exercise monetary policy by managing the rate at which they directly create new money, rather than the indirect and less predictable route of controlling the base (bank) interest rate. While the notion of governments printing money is often rejected as inherently inflationary, that is because such actions currently take place in addition to, rather than instead of, the creation of money by banks. With respect to questions of responsible monetary policy and the maintenance of price stability under this alternative model, it is worth reflecting on the chronic inflationary trend and acute financial crisis, and considering whether these important functions might be better performed by elected officials than the corporate entities which are central banks. Modeling of Fisher's original proposal by the IMF in 2006 generated 'strong support' for the range benefits claimed to arise from such a reform (Benes and Kumhof 2012), and the ideas have since received support from numerous economists and bankers including a Vice-President of the European Central Bank (Dyson et al. 2016).

As relatively simple to realize as these reforms could be, they do not appear likely in the foreseeable future. The financial crisis provided an opportune moment for a fundamental restructuring of our monetary systems, yet the very nature of fractional reserve banking did not enter the public discourse at that time. Neither is it generally mentioned in the context of mounting concern over spiraling levels of public and private debt in many countries: these discussions therefore overlook the fact that debt and money are two sides of the same coin, such that reducing debt necessarily means a constriction of the money supply. It is unsurprising that the public is poorly informed on this topic, as educational curricula at all levels routinely omit even the most basic principles outlined in this chapter about what money is and how it is created (Antonopoulos 2016). Whether these various omissions are incidental and arising from a lack of societal awareness of the importance of this topic, or whether they are engineered by vested interests, the result is an apparent lack of political will for governments to undertake the reforms necessary. Political will is not helped by the common fate of the two American presidents that have previously sought to undertake positive money initiatives: Abraham Lincoln in authorizing the issuance of debt-free United States Notes (greenbacks) through the First Legal Tender Act of 1862, and John F. Kennedy in seeking to displace Federal Reserve Notes with silver-backed certificates created by the treasury through the 1961 Executive Order 11110.

The apparent infeasibility of political reform does not mean that society must remain at the mercy of a debt-based monetary system which siphons off wealth from society and drives unsustainable economic growth: rather than reform the system we can seek to displace its influence through the increasing use of alternative and complementary currencies as mediums of exchange. From an ecological economic standpoint, the essential elements of any viable alternative currencies are that they must exist independent of debt and that their growth rates should be determined exogenously according to temporal economic demands and resources constraints. Throughout history, numerous examples of alternative currencies have been created, mostly because of specific socio-economic circumstances (Hileman 2014).

Complementary Currencies

Complementary currencies tend to be regional initiatives which exist in parallel to state administered fiat currencies and aim to keep money within local communities as they are only accepted by locally owned businesses and, in some cases, by local councils for the payment of property rates. These initiatives typically fulfill the requirement of existing independent of debt. To the extent that such currencies displace demand for debt-based money as a medium of exchange, they have the potential to circumvent the growth imperative and facilitate the transition to a steady-state economy. Initiatives have emerged at various scales in numerous countries: a prime example being that of the Brixton Pound (brixton-pound.org/). One benefit of this emergent multiplicity of currencies, as also applies to diversity in biological systems (Elmqvist et al. 2003), is that greater variation implies greater resilience against shocks: catastrophic disruption to one currency need not necessarily affect the functioning of others, or at least not to the same extent. On the other hand, the localized nature of such initiatives may be conceived of as a barrier to the efficiency of transactions between regions in an increasingly globalized commercial environment (Boonstra et al. 2013).

Cryptocurrencies

Cryptocurrencies based on blockchain technology represent an alternative market-based solution to the dominant debt-based money supply, but what kind of money do cryptocurrencies represent? Bitcoin, as an example, appears on its face to represent fiduciary money which obtains value based exclusively on the confidence that it will be accepted as a medium of exchange (Buyst et al. 2005). It is clearly not fiat currency at the present time, given that no government has yet decreed that Bitcoin must be accepted as payment for debts in order that courts will enforce the obligation. It also seems to differ from commodity money in that it lacks intrinsic value, and yet Bitcoin is treated a commodity by some official entities. According to an analysis by Chohan (2017), regulators around the world have adopted varying approaches to this question. As of September 2017, states including Bangladesh, Bolivia, and Ecuador have banned virtual currencies outright, while other national jurisdictions have adopted a wide range of legislative responses. Australia and Japan officially recognize Bitcoin as a means of payment, but not as legal currency. The EU Court of Justice has recognized Bitcoin as a means of payment, with the consequence that conversions between Bitcoin and fiat currencies are exempt from value added taxes, but that these taxes nevertheless apply to transactions for goods and services made using Bitcoin. In the United States, Bitcoin is similarly classified as a convertible decentralized virtual currency by the treasury, yet as a commodity by the Commodity Futures Trading Commission, and as property by the IRS. Israel also treats Bitcoin as an asset for taxation purposes, rather than as a currency. Despite these differences, it is a common finding from many countries that central banks determine that they lack jurisdiction to regulate cryptocurrencies as they do the traditional financial sector owing to the lack of recognized financial actors. Chohan (2017) notes that these regulatory frameworks are highly fluid and subject to alternations over time.

Regardless of how they are legally conceived, cryptocurrencies have demonstrated their viability as a medium of exchange and this is evidenced by the ever expanding list of companies which accept them as payment for the goods and services they provide: including the large online retailer Overstock.com, the travel booking agency Expedia, and the technology company Microsoft. The open question from a sustainability standpoint is whether these emerging technologies represent an improvement over the dominant debt-based money supply. To simplify the analysis and avoid generalities which may not apply to all of the approximately 1500 cryptocurrencies in existence (coinmarketcap.com 2018), we will begin by considering only a single cryptocurrency—the obvious choice being the market leader, Bitcoin—before discussing the implications of variations on this exemplary case, and indeed the notion of cryptocurrency plurality.

To begin with, it is worth considering whether Bitcoin fulfills the three essential functions of money: acting as a medium of exchange, a unit of account, and a store of value. Lo and Wang (2014) acknowledge that Bitcoin fulfills each of these functions, while identifying several limits to its efficiency in doing so, as well as several advantages over other forms of money. Given its lack of intrinsic value, the willingness of merchants to accept Bitcoin as a medium of exchange is entirely predicated on their expectations regarding the willingness of others to use it for future transactions. The advantages of Bitcoin transactions for merchants include lower explicit financial transaction costs, although the mining of new Bitcoins to validate the transaction implicitly devalues all existing holdings by a small extent (Lo and Wang 2014). This externality will cease to exist once the cap of 21 million Bitcoins is reached in 2140, at which point the transaction cost (mining fee) will have to be fully internalized as an explicit cost to the transacting parties in order to inspire miners to process the transaction (cryptocoinmastery.com 2017). Volatility in the value of Bitcoin, on the other hand, could act as an impediment to its use as a medium of exchange: particularly with respect to the issue of returns. As Bitcoin transactions cannot be cancelled, and as the value of Bitcoin is likely to have changed between the initial purchase date and the time of return, Lo and Wang (2014) report the tendency for merchants only to offer in-store credit for returns on orders made with Bitcoin. This volatility also limits Bitcoin's ability to act effectively as a unit of account, by requiring merchants to continually update their prices in order to offset their exchange rate risk. As a consequence, many retailers are reported to express their prices only in fiat currency units and then calculate the corresponding Bitcoin price (as a limited duration offer) at checkout (Lo and Wang 2014). As fiduciary money, Bitcoin's ability to act as a store of value is entirely dependent on the expectations of others, and is therefore prone to speculation and bubbles because its value 'rests wholly on self-fulfilling expectations' (Lo and Wang 2014). Accumulated experience over the short life of Bitcoin has shown it to be deflationary in nature most of the time until late 2017 (as discussed below), indicating that confidence exists that it will continue to be accepted by others. To summarize, Bitcoin does fulfill the three basic functions of money with various levels of efficiency, but would perform even better if it were to see some increased stability in terms of exchange rates. The increasing acceptance of Bitcoin by (especially e-commerce) merchants demonstrates that it is 'perceived by the mainstream to offer sufficiently positive net benefits to be worth experimentation' (Lo and Wang 2014).

These basic functions are better facilitated by forms of money featuring the characteristics of durability, portability, divisibility, fungibility, limited supply, and general acceptability (Desjardins 2015). Cryptocurrencies in general, and Bitcoin in particular, excel in many of these respects. Unlike tangible currencies such as notes and coins they are infinitely durable, requiring only the maintenance of the supporting IT infrastructure to ensure their enduring existence. Paper fiat currencies initially replaced gold due to their greater portability and hence improved ease of use as a medium of exchange, but even these cannot compete with digital currencies for the ease of transacting over large distances. Cryptocurrencies represent a further improvement in portability over centralized digital currencies in that the completion of transactions need not wait the several days often required for traditional clearing houses to validate international transactions. Bitcoin is viable as a deflationary currency due to the fact that each unit is highly divisible. Unlike fiat currencies, this characteristic enables the completion of low value transactions even as the unit price rises. Like all digital currencies, Bitcoin is fungible in that each unit (or portion thereof) is perfectly interchangeable. Any viable currency must be limited in supply in order to act as a store of value. The current version of Bitcoin is hard-coded with an absolute limit in its supply that cannot be changed without a hard fork which would create a new derivative, whereas some other cryptocurrencies and all commonly accepted fiat currencies are limited only in a temporal sense: the implications of this difference are further explored below. It is only with respect to the final characteristic, general acceptability, that Bitcoin can be seen as currently failing to embody the ideal attributes of money. Unlike the other characteristics, however, which are objective features of money itself, acceptability is a subjective assessment by individuals which is subject to change over time.

Having established Bitcoin's ability to fulfill the functions of money and identified the characteristics of money which enable it to do so, we now look at whether Bitcoin fulfills the characteristics of 'positive money'. In contrast to fiat currency which is mainly created from debt, Bitcoins are brought into existence through the productive efforts of miners to verify transactions and inscribe them onto the blockchain (Narayanan et al. 2016). The generation of new coins through mining is consistent with the notion of positive money in that new money can be brought into existence without increasing indebtedness. Of course, Bitcoin currently remains connected to debt to the extent that is bought and traded for fiat currencies, but this process does not reflect the fundamental nature of the cryptocurrency and these links will likely weaken as Bitcoin gains acceptance as a stand-alone currency.

Despite considerable fluctuation in the value of Bitcoin since its inception, a clear deflationary trend is evident, with the price rising from 0.06 USD in 2012 to consistently over 6000 USD throughout the final months of 2017 and early 2018 (coinmarketcap.com 2018). While this development may be explained away as resulting from speculation, these investment decisions of course take account of relevant characteristics of the currency, in particular the issue of scarcity. The total quantity of Bitcoin that will ever be issued into circulation is defined within the original algorithm hard-coded onto the blockchain and which cannot be altered. The algorithm defines that the absolute cap of 21 million Bitcoins is released at a tapered rate—halving every four years—according to a deflationary schedule which was defined when the system was created, and which is publicly known (Narayanan et al. 2016). This characteristic further differentiates Bitcoin from fiat currencies which have no defined limits and whose growth rates are determined through opaque decision making processes by a range of public and private entities. The effect of this uncertainty combined with significant growth rates is that fiat currencies are almost always inflationary—driving economic growth beyond sustainable levels through increased consumption in the shorter term (Kremer et al. 2013)—whereas the fixed volume and increasing value of Bitcoin encourages saving (Murphy et al. 2015). One argument that can be brought against deflationary currencies is the issue of divisibility; that is, the question of what one uses to buy, for example, groceries with when the currency has increased in value to the extent that one unit of the lowest denomination can purchase a car. While a major issue for fiat currencies as well as exchanges involving tangible commodities, this issue poses no problem for cryptocurrencies which are typically infinitely divisible. If this solution became untenable in the longer term as price tags required expression using ever increasing negative exponents, Ametrano (2016, p. 1) suggests as an alternative that 'price stability could be achieved by dynamically rebasing the outstanding amount of money: the number of cryptocurrency units in every digital wallet is adjusted instead of each single unit changing its value'.

So Bitcoin, considered in isolation, can be regarded as a form of positive money which is deflationary by design as long as demand exceeds the amount of new coins being created and therefore overcomes the unsustainable growth imperative which is an inherent consequence of debt-based monetary systems. However, the current situation is one in which Bitcoin exists in addition to fiat money and alongside a wide range of alternative cryptocurrencies, and can therefore be seen as increasing the aggregate money supply and acting as a driver for economic growth. Let's first deal with the issue of crypto-plurality. There currently exist around 1000 competing cryptocurrencies and the number is constantly growing through new initiatives and hard forks from existing schemes.[1] This

[1] A comprehensive list of cryptocurrencies can be found at https://cryptocoincharts.info/coins/info

development allows for the exploration of the various pros and cons of each scheme at this early stage in the development of this new technology. While not all cryptocurrencies place an absolute cap on the total quantity to be released, several important ones tend to specify a fixed quantity which is issued at given intervals, thereby producing an ever decreasing rate of increase which mimics the development of stocks of precious metals: despite increasing perpetually, from a 'strong sustainability' perspective these models still represent an improvement over the steady-rate increase demonstrated by most fiat currencies in recent times. The digital nature of cryptocurrencies even allows for the implementation of economic experiments, which would be hard to do in the real world alone. The cryptocurrency Freicoin,[2] for example, has a demurrage fee that encourages circulation by automatically charging a fee from money holders and strives to create a currency with neither inflation nor deflation. The economic theory behind it stems from Silvio Gesell, an anarchist, libertarian, and theoretical economist, whose revolutionary ideas were hard to implement and test in a non-digital society (Ilgmann 2015).

Potential regulatory interventions notwithstanding, the success of one or more cryptocurrencies will be determined by their attractiveness to investors, and this is already borne out by marked differences in market values. This result is unsurprising: hardly any investor, regardless how optimistic they are about the future of cryptocurrencies in general, would regard a world in which 1000 cryptocurrencies hold even vaguely equal market shares as a probable outcome in the longer term. It would be simply infeasible for single businesses to accept the full spectrum of currencies as payment for their goods and services, and inefficient for different businesses to subscribe to different sets of currencies. Much more likely is that one or two cryptocurrencies, and not necessarily the current market leaders, will rise to prominence and come to dominate the market; this would be reflected in businesses publicizing the fact that they accept those currencies to the exclusion of all others and displaying their prices in the respective units. As such, the notion that cryptocurrency

[2] http://freico.in/

plurality would result in an effectively unlimited monetary supply would appear to be unfounded in reality.

On the other hand, it seems that cryptocurrencies will exist in parallel to the fiat money supply for some time to come and that the expansion of cryptocurrencies will therefore have an overall inflationary effect on the economy. Longer term expectations that these new currencies can yield sustainability benefits is therefore valid only to the extent that they can displace debt-based money as a medium of exchange, rather than complementing it. These changes, if they eventuate at all, are likely to be driven by consumer preferences regarding social sustainability considerations, as exemplified by the literature touting the decentralized nature of cryptocurrencies as their primary advantage over centralized banking systems. But while ecological sustainability is often marginalized or entirely overlooked in discussions of the merits of cryptocurrencies, it could well be in this respect that cryptocurrencies and the blockchain in general hold the greatest promise for transformative societal change.

The institutionalized growth imperative inherent to debt-based currencies and the potential structural advantages of alternative monetary systems notwithstanding, cryptocurrencies do not yet represent a panacea for the world's sustainability issues. A major concern of these new technologies and one that is receiving increasing attention in the literature is the massive energy requirements involved in the mining procedure called proof-of-work as distributed computers compete to solve complex algorithms in order to validate transactions.[3] As the number of crypto transactions grows with time, so too will the energy requirements of the financial sector. However, the high energy costs for mining each block of transactions in Bitcoin is not an inevitable characteristic of cryptocurrencies. The original idea of proof-of-work, as published in the seminal paper from Nakamoto (2008) was intended to ensure that it would be almost impossible for a single node to take control of the network. The rise in popularity of Bitcoin in recent years led to the development of highly specialized,

[3] The Bitcoin Energy Consumption Index can be found on this website: https://digiconomist.net/bitcoin-energy-consumption

energy-consuming hardware (application-specific integrated circuits) and the formation of so-called mining pools, which actually represent a centralization of mining power that is in stark contrast to the decentralization philosophy of blockchain-based technologies. It has to be noted, however, that this huge energy consumption is by no means necessary for the creation of a block from a technical perspective and that alternative ways for finding consensus are currently being discussed in various communities (e.g. proof of stake, proof of burn, proof of elapsed time, Byzantine fault tolerance and variations thereof, Federated Byzantine agreement (Baliga 2017)). Further development is therefore necessary to reduce the energy footprint associated with each transaction, but as the steady-state economy also implies a non-growing number of transactions, the footprint need only be reduced to an acceptable level and not close to zero as would be necessary in an eternally growing economy: such changes seem quite feasible through generalized advances in the energy efficiency of computing processes, and perhaps more specific attention to the characteristics of consensus algorithms used by cryptocurrencies.

Conclusion

This chapter has highlighted an often overlooked potential benefit arising from further expansion of the use of cryptocurrencies based on the blockchain. It begins by building the case that continuous economic growth is impossible in a finite world and that the consequences of further pursuing this development strategy will have deleterious effects for environmental integrity and consequently for societal wellbeing. Debt-based monetary systems which dominate the global economy are subsequently identified as the primary institutional driver that compels humanity to pursue further economic growth despite the growing evidence that it is contrary to our collective self-interest. Finally, in the context of a political climate which lacks the necessary will to undertake crucial financial reforms, the emergence of cryptocurrencies is discussed as a market-based remedy which holds the potential to mitigate the ills of debt-based fiat money and facilitate the transition to an ecologically and socially sustainable global society.

References

Ametrano, F. M. (2016). *Hayek Money: The Cryptocurrency Price Stability Solution*. Retrieved January 10, 2018, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425270

Antonopoulos, A. M. (2016). *The Internet of Money: A Collection of Talks by Andreas M. Antonopoulos* (Vol. 1). Merkle Bollom LLC.

Baliga, A. (2017). *Understanding Blockchain Consensus Models*. Pune: Whitepaper, Persistent Systems.

Banco Central do Brasil. (2018). *Reserve Requirements*. Retrieved February 19, 2017, from https://www.bcb.gov.br/POM/SPB/Ing/ReserveRequirements_PrimaryRules.pdf

Benes, J., & Kumhof, M. (2012). *The Chicago Plan Revisited* (IMF Working Paper No. 12/202).

Boonstra, L., Klamer, A., Karioti, E., Do Carmo, J. D., & Geenen, S. (2013). *Complementary Currency Systems: Social and Economic Effects of Complementary Currencies*. Rotterdam: Erasmus Universiteit Rotterdam.

Busch, K. (2010). *World Economic Crisis and the Welfare State. International Policy Analysis*. Berlin: Friedrich-Ebert-Stiftung.

Buyst, E., Danneel, M., Maes, I., & Pluym, W. (2005). *The Bank, the Franc and the Euro. A History of the National Bank of Belgium*. Tielt: Racine Press.

Chohan, U. W. (2017, September 20). Assessing the Differences in Bitcoin & Other Cryptocurrency Legality Across National Jurisdictions. Retrieved December 20, 2017, from https://doi.org/10.2139/ssrn.3042248

Coinmarketcap. (2018). *Cryptocurrency Market Capitalizations*. Retrieved February 16, 2018, from https://coinmarketcap.com/all/views/all/

Cojanu, V. (2009). Georgescu-Roegen's Entropic Model: A Methodological Appraisal. *International Journal of Social Economics, 36*(3), 274–286.

Cryptocoinmastery. (2017). *What Happens When All 21,000,000 Bitcoins Have Been Mined?* Retrieved February 16, 2018, from http://cryptocoinmastery.com/what-happens-when-all-21,000,000-bitcoins-have-been-mined/

Dale, G. (2012). The Growth Paradigm: A Critique. *International Socialism, 134*. Retrieved February 7, 2018, from http://isj.org.uk/the-growth-paradigm-a-critique/

Daly, H. E. (1991). *Steady-State Economics*. Washington, DC: Island Press.

Daly, H. E. (2005). Economics in a Full World. *Scientific American, 293*(3), 100–107.

Desjardins, J. (2015). *Infographic: The Properties of Money*. The Money Project. Retrieved February 16, 2018, from http://money.visualcapitalist.com/infographic-the-properties-of-money/

Douthwaite, R. (2006). *The Ecology of Money*. Cambridge: Green Books.

Dyson, B. (2014). Positive Money: How to Fix the Creation of Money? *Green European Journal, 7*. Retrieved February 7, 2018, from https://www.greeneuropeanjournal.eu/positive-money-how-to-fix-the-creation-of-money/

Dyson, B., Hodgson, G., & van Lerven, F. (2016). *Sovereign Money: An Introduction*. Retrieved January 9, 2018, from positivemoney.org/wp-content/uploads/2016/12/SovereignMoney-AnIntroduction-20161214.pdf

Elmqvist, T., Folke, C., Nyström, M., Peterson, G., Bengtsson, J., Walker, B., & Norberg, J. (2003). Response Diversity, Ecosystem Change, and Resilience. *Frontiers in Ecology and the Environment, 1*(9), 488–494.

Farina, A., Johnson, A. R., Turner, S. J., & Belgrano, A. (2003). 'Full' World Versus 'Empty' World Paradigm at the Time of Globalisation. *Ecological Economics, 45*, 11–18.

Federal Reserve. (2017). *Reserve Requirements*. Retrieved January 9, 2018, from https://www.federalreserve.gov/monetarypolicy/reservereq.htm

Fisher, I. (1935). *100% Money*. New York: Adelphi Company.

Georgescu-Roegen, N. (1971). *The Entropy Law and the Economic Process*. Cambridge, MA: Harvard University Press.

Georgescu-Roegen, N. (1975). Energy and Economic Myths. *Southern Economic Journal, 41*(3), 347–381.

Hardin, G. (1995). *Living Within Limits: Ecology, Economics, and Population Taboos*. Oxford: Oxford University Press.

Hileman, G. (2014). *A History of Alternative Currencies*. Retrieved February 5, 2018, from www.hillsdale.edu/wp-content/uploads/2016/02/FMF-2014-A-History-of-Alternative-Currencies.pdf

Huber, J., & Robertson, J. (2000). *Creating New Money: A Monetary Reform for the Information Age*. London: New Economics Foundation.

Hudson, M. (2012). *The Road to Debt Deflation, Debt Peonage, and Neofeudalism* (Working Paper 708). Levy Economics Institute of Bard College.

Ilgmann, C. (2015). Silvio Gesell: 'A Strange, Unduly Neglected' Monetary Theorist. *Journal of Post Keynesian Economics, 38*(4), 532–564.

Kerschner, C. (2010). Economic De-growth Vs. Steady-State Economy. *Journal of Cleaner Production, 18*(6), 544–551.

Kremer, S., Bick, A., & Nautz, D. (2013). Inflation and Growth: New Evidence from a Dynamic Panel Threshold Analysis. *Empirical Economics, 44*(2), 861–878.

Lo, S., & Wang, C. J. (2014). Bitcoin as Money? Current Policy Perspectives. No. 14-4, Federal Reserve Bank of Boston.

Madhavan, S., & Barrass, R. (2011). Unsustainable development: Could It Be a Ponzi Scheme? *Sapiens, 4*(1). Retrieved February 7, 2018, from http://journals.openedition.org/sapiens/1083

Meadows, D. H., Randers, J., & Meadows, D. L. (2004). *The Limits to Growth: The 30-Year Update*. White River Junction: Chelsea Green Publishing Company.

Monnin, P. (2014). *Inflation and Income Inequality in Developed Economies* (CEP Working Paper 2014/1). CEP: Council on Economic Policies. Retrieved February 3, 2018, from https://www.cepweb.org/…/CEP_WP_Inflation_and_Income_Ine

Murphy, E., Murphy, M., & Seitzinger, M. (2015). *Bitcoin: Questions, Answers, and Analysis of Legal Issues*. Congressional Research Service. Washington. D.C.

Nakamoto, S. (2008). *Bitcoin: A Peer-To-Peer Electronic Cash System*. Retrieved August 12, 2017, from https://bitcoin.org/en/bitcoin-paper

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton: Princeton University Press.

Nicolini, J. P. (2015). Macroeconomic Policy During a Credit Crunch (No. 15-2). Federal Reserve Bank of Minneapolis.

OECD. (2017). OECD Economic Outlook and Interim Economic Outlook. Organization for Economic Co-Operation and Development (OECD). Retrieved February 16, 2018, from http://www.oecd.org/eco/economicoutlook.htm

RBA – Reserve Bank of Australia. (1991). *Inquiry into the Australian Banking Industry. Reserve Bank of Australia*. Retrieved February 19, 2017, from https://www.rba.gov.au/publications/submissions/financial-sector/inquiry-australian-banking-industry/pdf/inquiry-australian-banking-industry.pdf

Rockstrom, J., et al. (2009). A Safe Operating Space for Humanity. *Nature, 461*, 472–475.

Stiglitz, J. E., Sen, A., & Fitoussi, J.-P. (2009). *Report by the Commission on the Measurement of Economic Performance and Social Progress*. Retrieved December 20, 2017, from www.stiglitz-sen-fitoussi.fr

Wikimedia. (2018). *Components of US Monetary Supply*, from https://commons.wikimedia.org/wiki/File:Components_of_US_Money_supply.svg

WorldBank. (2017). *Broad Money Growth*. Retrieved January 6, 2018, from https://data.worldbank.org/indicator/FM.LBL.BMNY.ZG?locations=US&view=chart

Part III

Society

8

At Your Service: How Can Blockchain Be Used to Address Societal Challenges?

Niels Faber and Jan Jonker

Introduction

The aim of this chapter is to explore possible applications of distributed transaction technologies, such as blockchain, involving multiple constituents. We investigate its use, maintenance, and verification in relationship to societal challenges. Particularly, we set out to touch on the possible uses of such technologies and how they would accord with a society that strives for sustainability and circularity. Our starting point is the identification of the concept of *transaction* which lies at the core of blockchain technology. Various understandings of a transaction come into play. We specify three perspectives that are relevant in this paper: economic, accounting, and IT. In classic economic terms, a transaction implies an exchange in which two actors, a supplier and a buyer, exchange goods or services (supplier to buyer) for some form of payment (buyer to supplier). The result of such transactions is the creation of various values between a supplier and buyer. The supplier's stock of goods decreases in exchange

N. Faber (✉) • J. Jonker
Institute of Management Research, Radboud University,
Nijmegen, The Netherlands

H. Treiblmaier, R. Beck (eds.), *Business Transformation through Blockchain*,
https://doi.org/10.1007/978-3-319-99058-3_8

for an increase in, for instance, the supplier's bank account. Reversely, the stock of goods of the buyer increases and a decline in the bank account is experienced. This simple metaphor is used to explain the process that unfolds with transactions that involve the exchange of goods for money while, of course, it will alter the moment this process is amalgamated with services. From a bookkeeping and accounting perspective, a transaction is considered as a registration of this exchange of goods and services for some form of compensation in a variety of ledgers. Here, each involved ledger records the (monetary) value of the goods or services delivered and payment(s) received. From the realm of information processing, a transaction is understood as a series of operations that form a whole for an information carrier (e.g., a database or file system). This series of operations occurs entirely, meaning that the transaction succeeds, or not at all that is the transaction fails. Key to the transaction concept in information processing is that, before and after the transaction, the information carrier is in a verifiable and consistent state (Gray 1981).

Each of the presented perspectives can be related to the concept of blockchain technology. First, the technology provides a technical foundation that enables transactions as intended in information processing. The technology facilitates the storing of complete transactions and makes these immutable. Second, this foundation ensures the correct handling of transactions in the economic realm. This pertains to two issues, specifically (i) blockchain ensures the correct registration of the transactions in the ledger regarding the actors involved (i.e., the bookkeeping perspective) and, consequently, (ii) it facilitates the administrative component of transactions in the economic sense. Hence, the recording of the exchange of goods and services for some form of payment is reduced to transaction handling at the level of information processing. In blockchain technology, such transactions are recorded in a distributed ledger (Nakamoto 2008). In conclusion, it facilitates transactions regarding all three perspectives.

We use this contribution to explore how blockchain technology relates to sustainability and circularity, two of the current societal challenges. While sustainability and circularity are different ideals, they may very well be considered as two sides of the same coin and members of the same family. Sustainability pinpoints the issues and challenges that society faces in relationship to its natural, social, and economic environments (e.g., Rockström et al. 2009). Additionally, it provides some direction for resolving these, but to a limited extent; realising a sustainable development situated within an inter-generational playing field. In this field, the primary task is to preserve the potential of natural, social, and economic resources in such a way that next generations are able to utilise these same resources to prosper (WCED 1987). Circularity, or the concept of a circular economy (e.g., Stahel 1982; Ellen MacArthur Foundation 2012), promises to provide a more practical approach, emphasising the economics of materials and products. Building on, among others, Stahel (1982), this concept attempts to turn current linear economies into economies that build on closed loops of (raw) materials and products. In these loops, materials that have thus far been considered as waste are reused and recycled, and products are designed for repair in order to reduce the need for virgin materials in the whole of the economy (e.g., Jonker et al. 2018). It is in its effects that the circular economy intends to contribute to the pursuit of sustainable development.

Inspired by Porritt's (2007) framework of capitals, we address both sustainability and circularity from a transactional perspective. From this framework, we derive three principles to support the transactional perspective on sustainability and circularity. First, the framework conceptualises the world as a coherent set of five types of capital: (i) natural, (ii) human, (iii) social, (iv) manufactured, and (v) financial capital. Natural capital refers to all natural and biological resources that the Earth has to offer. Individual capital is comprised of all individuals and relates to them both physically and mentally. Social capital concerns communities, institutional frameworks, and society at large in which humans reside. Manufactured capital refers to technologies, infrastructures, and so on, that humans have constructed to support and facilitate their lives. Finally, financial capital refers to monetary value that humans create and use in their economic systems. Together, the five capitals represent the environment in which humans live, individually and collectively depend on, and make use of throughout their lives. Because the types of capital are interconnected, using these does not occur in isolation and hence multiple capitals will be affected by human actions simultaneously.

The concept that humans use the indicated capital generates the second principle, specifically, that individual and collective human activities occur in relationship to these types of capital in the form of transactions. Humans employ the capital in the goods they make and services they deliver to sustain and improve life (Porritt 2007). These interactions follow the same pattern as an exchange of goods and services in an economic system. For example, a natural resource such as an iron mine experiences a decrease of its iron stock when excavated. On the other hand, the excavators see an increase in their stock of useful iron ore. Whereas the first principle conceptualises the stocks of resources, this second principle identifies the flows of goods and services from the capital (e.g., Tietenberg 2000). Hence, the capital framework allows for the conceptualisation of the interactions between humans and Earth's capitals as transactions.

The third and final principle that shapes our transactional perspective on sustainability and circularity is the ideal of limitations; there are ecological ceilings and social foundations which both need to be observed (Raworth 2017). Each transaction must occur within the limitations of the capital involved regarding (i) volume of use, (ii) intensity of use, and (iii) structural effects. Pertaining to the volume of use, iron ore cannot be mined exceeding the mine's capacity. As to intensity, farming arable land should not take place beyond its regenerative and restorative capacities; the soil needs time to recover from its use. Structural effects refer to the lasting implications of volume and intensity of use of a capital. The assumption is that, if the limitations of a specific capital are not observed over a long period of time, the capacity of the capital diminishes. Restoring this capital will require considerable investment in issue such as time, labour, energy, nutrients, and so on.

The three principles derived from Porritt's (2007) five-capital framework set the stage of a transactional perspective on sustainability and circularity which consequently enables proposing a multi-capital founded approach to bookkeeping. The capital approach sees the world classified in stocks and flows of capital. As such, this perspective identifies multiple actors engaging in a multitude of transactions with regard to these types of capital. Basically, this is what is normally referred to as 'the economy'. Lastly, sustainability and circularity are framed by the idea that all of these types of capital are bound by specific social foundations and ecological ceilings (Raworth 2017). This corresponds to the idea that there are 'limits to use' (inspired on Meadows et al. 1972). Consequently, sustainability and circularity should operate within an economic, social, and ecological bookkeeping and accounting framework that allows for recording individual and collective human activities in relationship to each capital. Ultimately, it becomes possible to record a full administration of human activities to map out how humankind shapes the environment in which it resides. When taking capital limitations into consideration, this also allows for checks and balances for each type of capital in order to determine if we satisfy the requirements of a safe operating space for humankind (Rockström et al. 2009).

Against the backdrop of the presented transactional perspective on the socioeconomic challenges of sustainability and circularity, the question we set out to answer is what blockchain technology could contribute.[1] We do so by, first of all, typifying the characteristics of blockchain technology in section "The Epistemology of the Blockchain". Section "Societal Challenges" continues with a theoretical and conceptual exploration of the concepts of sustainability and circularity. This enables us to make a comparison between, on the one hand, blockchain and, on the other hand, its contributions to the indicated societal challenges in the section "At the Crossroads Between Blockchain and Societal Challenges". In the section "Discussion and Conclusions", we conclude our debate and include several points for discussion and further research. We finish this paper with proposing a preliminary research agenda.

The Epistemology of the Blockchain

This section aims to explain blockchain technology, not from a technological perspective but from a phenomenological perspective. We focus on its implications for social interactions and the transactions that follow from the way of framing. We aim to construe its possible role in an emerging debate on the changing role of organisations, systems, and institutions and the position that blockchain might have within. This debate is evidently informed by the emerging need to address issues such as sustainability and circularity. In order to do so, we briefly discuss the

[1] The technology of blockchain is based on energy and is, by itself, not sustainable from the perspective of eco friendliness, e.g., to perform a transaction on blockchain, the action itself and, consequently, the energy consumed are not necessarily sustainable.

various fields of the application of blockchain that have already emerged around the technology.

Blockchain technology has become known as the technological infrastructure on which cryptocurrencies such as Bitcoin, Dogecoin, or the newer Ethereum operate (Nakamoto 2008). The essence of blockchain is to enable distributed transactions within a heterogeneous network while providing almost absolute transparency regarding the occurrence of transactions. Furthermore, the technology affords the possibility to make use of multiple transaction means (e.g., money, tokens, currency, time, mobility, et cetera); we term this as 'hybridity' (Faber and Jonker 2017; Jonker and Reinhoudt 2015). In the realm of cryptocurrencies, blockchain offers functionality such as protection against double spending, transparency of transactions taking place, anonymity of individuals involved in transactions, and many more (e.g., Nakamoto 2008; Kim 2015). Offering its financial functionality, blockchain pushes aside the traditional role of banks in the current centralised financial-economic system. Similar to normal bookkeeping systems, it keeps track of transactions in a ledger. However, in this aspect, some important differences also exist. First, the blockchain is nothing more than a means to store information and keep track of transactions. Its use for cryptocurrencies resembles the operations of a financial ledger. The blockchain keeps accurate track of the 'money' of an individual and registers all expenses and incomes to it. This 'money' is just information; it does not exist outside of the blockchain. Second, the ledger does not reside with a single actor in the system but is distributed among all of the participants. This means that all users of the ledger have a complete copy of it on their local storage devices from the moment the ledger is initiated. The implications of this are (i) that all participants have a full history of all of the transactions that have been registered from the beginning and (ii) that they would be able to see how the digital currency moves around.[2] Third, all transactions are verified automatically by the entire community. Based on encryption technology, 'blocks' are created and distributed among all of the partici-

[2] The latter might imply principally that one could check the personal accounts of all of the others. This is resolved through encryption.

pants in the network aligned in a non-corrupted sequence. A transaction only is added to the blockchain when these technical specifications are unconditionally met (Nakamoto 2008).

While cryptocurrency is the primary focus of application, and consequently the public debate, blockchain technology is more versatile. It is a technology that is able to register all sorts of transactions and may be used as a carrier of all types of information. Considering this, Swan (2015) identifies three categories or generations of applications of blockchain. We consider these categories as different levels of development of blockchain technology application. Blockchain 1.0 applications concern the use of the technology for cryptocurrencies such as the previously mentioned Bitcoin and Dogecoin. At present, the number of cryptocurrencies has exploded, and Bitcoin itself (together with other coins) has become the object of a speculative hype which popular media (CNN 2017) have compared to the alleged 'Black Tulip'-mania in the seventeenth century (e.g., Boissoneault 2017; Scandinavianlife 2017). Blockchain 2.0 extends the use of the technology to a platform for the registration of contracts. This may, for instance, be stocks, deeds, mortgages, and so forth. Such contracts in blockchain are referred to as smart contracts (Swan 2015). Additionally, Blockchain 2.0 recognises all sorts of applications that build on the concept of decentralised storage of information and processing of transactions. This level builds on so-called tokens (Atzori 2017; Crosby 2016); a token is a digital reference to either cryptocurrencies (e.g., Bitcoin, Ethereum) or physical or virtual objects. Tokens are entered into blockchain through Oracles (Swan 2015). An Oracle is an agent that finds and verifies real occurrences and submits this information to a blockchain which can subsequently be used in smart contracts. Smart Contracts contain a set of values and only unlock those values if the predefined conditions are met. The primary task of Oracles is to deliver those values in a secure and trusted manner. Blockchain 3.0 concerns its use in the realms of justice, governance, and coordination. Central to this category is the use of blockchain to organise activities of people, organisations, or institutions, for example, applications of censorship-resistant organisations, identity verification, or governance services (Swan 2015; Tapscott and Tapscott 2016). Arguably, the widened scope of applications of blockchain technology might provide a number of interesting features on each level in relationship to societal challenges, in particular with regards to sustainable development and the realisation of a circular economy. We propose using a slightly different classification of blockchain from the types that Swan (2015) identifies, respecting the three distinct levels of functionalities as stipulated above. These are (1) Blockchain 1.0: accounting, (2) Blockchain 2.0: contractual, and (3) Blockchain 3.0: community level.

The Accounting Level

The accounting level concerns the level of the blockchain technology itself and thus the principal functions that are embedded within. These functions are transparency of transactions and underlying procedures, traceability, accounting, and immutability. Transparency of transactions is ensured through the registration of all of the details of a single transaction on the ledger. Transparency regarding the underlying procedures concerns the complete set of checks and balances that is performed for each transaction. Traceability follows from the way that the blockchain is constructed. It holds mutations of accounts of individuals which first implies that, in order to know what the status of someone's account is, all of the transactions on this account must be checked. Second, this means that a full history from the beginning of the blockchain needs to be kept in order to know the exact status of the entire system (i.e., all accounts of all participants). The accounting function implies that a transaction is registered on the blockchain at the moment it occurs. Finally, the function of immutability concerns the inability to make changes to registrations that are already on the blockchain. This follows the accounting concept of journaling. Transactions are recorded in the chronological order in which they occur. In the event of the registration of a faulty transaction, a new compensating transaction must be executed.

The Contractual Level

The contractual level concerns a level of functions that builds upon the accounting level. We perceive this level as a collection of functions that shape the attitudes and behaviours of participants and how this affects the peer-to-peer interactions between them. The single function we identify at this level is that of system-embedded trust. Take, for example, the delivery of a birth certificate by means of a blockchain. The placement of the certificate on the blockchain makes this (1) accessible to all parties involved and (2) guarantees its authenticity beyond any reasonable doubt. This function extends the underlying accounting level functions such as encryption and traceability as is embedded in the blocks. Together, the entire set of functions from the technological angle provide a system that ensures the coherent validity of all of the transactions that are unfolding. Consequently, at the contractual level, this is considered to yield trust among participants that is guaranteed by the technology and without the need to include a trusted third party (such as banks, accountants, or solicitors) that vouches for each step in the transaction process (Swan 2015). The contractual level results in the construction of trusted processes without intermediaries leading to reliable contracts between two or more parties.

The Community Level

The community level extends the contractual level. At the community level, we perceive functions that relate to the societal context in which the blockchain technology is used. This often implies that using blockchain at the community level will have system implications. At this level, we perceive a wide variety of possible applications of blockchain among which include embedding entire value chains, realising coordination, establishing governance systems with embedded shared values, or piecing together entire legal frameworks. Bear in mind that the scope of application is widened, while, at the same time, accountability and reliability remain assured. All participants in a blockchain system approach are guided by the same allocated values. At this level, three distinct sublevels emerge.

1. Collective governance of common pooled resources. This sublevel results in avoidance of waste and spill as well as a contribution to systemic governance;
2. Collective valuation. This sublevel necessitates smart contracts that define values of different types. Think, for example, of the value of mobility or currency;

3. Conversion of transactional values. Under the precondition of smart contracts in which the conversion is specified, values of different kinds are exchanged. Consider, for instance, the exchange of time for energy or mobility.

Using blockchain at this system level affords a broad range of unexplored possibilities. In the end, it is inherently a system that exists and operates based on the premise of a community that registers its transactions on it. While the public eye currently mainly focuses on the first level, we contend that especially the second and even more the third level offer a promising technological platform to address societal challenges.

Societal Challenges

Taking a comprehensive perspective on today's society reveals an increasing number of wicked problems (Churchman 1967; Rittel and Webber 1973). Wicked problems are complexly interlinked and have no single solution. This implies that problems of the wicked kind may no longer be solved by single disciplines, by one people or one nation, or within one specific geo-region. In attempting to solve one element, new problems arise elsewhere. Conditions that might lead to solving the specified issue are incomplete and contradictory, and requirements under which solutions are created might appear to change over time. Problems of a wicked nature seem to be characteristic for our times, be it in food, politics, health, energy, asylum seekers, et cetera (Faber and Jonker 2015). Recently, an inventory of wicked problems was made by the United Nations leading to the identification of the Sustainable Development Goals (SDGs; United Nations 2015).[3]

[3] The debate on the SDGs can be brought down to a discussion on sustainability (WCED 1987) that, over time, has fanned out into three separate debates on (1) circularity, (2) inclusivity, and (3) sustainification and the ways they are related to each other. For clarity, it increasingly boils down to a 'radical' process of sustainification, which in its turn is explained as the process in which various actors (governments, businesses and citizens) collectively engage in realising far reaching, impactful goals, or moon shots regarding sustainability (Ellen McArthur Foundation 2012; UNEP 2011; European Commission 2018).

Within the SDGs and despite of the richness of the debate on societal challenges, we limit ourselves to the use of materials.[4] We have selected the material perspective because the current use of material (commodities) within our global economies is such that humankind could call itself 'addicted to material' (UNEP 2011; Meadows et al. 1972, 1992, 2005). In many of the SDG's, material plays a central or peripheral role. Reducing this material addiction addresses a fundamental debate between economic prosperity and ecological preservation. This is generally referred to as the 'decoupling debate' (UNEP 2011). In essence, this debate centres around two decoupling aspects. First, resource decoupling implies the realisation of the same or higher levels of output with the same use of resources. Second, impact decoupling suggests the reduction of environmental, ecological, and health impacts per produced unit (UNEP 2011, pp. 67–68). In this context, we explore how blockchain technology might play a role in addressing this two-faced decoupling debate. This leads to three major strategic (business) perspectives on decoupling, namely: (i) servitisation and dematerialization, (ii) life-cycle extension, and (iii) recycling leading to substitution and conversion. Each of these topics will be briefly elaborated.

Servitisation and Dematerialisation

The origins of the debate on servitisation stem from the landmark publication on the 'performance economy' by Stahel (1982). Since then, this elaborated way of thinking has been developed further (Mont 2002; Tukker 2004; Tukker and Tischner 2006). This has led to the introduction and conceptualisation of the concept of servitisation; more in particular, this has led to a typology of product-service systems (PSS). For instance, Tukker (2004) recognizes eight distinct types of PSSs. The general idea behind servitisation is to 'sell' the functionality of a product while the producer retains ownership. This leads to contracts where clients use the

[4] Such a perspective on materials is connected to the SDGs 7 (affordable and clean energy), 8 (decent work and economic growth), 9 (industry, innovation, and infrastructure), 12 (responsible consumption and production), and 13 (climate action).

services, which is currently a common practice with, for instance, planes, trains, and automobiles. This implies that the use of a specific product is intensified and, as a result, fewer products need to be produced. Ipso facto this leads to dematerialisation and hence the decreasing use of materials. In general, this is called resources or asset pooling. This subsequently results in incentives for the producer to focus on optimal lifetime extension at low costs – including negative aspects of the use of specific products (e.g., pollution, use of spare parts, fuel consumption, etc.). In short, servitisation requires the accounting of services provided (e.g., a local trading system of home-made electrical power) and a bookkeeping system of materials invested in and used (status quo) as well as their current qualities. Blockchain could provide such a system.

Life-Cycle Extension

Organising, at least in Western society, is predominantly based on an industrial model geared towards steady economic growth and as a consequence of high levels of consumption. Products are used for a period shorter than their potential lifespan. This leads to the promotion of the highest possible throughput speed based on the principle of 'planned obsolescence'—meaning, in practice, that goods are perceived as unusable or obsolete after a limited period of use. In economic terms, these products have lost their value. However, suppose we break this cycle of production, consumption, and waste generation? Suppose, in 2017, a washing machine is designed with a life expectancy of 50 years. What are the implications for the design and value proposition of this machine? Is it the solidity and the reparability or should we focus more on the efficient use of resources in its functioning such as water, electricity, and chemicals? So, the concept of life-cycle extension has implications for the way a product is designed, how it operates, and the passing of ownership. Regarding the latter, the product will become subject to transactions on first-hand, second-hand, and n-hand markets. The application of blockchain in the process of life-cycle extension enables the tracing of the various 'events' that occur during the life cycle of a product. While any computer may offer such functionality, the use of blockchain ensures reliable transparency of the total life cycle of each unique product.

Recycling Towards Substitution and Conversion

There is a long-standing debate in Western society about the notion of recycling which has been inspired by the seminal works of Stahel (1982). In the mid-1970s of the twenty-first century, this was fuelled by the introduction of the now famous trio of reuse, reduce, recycle. This triplet marked the beginning of raising awareness regarding the value of products and assets at the end of the economic life cycle. Over a period of almost five decades, the 'discovery' of material value(s) at the end of the life of products has steadily grown in importance. Inspired by the works of the Ellen MacArthur Foundation (2012, 2013, 2014) and the European Commission (see the circular economy package of European Commission 2015), the ideal of circular materiality has gained significance leading to an emerging economic perspective on sustainability. So, what began as an end-of-pipe effort to gain leftover values from waste has now positioned itself in the centre of policy making in politics as well as business. As a result, recycling has matured and developed into four related strands. These are (1) chemical, (2) thermal, (3) mechanical, and (4) manual recycling. Chemical recycling concerns the decomposition of materials into their original chemical components. This should be done in closed cycles in order to assure maximum retention of the materials and their compounding parts and hence the sustainification of such processes. It is applied in, for example, polymer, plastic, composite, and in the near future, possibly also in textile recycling. Thermal recycling implies the use of heat in various forms to bring materials back to their original state. It is often applied to metals of all sorts such as copper, aluminium, steel, or gold. There is a growing market in this respect for so-called 'rare' metals (e.g., Ayres and Ayres 2002). It should not be confused with extraction of the thermal value of materials through incineration. Mechanical recycling has gained considerable attention in the last decade chiefly because of the increased sophistication of the material separation processes that are involved. It leads to the separation of materials making use of a combination of e.g., weight, light, air, force, or vibrations depending on the nature of the materials at stake. Finally, manual recycling is a labour process in which people take apart and classify and sort materials by hand. This is a common form of recycling often used, for example, in textiles, household appliances, consumer electronics, or automobiles.

While the recycling practice has gained momentum, simultaneously but on a more industrial scale, attention has been given to develop processes enabling the conversion of materials that have previously been considered 'dangerous' waste such as, for instance, CO_2 and related gases, food and kitchen waste such as citrus peels, or sewage sludge. Each of these waste streams is stable over time and considerable in size and thus permits ample opportunity for upscaling. It leads to transformation processes creating additional or even virgin materials and components. Gradually, the stage of experiment is over, and the technical facilities move out of the laboratory into industrial installations. If, in the upcoming years, such processes integrate into the concept of a circular economy, then the economic side of the circular economy takes shape and becomes mature.

Finally, the substitution concept circles around the question of choosing bio-based materials when designing and constructing devices, buildings, vehicles, and so on. The core of this concept is based on the idea that materials can either be grown (e.g., plastic from corn, petrol from algae, or building bricks from straw) or clean 'mono' waste streams are created that serve as excellent substitutes in other sectors (e.g., tomato foliage can be used in the paper industry and carapaces of shrimps can be used in the production of drugs). It is noteworthy that the challenge of creating substitutes has led to a vivid debate. The concept of the availability and use of natural space and the discussion of growing food versus 'growing petrol' are especially at stake (UNCTAD 2007). This leads to an ongoing vehement and emotional discussion between NGO's, businesses, citizens, farmers, and governments.

Talking Transition

Considering the previously introduced three strategic perspectives on decoupling, the three levels of the application of blockchain technology, and the societal challenges, it becomes apparent that we are facing a society in transition. We understand transition as a fundamental rearrangement of institutions (inspired by Geels and Schot 2007) that assure societal functions as a whole, such as health, safety, or energy. These functions result from the combined effort of a broad range of actors that are involved. Transition can be juxtaposed to industrial and, subsequently, organisational change and transformation. Organisational change addresses changes within the context of a specific organisation or – at best – a part of the value chain. Transformation is a process in which available capacities and competencies are rearranged to offer a new value proposition (Jonker and de Witte 2013). This can be the challenge of an organisation or a cluster of partners. Both stand in sharp contrast to the challenge of transition since this deals with re-inventing and reshaping a system. This is not just the amalgamation of combining individual organisational efforts but requires a fundamental reconsideration of the premises and suppositions that underpin a particular functional system. Whereas an organisational change or a transformation generally takes between several months to no more than five years, a transition easily spans a period of various decades (Perez 2010). It is assumed here that the identified societal challenges will instigate a transition towards new systems encompassing various domains such as energy, food, mobility, healthcare, et cetera. Hence, it becomes intriguing to investigate how blockchain and the aforementioned societal challenges meet. The underlying rationale is to investigate how the technology enhances sustainability.

At the Crossroads Between Blockchain and Societal Challenges

We have decided to address the identified societal challenges from a strategic business perspective leading to a decoupling from assets and their impact. In this debate, we investigate the possible role(s) of blockchain. Previously, we recognised three distinct levels of the application of blockchain technology, specifically, (1) accounting, (2) contractual, and (3) community levels. The question we explore further is what level(s) of application of blockchain technology foster the transition and address the three strategic perspectives on decoupling.

Table 8.1 presents a first suggestion of how the various levels of applying blockchain technology may contribute to strategic challenges that involve the decoupling of assets and impacts. At the accounting level, the basic functionalities of record keeping and the ability to retrace transactions is offered. For servitisation, this implies that transactions regarding the use of services and functionalities may be registered in the blockchain. The basic principle of servitisation is that users pay for the offered functionality only during the actual periods of use. Whenever an asset such as, for instance, a washing machine is servitised, its uses by a variety of users and thus the transactions imposed on it may be easily recorded chronologically on the blockchain accounting level. Similarly, for life-cycle extension, the accounting of assets around their life cycle records effectively on an accounting blockchain. Operations that aim to extend the asset's life cycle, namely repairs and refurbishments, may subsequently be noted down regarding the asset on the same blockchain. Not until the cessation of use and possibly scrapping will the asset be stricken through on the blockchain. Due to the workings of the blockchain, once registered, an asset cannot be removed from it. The only way to indicate that an asset is taken from operation is to have it registered explicitly on the blockchain, for example, by marking the asset as 'terminated'. With regards to decoupling through recycling, conversion, and substitution,

Table 8.1 Strategic decoupling on crossroads with blockchain application levels

Strategic decoupling and blockchain levels	*Servitisation/ dematerialisation*	*Life-cycle extension*	*Recycling, conversion, substitution*
Accounting	Accounting of transactions of use during life cycle	Accounting of assets and parts; repair and refurbishment during life cycle	Track and trace of components leading to (virgin) material pools
Contractual	Enables provision and quality of delivery of functions	Enables contractual transparency in product-service systems	Enables transparent substitution of materials (part or whole)
Community	Collective valuation leading to accessibility	Governance of stock and flows of assets and materials	Enables the use of multi-transactional means

the accounting blockchain level provides the functionality to register the materials and components used in products. Similar to the registrations underpinning life-cycle extension, tokens represent materials and components in the blockchain. For each product produced, the materials and components it encompasses can thus be traced during the life cycle of the product. At the end of life, the materials and or components may be salvaged and recycled, converted or substituted. Regarding recycling and conversion, changes in the quality of the materials can also be incorporated into the accounting that occurs on the blockchain. This approach is similar to the concept of the Madaster (2018), a central database for materials. However, the Madaster concept does not specify the nature of the technology that is used. It only stipulates the registration of materials and their dematerialisation over time. This may also be realised in more traditional database technologies. The use of blockchain technology inherently ensures the immutability of the registrations that are made. In other words, when a material or component is entered in the blockchain at a specific moment in time, it can no longer be erased from it.

At the contractual blockchain level, the focus shifts from the mere registration of 'things' to a level where criteria for possible and allowable transactions on assets are set. Regarding servitisation and dematerialisation, the contractual level arranges access and sets the quality conditions for the delivery of services and functions. The implications for servitisation are contracts that are effectuated digitally on the basis of performance (Stahel 1982). Ownership remains with the service delivery agent, in this case, the manufacturer. This leads to a contractual arrangement in which the quality of the service is conditionally satisfied in a service contract while the user of the service does not own the asset itself. Using blockchain in this process of servitisation leads to transparency in the quality of the service and the status of the assets used in the delivery of it. This traceability demonstrates how the conditions in the contract are being met. This subsequently provides transparent insights concerning the life cycle of assets and, therefore, it becomes feasible to maintain the quality of PSS. Furthermore, it enables predicting the level of maintenance that is required. During the life cycle, the insights in the quality of the assets based upon the contractual level also facilitates the timely and transparent substitution of materials and components. At the end of the life cycle, the contractual level provides a ‘snapshot’ of the product quality in terms of the materials and components employed. Such a snapshot forms the basis for ‘material roundabouts’. At the end of the life cycle, the use of blockchain technology provides a detailed description of the materials and components used which enables focused processes of recycling and, if applicable, conversion and substitution.

The community level in relationship to blockchain is undoubtedly the most challenging. The reason is that experience with this technology and communities is relatively scarce. Blockchain is used in situations such as car sharing, the exchange of current, and battery capacity sharing within communities. On the level of the community, the strategic decoupling debates ultimately touch upon three interrelated topics including (i) collective valuation, (ii) governance of stocks and flows, and (iii) the use of multi-value transactions. The latter implies that the blockchain leads to a debate on the exchange of values. This begins with valuation which is the process in which a community (or a group of people linked to each other) engage in determining the value of tangible and intangible assets in such a way that it leads to mutual consent. Furthermore, this process of valuation leads to allocation of access to community services that are based upon collectively created stocks and flows. In turn, this necessitates agreement upon a set of rules and regulations, enabling the governance of the values involved. The emerging governance framework should be constructed in such a way that it encapsulates the life cycle of assets and materials involved. Some of these assets will have a life cycle of decades (e.g., houses, utilities, infrastructure, etc.) while others function on a much shorter life expectancy (e.g., household appliances, packaging, consumables, et cetera). Finally, on the level of the community, blockchain enables the identification, valuation, and use of multi-transactional means. This implies that the value of assets or materials either resulting from processes of recycling, conversion, and substitution are perceived as valuables in so-called hybrid transactional processes (Faber and Jonker 2017). The latter implies that transactions are not, by definition, based on processes of monetization (i.e., the valuation of assets in financial terms) but instead enable direct use of those means in transactions. In the blockchain, the conditions of these transactions, and thus the exchange of values, are set. In this respect, Oracles provide predefined conditions encapsulating delivery data, such as water temperature, successful payment, price fluctuations, quality, and so on. In conclusion, taking these observations one step further, the use of multi-transactional means in a community setting requires the clear definition and construction of a transactional system. Blockchain contains the ultimate promise to enable such a system. At this specific level, currently, we only observe modest projects at the crossroad of hybrid means and blockchain technology.

Discussion and Conclusions

We are coming to the close of this contribution. Admittedly, this has been a very conceptual treatise in which we have attempted to frame the crossroads at which blockchain technology meets societal challenges. While still in its infancy, blockchain technology offers a promising perspective on enhancing sustainability. We have provided a tentative exploration of how the three levels of this technology may contribute to the strategic decoupling debates. At present, the actual practices of how to apply blockchain in an effective manner beyond cryptocurrencies is limited. We, therefore, would like to advocate a policy enabling the creation of Living Labs, Communities of Practices, Hackathons, Urban Experiments, Challenges, and so on to explore the full potential of this technology in-depth. We then can share experiences and use them to build a knowledge agenda that identifies research streams and educational programmes. Such an agenda will almost certainly need to address technological, sustainable, and societal issues. Of these three, most probably the societal issues will reveal a need for behavioural, social, and organisational innovation and turn out to be the most 'wicked' of the problems to address.

One disadvantage of the use of blockchain technology that has emerged from the greedy trading of Bitcoins is the excessive use of energy (Malone and O'Dwyer 2014).[5] For instance, the Bitcoin application and, in

[5] It is estimated that last year bitcoin used more than 30 TWh of electrical energy. To understand the meaning of these kind of figures, this represents 30,000,000,000 kWH. This amount of energy (gas or other sources not included) is used by roughly 8.5 million households in the Netherlands.

particular, the mining of new cryptocurrencies on this platform exceed the consumption of 56 TWh per annum (Digiconomist 2018), which represents the *electricity* consumption of approximately 16 million Dutch households (MilieuCentraal 2018). Therefore, in order to become a technology that can be used by a broad range of parties, blockchain itself needs to 'sustainify'. This is not only a matter of providing sustainable energy at the input side but, moreover, a re-conceptualisation of the calculations that are done to operate the platform. Current calculations used in certain implementations of blockchain (in particular, Bitcoin) are of such a complex nature that they require excessive computational time and, consequently, energy. Finally, we presently know very little regarding the potential of the technology of blockchain for sustainification. We, therefore, need a rich variety of initiatives that enable discovering what might be possible. In this respect, we look at a promising future.

References

Atzori, M. (2017). Blockchain-Based Architectures for the Internet of Things: A Survey. *SSRN Scholarly Paper ID 2846810*. Rochester: Social Science Research Network. https://papers.ssrn.com/abstract=2846810

Ayres, R. U., & Ayres, L. (Eds.). (2002). *A Handbook of Industrial Ecology*. Cheltenham/Northampton: Edward Elgar Pub.

Boissoneault, L. (2017, September 18). There Never Was a Real Tulip Fever. *Smithsonian*. https://www.smithsonianmag.com/history/there-never-was-real-tulip-fever-180964915/

Churchman, C. W. (1967). Wicked Problems. *Management Science, 14*(4), B-141–B-241.

CNN. (2017, August 12). Tulip Mania: Bitcoin vs History's Biggest Bubbles – Dec. 8, 2017. News. *CNN Money*. http://money.cnn.com/2017/12/08/investing/bitcoin-tulip-mania-bubbles-burst/index.html

Crosby, M. (2016). BlockChain Technology: Beyond Bitcoin. *Applied Innovation Review, 2*, 6–19.

Digiconomist. (2018). Bitcoin Energy Consumption Index. *Digiconomist*. https://digiconomist.net/bitcoin-energy-consumption. Accessed 22 Mar.

Ellen MacArthur Foundation. (2012). *Towards the Circular Economy Vol. 1: Economic and Business Rationale for an Accelerated Transition*. Cowes: Ellen Mac Arthur Foundation https://www.ellenmacarthurfoundation.org/assets/

downloads/publications/Ellen-MacArthur-Foundation-Towards-the-Circular-Economy-vol.1.pdf.

Ellen MacArthur Foundation. (2013). *Towards the Circular Economy Vol. 2: Opportunities for the Consumer Goods Sector*. Cowes: Ellen Mac Arthur Foundation https://www.ellenmacarthurfoundation.org/assets/downloads/publications/TCE_Report-2013.pdf.

Ellen MacArthur Foundation. (2014). *Towards the Circular Economy Vol. 3: Accelerating the Scale-Up across Global Supply-Chains*. Cowes: Ellen Mac Arthur Foundation https://www.ellenmacarthurfoundation.org/assets/downloads/publications/Towards-the-circular-economy-volume-3.pdf.

European Commission. (2015, December 2). *European Commission – PRESS RELEASES – Press Release – Closing the Loop: Commission Adopts Ambitious New Circular Economy Package to Boost Competitiveness, Create Jobs and Generate Sustainable Growth*. European Commission Press Release Database. http://europa.eu/rapid/press-release_IP-15-6203_en.htm

European Commission. (2018). *Action Plan: Financing Sustainable Growth*. European Commission. https://www.duurzaambedrijfsleven.nl/download/ec-action-plan-financing-sustainable-growth.pdf

Faber, N. R., & Jonker, J. (2015, November 1–4). *A Hub Is a Hub, Not a Network: Towards a Typology of Hubs Framed as a Transferor for Sustainable Development*. Paper Presented at the Global Cleaner Production and Sustainable Consumption Conference, Sitges.

Faber, N., & Jonker, J. (2017). Crypto Currency and Hybrid Banking. In *Proceedings of the Second International Conference of New Business Models NBM@Graz 2017*. Graz.

Geels, F. W., & Schot, J. (2007). Typology of Sociotechnical Transition Pathways. *Research Policy, 36*(3), 399–417. https://doi.org/10.1016/j.respol.2007.01.003.

Gray, J. (1981). The Transaction Concept: Virtues and Limitations. In *VLDB* (Vol. 81, pp. 144–154). Cupertino, CA: Citeseer.

Jonker, J., & de Witte, M. C. (2013). Essenties van Verandermanagement (4). Vijf Strategieën Voor Waardecreatie. http://repository.ubn.ru.nl/bitstream/handle/2066/112970/112970.pdf

Jonker, J., & Reinhoudt, J. (2015). *Hybrid Banking: Paying with More Than Just Money*. Nijmegen School of Management, Nijmeger.

Jonker, J., Stegeman, H., & Faber, N. (2018). *The Circular Economy – Developments, Concepts, and Research in Search for Corresponding Business Models* (Working Paper). Nijmegen: Radboud University, Nijmegen School of Management. https://www.researchgate.net/profile/Niels_Faber/publication/313635177_The_Circular_Economy_-_Developments_concepts_and_research_in_search_for_corresponding_business_models/links/58a0b51645851598bab86654/The-Circular-Economy-Developments-concepts-and-research-in-search-for-corresponding-business-models.pdf

Kim, T. (2015). The Predecessors of Bitcoin and Their Implications for the Prospect of Virtual Currencies. Edited by Luo-Luo Jiang. *PLOS ONE, 10*(4), e0123071. https://doi.org/10.1371/journal.pone.0123071.

Madaster. (2018). *Home:: Madaster*. https://www.madaster.com/nl

Malone, D., & O'Dwyer, K. J. (2014). Bitcoin Mining and Its Energy Footprint. In *25th IET Irish Signals and Systems Conference and China-Ireland International Conference on Information and Communications Technologies (ISSC/CIICT 2014)* (Vol. 639, pp. 280–285). IET Conference Publications 639. Limerick: Institution of Engineering and Technology. https://doi.org/10.1049/cp.2014.0699.

Meadows, D. H., Meadows, D. I., Randers, J., & Behrens, W. W., III. (1972). *The Limits to Growth: Report for the Club of Rome's Project on Predicament of Mankind*. New York: New American Library.

Meadows, D. H., Meadows, D. L., & Randers, J. (1992). *Beyond the Limits: Confronting Global Collapse Envisioning a Sustainable Future*. Post Mills: Chelsea Green Publishing.

Meadows, D. H., Randers, J., & Dennis, M. (2005). *Limits to Growth: The 30-Year Update*. London: Earthscan.

MilieuCentraal.nl. (2018). Gemiddeld energieverbruik. *MilieuCentraal.nl*. https://www.milieucentraal.nl/energie-besparen/snel-besparen/grip-op-je-energierekening/gemiddeld-energieverbruik/. Accessed 22 Mar.

Mont, O. (2002). Clarifying the Concept of Product–Service System. *Journal of Cleaner Production, 10*(3), 237–245. https://doi.org/10.1016/S0959-6526(01)00039-7.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf

Perez, C. (2010). Technological Revolutions and Techno-Economic Paradigms. *Cambridge Journal of Economics, 34*(1), 185–202. https://doi.org/10.1093/cje/bep051.

Porritt, J. (2007). *Capitalism as if the World Matters*. London: Routledge.

Raworth, K. (2017). *Doughnut Economics: Seven Ways to Think Like a 21st-Century Economist* (1st ed.). London: Penguin Random House UK.

Rittel, H. W. J., & Webber, M. M. (1973). Dilemmas in a General Theory of Planning. *Policy Sciences, 4*(2), 155–169. https://doi.org/10.1007/BF01405730.

Rockström, J., Steffen, W. L., Kevin, N., Åsa, P., Stuart Chapin III, F., Eric, L., Timothy, M. L., et al. 2009. Planetary Boundaries: Exploring the Safe Operating Space for Humanity. *Ecology and Society*, *14*(2). http://pdxscholar.library.pdx.edu/iss_pub/64/

Scandinavianlife. (2017, December 15). The Truth About the Tulip Bubble. The Tulip Bubble Was Initiated by the Government. *Steemit*. https://steemit.com/bitcoin/@scandinavianlife/the-truth-about-the-tulip-bubble-the-tulip-bubble-was-initiated-by-the-government

Stahel, W. R. (1982). The Product-Life Factor. In S. G. Orr (Ed.), *Inquiry into the Nature of Sustainable Societies: The Role of the Private Sector* (pp. 72–104). Geneva: HARC.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy* (1st ed.). Beijing/Sebastopol: O'Reilly.

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York: Penguin Books.

Tietenberg, T. H. (2000). Sustainable Development: Defining the Concept. In T. H. Tietenberg (Ed.), *Environmental and Natural Resource Economics* (Vol. 5, pp. 86–98). Reading: Addisson-Wesley.

Tukker, A. (2004). Eight Types of Product–Service System: Eight Ways to Sustainability? Experiences from SusProNet. *Business Strategy and the Environment, 13*(4), 246–260. https://doi.org/10.1002/bse.414.

Tukker, A., & Tischner, U. (2006). Product-Services as a Research Field: Past, Present and Future. Reflections from a Decade of Research. *Journal of Cleaner Production, 14*(17), 1552–1556. https://doi.org/10.1016/j.jclepro.2006.01.022.

UNCTAD. (2007). The Biofuels Controversy. *UNCTAD/DITC/TED/2007/12*. New York: United Nations. http://unctad.org/en/Docs/ditcted200712_en.pdf

UNEP (Ed.). (2011). *Decoupling Natural Resource Use and Environmental Impacts from Economic Growth*. UNEP: Kenya.

United Nations. (2015). *Sustainable Development Goals – United Nations*. United Nations Sustainable Development. http://www.un.org/sustainabledevelopment/sustainable-development-goals/

WCED. (1987). *Our Common Future*. New York: Oxford University Press.

9

Blockchain, Digital Identity, E-government

Clare Sullivan and Eric Burger

Introduction

This chapter examines the legal and technical implications of the application of blockchain technology to authenticate and verify identity for e-Government services and transactions.

On 25 September 2015, the United Nations (UN) General Assembly formally adopted the 2030 Agenda for Sustainable Development which consists of 17 Sustainable Development Goals (SDGs) and 169 specified targets to be achieved by member nations within the next 15 years. A major objective is set by SDG 16.9 is for nations to "[b]y 2030 provide legal identity for all, including birth registration." This is a goal in its own right and it underpins seven other SDGs to be achieved by the UN

C. Sullivan (✉)
Center for National Security and the Law, Georgetown University, Washington, DC, USA
e-mail: cls268@georgetown.edu

E. Burger
Computer Science, Georgetown University, Washington, DC, USA
e-mail: ewb25@georgetown.edu

H. Treiblmaier, R. Beck (eds.), *Business Transformation through Blockchain*,
https://doi.org/10.1007/978-3-319-99058-3_9

member nations. This is the first time that a legal identity for all persons has been officially stated as a global objective. It is a development that has significant implications for governments and individuals.

In a digital world where nations are moving to e-government systems that require a digital identity to transact, the goal of a legal identity for all is, for all practical purposes, a digital identity for all. "Legal identity" is not defined in SDG16.9 and unlike the terms "legal person" and "legal entity," legal identity is not a term which has legal meaning. Identity is not a concept traditionally recognized by the law in many countries, particularly those with a common law legal heritage. Even in civil law countries, where there is a legal concept of identity, it was developed for another era and does not address the nature and implications of a digital identity. This chapter outlines the typical composition and functions of digital identity and discusses its commercial and legal importance, and its emergent legal nature in light of SDG 16.9. This discussion highlights the importance of the accuracy and integrity of digital identity to both individuals and governments.

The application of blockchain technology to identity authentication and verification has the potential to fundamentally transform the way identity information is controlled, authenticated, and verified. This development has been presented controversially, as the means of creating an entirely new and separate virtual legal regime outside existing frameworks and norms. However, blockchain technology can be used within existing national and international legal frameworks to address security vulnerabilities inherent in existing procedures for identity authentication, verification, and storage. This chapter examines the legal, policy, and technical implications of this application of blockchain technology to digital identity, in the context of SDG 16.9, with a focus on the privacy and security implications.

The Evolution of Digital Identity as a Legal Concept

Digital identity is the unique identity assigned to an individual under a particular digital identity scheme, typically a government-backed scheme. Digital identity is composed of information that is derived primarily from a person's birth certificate which is the primary and seminal identity document. While the birth certificate and other identity documents are usually still in paper form, digital identity is stored and transmitted in digital form.

Historically, identity has been a nebulous notion under the law, particularly in common law countries. In contract law, for example, identity has largely been in the background as the law focused on whether there is an agreement and particularly whether there is a meeting of the minds necessary for a contract, informed consent, and arms-length dealing. This focus, which mainly developed in response to commercial practice in the nineteenth and twentieth centuries, led to identity being largely pushed to the sidelines in commercial dealings. Twenty-first century technological advances have created a whole new environment for interaction, including for commercial dealings, that does not involve personal acquaintance or even any personal dealings. As transactions previously conducted in person are replaced by those without any personal interaction, the requirement to have and to present a digital identity for transactions has increased to the point that it is now a primary way an individual transacts.

Digital identity is the means by which a person is recognized and is able to transact in the digital age. As a consequence, digital identity has moved from a notion of uncertain nature, especially in the law, to an unprecedented level of personal, commercial, and legal significance. Now digital identity is poised to assume even greater importance in view the UN SGD 16.9 for a legal identity for all by 2030. This recognition of the significance of legal identity which is in effect digital identity, is a turning point. It makes clear the importance of digital identity to governments and the private sector, and especially to individual. It also strengthens the call for greater protection of digital identity and for recognition of individual rights in identity under international law.

Significance of Digital Identity

Note: in order to fit the confines of a book chapter, this section is necessarily a summary of the major points raised by Sullivan (2007, 2010).

Digital identity has revolutionized service delivery for commerce and the way in which government transacts and interacts with its citizens. It has brought many benefits by increasing the efficiency and cost effectiveness of service delivery, but there are significant ramifications, especially for individuals. This is because of the architecture of digital identity schemes and the functions of digital identity.

Government-authenticated digital identity is necessarily based on the premise of one person: one identity. An individual can legitimately have only one, official digital identity under the scheme. This is a major development because traditionally under the law an individual could usually legitimately use an assumed name. Likewise, one could create a pseudonymous, on-line identity, for example. The move to digitalize government services and transactions is driven not only by the need to reduce costs and to increase efficiency in service delivery but most importantly, to reduce fraud. Uniqueness and exclusivity are therefore essential features of digital identity and these features underpin schemes that use digital identity, especially for transactions. This is so regardless of whether a nation has formally established a national identity scheme and has designated it such; or whether a de-facto approach has been adopted whereby a digital identity is used by individuals to transact. In either case, although it may not be an objective, the reality is that a digital identity used for government services will be used for transactions with the private sector. That has been the experience to date and it is an outcome that is clearly inevitable. What this means is that the digital identity required for government transactions effectively becomes the individual's digital identity for transactions generally, and that identity becomes the primary means by which an individual is recognized and can enter into transactions in the digital age.

Digital identity, in this context, consists of two sets of information: transaction identity and a larger more extensive collection of information which records transactions and other information about the individual, depending on the mandate and particular purposes of the transacting organization/s. Each set of information has different purposes and functions and is of a different nature. The most main functions of transaction identity, that is the part of digital identity used for transactions, are first to recognize a person and then enable transactions, whereas the other information which makes up digital identity is more extensive and dynamic because it is updated to reflect transactions, and administrative information. It tells a story about a person and his/her transactions and usually other associated information; and that is its sole purpose. This information is personal information which is linked to an individual by, and through, transaction identity. It is generally protected under data protection law in most nations. This is because most nations have adopted the EU data protection model for domestic legislation, the notable exception being the United States.

Transaction identity is the most important part of digital identity, primarily because of its transactional functions. Transaction identity, that is, the part of digital identity required for transactions, is a small, defined, relatively static set of identity information, Typically, it is the individual's full name, date of birth, often place of birth, and identifying information such as a signature and/or a unique number such as a PIN but not all this information is necessarily needed for every transaction. The information needed varies depending on the requirements of the transacting entity and the nature and value of the transaction. Often all that is required for routine transactions is full name, date of birth, gender and a hand-written signature or PIN. This information is largely static and is derived from the seminal identity document, the birth certificate.

Digital identity schemes depend on two processes which are authentication of identity at the time of initial registration under the scheme; and verification of identity at the time of a transaction. On registration, an individual is required to establish his/her identity by providing identity documents which usually include birth certificate, passport, driver's and other licenses, marriage certificate if there has been a name change as a result of marriage, and other official documents such as those issued by government authorities, stating name and address. As mentioned, the birth certificate is the primary identity document from which most of the required documents, including other documents such as a passport, which are also considered primary, are derived. Identifying information such as signature, photograph, and biometrics such as a face scan, iris scans and fingerprints, are also usually recorded at the time of registration, or sometimes at the time an identity card is collected. The primary function of this information is to the link to the individual who presented the information and to link that person to the recorded digital identity.

The document checking required for identity authentication follows the Know Your Customer (KYC) requirements required under Anti-Money Laundering/Counter Terrorism Financing (AML/CTF) legislation that was widely adopted around the world following the September 11 attacks in the United States; and since that has been updated and expanded to regulate new money laundering targets and address new forms including use of trade in goods and services. The KYC protocols, also commonly referred to as the 100-point identity check, include an in-person interview at which time the applicant provides a range of specified identity documents that are ranked in terms of their standing to establish his/her identity. Originals of the identity documents are presented in person by the applicant and copies of those documents are made at that time by the authenticating agency for the record as required by the AML/CTF legislation. Much depends on the accuracy and integrity of this process including whether there is robust and independent checking of the presented documents because the information recorded from these documents establishes an individual's digital identity, particularly the set of information required to transact.

After registration, transaction identity is by the individual to transact. Identity is verified when all the required transaction identity information as presented matches the information on record. Transaction identity operates much like a key to allow access to the system to enable transactions. First, one digital identity is located from all the identities registered under the scheme; and then that identity is verified to enable it to transact under the scheme. Irrespective of whether the transaction identity is presented in person or remotely, if all the information as presented matches the information on record, then the system automatically authorizes dealings with that identity. Of course, the assumption is that dealings are with the person who presents the transaction identity but the system in fact deals with the digital identity (Sullivan 2016).

To understand transaction identity, we need to understand who, or what, is a person in law. However, this is the subject of much debate. Central to this debate is whether the legal person must "approximate a metaphysical person" (Naffine 2003). The orthodox positive view is that legal personality arises from rights and duties rather than from intrinsic humanity. The most well-known example is a corporation which the law has endowed with legal personality. For more in-depth discussion of the point, see Sullivan (2012, 234).

Transaction identity consists of information which has both meaning and function and arguably of a distinct legal character. The transacting entity deals with transaction identity, not with the individual. Invitations to treat and contracts are made with that identity—an identity that is composed of digitally stored information, which is accorded authenticity by the system and which arguably has legal personality, Transaction identity is a construct. It is a collection of designated information that is given legal status and effect by the scheme. It is information which, as a collective, has meaning and function. As such, it challenges the traditional legal approach on many levels and while it may seem bold to assert that it is endowed with legal personality, when viewed from the perspective of other disciplines such as computer science, the notion that information has function, as well as meaning, is well established (Sullivan 2016).

To illustrate these points, note that when considered separately and independently, the information that comprises traction identity is of limited use even in definitively identifying an individual. For example, unless it is especially unique, name alone will not single out an individual from a population. As a set, however, the information that constitutes transaction identity is more likely to identify a person; but transaction identity does more. It enables the automated system to transact. It is these operational functions that make transaction identity important, especially to an individual. This identity is generally the primary means by which a person is recognized and is able to transact in the digital era. Although a general assumption is that there is a reaching behind transaction identity to deal with a person, the system does not operate in that way. There is automated machine to machine matching of data. If for example, the transaction identity information as presented at the time of a transaction does not exactly match that on record, the system will not recognize the identity even if it is otherwise authentic and the system will not enable transactions. This can have serious implications, especially for an innocent individual. It underscores the point that the integrity of these systems depends on the accuracy of the information recorded at the time identity is authenticated, and on system integrity, particularly susceptibility to fraud and error (Sullivan 2016).

A key feature of all modern identity schemes is that the information needed to establish identity at the time of a transaction varies depending on the requirements of the transacting entity. Typically, all that is required for routine transactions is full name, date of birth, gender, and a signature or PIN. In some schemes biometrics are used though not typically for all transactions. Most routine transactions only involve matching a photo, hand-written signature, or a PIN. In many cases, only signature and photo will be checked. The primary purpose of this "identifying" information is to link the digital identity with a person but that link is relatively tenuous. All the identifying information currently used have error rates which can result in false positives and false negatives. Photo and signature checks have the highest incidence of error but biometrics also have error rates. For example, in a study in which supermarket cashiers compared real people not known to them to photographs on the credit cards they presented, only 50 percent accurately accepted or rejected the cards. When the card contained a photograph resembling the person presenting it, only 36 percent of the cashiers correctly rejected the card (Kemp et al. 1997). Also see (Hancock et al. 2000; Walker and Hewstone 2006; Hancock and Rhodes 2008; Kerstholt et al. 1992; Stevenage and Spreadbury 2006) for more on biometric identification errors.

A number of features and factors make digital identity susceptible to fraud, misuse and mistake in the initial authentication process, and subsequently when digital identity is used for verified transactions. The nature and functions of digital identity, and particularly of transaction identity, and its significance in the digital era means that the consequences of system error, or fraud are serious especially for the affected individual. Difficulty can arise in the individual establishing in both that "I am who I say I am" and in establishing "I am not who the record says I am."

Conventional Digital Identity

A conventional digital identity system is a centralized system that stores potentially encrypted or hashed values of identifiers and associates them with the digital identity. After establishing a digital identity, the individual can access that identity using an authentication system. Most authentication systems use one or more factors, usually derived from something you are (e.g., biometrics), something you have (e.g., a security token), or something you know (e.g., a password or PIN (Personal Identification Number).

There are two principal interoperable ways that digital identity systems extend identity beyond one system or network. For example, proprietary identity management systems, such as those offered by Facebook, Google, Microsoft, Yahoo, and others, provide digital identity within their proprietary platforms, but also will extend that identity to anyone who the user gives permission to the identity provider. You may have experienced this when logging into one system that asks you to use your Google or enterprise credentials to access a third-party service. The specific technology for this is known as OAuth (Hardt 2012).

This method has the benefit of reusing existing relationships the individual might have. However, there are very few instances of such identity providers using strong enrollment procedures. For the most part, what the identity provider is attesting to is the validity of an email address. However, some identity providers, such as universities and the Federal government, will be attesting to the actual identity of the individual.

Besides the (usually) weak identity verification on enrollment, the first method suffers from a number of security issues. First, if the underlying information is stored in a retrievable format, for example, actual passwords, social security numbers, addresses, etc., then there is the possibility of that information leaking due to a breach. Second, the availability of the identity service is at the pleasure of the identity provider. They may choose to withhold information to an entity the subject wishes to transact with. Finally, they may use or sell the subject's personal information without the subject's knowledge or consent.

The second convention method of identity is to use public key cryptography. In public key cryptography, we use mathematical functions that are easy to compute in one direction, but the inverse function is incredibly hard to compute. The conventional function we use is to take the modulus of the multiplication of two coprime numbers. While relatively easy to do the multiplication and remainder calculation, it is extremely hard to factor a large number. The mathematics of the most common public key cryptosystem, RSA, is such that we can publish one of the factors as a public key and one of the factors as a private key. People can use the public key either to encrypt a message for the key owner that only the key owner, with the private key can decrypt or to decrypt a message from the key owner that only the key owner could have encrypted using their private key (Rivest et al. 1978).

One issue with public key cryptography is knowing the public key is really the public key of the subject. In digital commerce we do not generally assume the subject can physically meet the transacting party in order to exchange keys. The conventional approach is to use a Public Key Infrastructure (PKI). In a PKI, there will be a set of trusted Certificate Authorities (CAs). The public keys of this trusted set of CAs are distributed with operating systems, browsers, etc. With that bootstrap of public keys in devices, we then have the CAs sign the public key of the subject. When an entity is presented with the subject's public key, the entity verifies that a trusted CA has signed the subject's public key.

In this manner, the CA acts as the identity provider. The transacting entity trusts the CA to do the appropriate level of identity validation for the use of the public key. For example, in order to issue a domain validated certificate, for using TLS (Transport Layer Security protocol), for example, for HTTPS (secure Web browsing), a CA validates the requestor in fact has control over the domain in question. For an enterprise validated certificate (where the green lock icon with the corporate name highlighted), the CA validates the existence of the company and that a registered agent is requesting the public key signing. The US Federal government, when it issues a PIV card (Personal Identity Verification card) or CAC (Common Access Card), or the Estonian government, which it issues an e-ID card, requires a face-to-face interview, often including biometric collection and verification.

What distinguishes the first from second model of conventional digital identity is in the former model, the identity provider holds all of the information on the subject and access to verification data is under the control of the identity provider. In the latter model, the CA only vouches for the veracity of the identity by the kind of signature they calculate over the subject's public key. From that moment on, the subject is in control of whom they give their public key to or uses of their private key.

Blockchain and Digital Identity

Public blockchain is best known as the technology that underpins Bitcoin, a virtual peer-to-peer currency and payment system that enables users to transact without using a traditional intermediary such as a bank or government department or agency. Simply explained, a blockchain is a chain of linked records called blocks. As data is added, new blocks ae added to the chain. Each block has a hashed key that links it to the preceding block, a timestamp for when it was added or altered, and transaction data. A feature of blockchain is its immutability, meaning that once a transaction is recorded on the chain, data cannot be retroactively altered. With public blockchain, at least a majority of nodes computing the blockchain would have to collude to undo a transaction. This is highly unlikely to occur in practice. We call the distributed nature of this verification of blockchain "consensus based." Unlike the conventional digital identity systems, where one either trusts in the organization running the identity provider or the organization running the CA, public blockchain is said to create a new trust-based system, where the trust is in the network of servers and the software system, not on any one particular company.

Public blockchain technology provides non-repudiation of events by a group of distributed servers, usually controlled by different people in different locations. A block chain is a public ledger distributed across many computers, using cryptography to ensure the security and accuracy of the information stored in the ledger. Most public blockchain systems use keys and signatures to control who can do what within the shared ledger. Blockchain nodes within the network have their own copy of the ledger, and transactions added to the ledger are public and broadcast to all the participating nodes so in effect, that transaction appears in all copies of the blockchain. According to rules agreed to by the network, one, any, or all of the participants can add transactions to the blockchain. Blockchain algorithms aggregate transactions in "blocks," and blocks are added to the chain of existing blocks, using a cryptographic signature. For public blockchains, that signature includes a proof of work. This proof of work makes it cryptographically unlikely that anyone, including a fraudster of hacker, can alter prior blocks. The public and distributed nature of the blockchain makes it hard to get a false block accepted by the network.

Trust Enabled by Blockchain

From a computer science perspective, there is no difference between a sovereign state issuing a proprietary digital identity stored on a computer under the state's control and a digital identity stored on a blockchain. However, there are practical differences that result in s models that are easier to embody on a blockchain. The issue for the conventional digital identity is the subject has to trust the state or agent (such as a company) to protect the subject's identifying information; to only release that information to parties with a need to access the information; to ensure the information is not incorrectly altered or lost; and that the information is available when needed. Moreover, the subject is trusting the state or agent to not lie about the identifier. Finally, the digital identity is "owned" by the state or agent: they have total control over the identity.

A public blockchain provides secure, public storage with integrity guarantees. Information on the blockchain cannot be maliciously altered or withheld (although one could argue that since the information is open for all to see, this is a bug, not a feature). The information is highly available, given there are hundreds of copies of the blockchain in the network. Most importantly, except for the organization promoting and managing the policy for the blockchain, the blockchain itself and the data on it is not owned by anyone.

Note that many blockchains being established today have concepts of built-in access rights. The idea is to give the subject access control to the data via encryption, instead of identity provider-enforced policy. For example, the subject can encrypt select data on the blockchain belonging to the subject and the subject can select who gets the appropriate key(s) to decrypt the data.

Example of Blockchain for Identity Use

An example of the use of blockchain is to provide a digital identity for a refugee who is unable to produce documentation such as a birth certificate, which is the seminal identity document, to establish his/her identity. The refugee may have no identity documents, but the refugee may have nearby family relations. Identity is important as an individuals' inability to produce any identity documents can hamper the provision of humanitarian aid and the person's ability to obtain employment, education, health care, and generally build a new life. One idea is to create a web of trust, similar to the web of trust established by the PGP (Pretty Good Privacy) public key web of trust. Extending the web of trust to digital identity, a person who is undocumented may say his name is Jamal al-Assad, that he was born in a particular village, on a particular date. That assertion may be substantiated by other members of his family such as his parents and siblings and member of his village who may say for instance that they were neighbors at the time of his birth and know he was borne into the family at the asserted time. One could setup a blockchain-based digital identity system such that individuals can "vouch" for the identity of others on the blockchain. With a web of people vouching for each other, the consensus is that this refugee is who they say they are, and that "fact" is substantiated by the blockchain community.

This is the basic approach used by Bitnation, one of several blockchain-based initiatives. Bitnation describes itself as "a decentralized, open-source movement, powered by the Bitcoin blockchain 2.0 technology, in an attempt to foster a peer-to-peer voluntary governance system, rather than the current "top-down," "one-size-fits-all" model, restrained by the current nation-state-engineered geographical apartheid, where your quality of life is defined by where you were arbitrarily born." Bitnation further states that it "provides the same services traditional governments provides, from dispute resolution and insurance to security and much more—but in a geographically unbound, decentralized, and voluntary way. Bitnation is powered by Bitcoin 2.0 blockchain technology—a cryptographically secured public ledger distributed among all of its users. As we like to say—"Bitnation: Blockchains, Not Borders." (Tempelhof et al. 2017) Key to this view and these services is the use of blockchain to vouch for claimed identity outside existing legal frameworks. As noted above, rather than using strict, mostly deterministic KYC procedures as required by AML/CTF legislation, identity is authenticated and verified by the community, using a distributed ledger on a global, open platform, essentially establishing a system of self-sovereign identity.

Bitnation gained international prominence by providing an emergency block-chain-based digital identity to enable access to aid for Syrian refugees who cannot establish their identities to open a bank account to receive funds. A digital identity is established on the blockchain and financial aid is delivered to the refugee through a Bitcoin Visa card. Susanne Templehof, founder of Bitnation explains that "the Blockchain Emergency ID is a rudimentary emergency ID, based on the blockchain technology, for individuals who cannot obtain other documents of identification." "[W]e are providing emergency ID and then this visa card because most refugees will be unemployed. They won't be legally able to get a job for several years and they can't open a bank account." The blockchain is used to cryptographically establish an individual's existence and family relations to generate a digital identity. That identity then generates a Quick Response Code, an optical label that contains information in machine-readable form that can be read by a mobile phone, to apply for a Bitcoin Visa card which can then be used throughout Europe without the need for a bank account (Allison 2016).

Note that on the face of it, Bitnation could have setup a conventional data base and provided this service as a conventional identity provider. However, a question that would immediately raise is, "By what authority does Bitnation issue digital identity?" While blockchain does not directly answer that question, it does address the issue. Namely, if Bitnation used conventional means to be an identity provider, individuals, enterprises, and states would have to fundamentally trust Bitnation to properly account for the identities and links in its identity web of trust; one would have to trust the integrity of Bitnation's data base and operations; and one would have to trust the integrity of the links in Bitnation's web of trust. For conventional identity providers, we have this trust based on fiat and audit. We trust the digital identity provided by a government because the government asserts the identity is accurate (fiat). We (sometimes) trust a digital identity provided by an enterprise because beyond the enterprise asserting the identity is accurate, that enterprise may be subject to government-imposed laws (such as KYC-AML for banks) or the enterprise may, for example, voluntarily subject itself to audit to raise the public's trust expectations in the enterprise's assertions of its customers' digital identities.

As evidenced by the quote above by Bitnation's founder, Bitnation is somewhat antagonistic to traditional government sovereignty. It would be unlikely for any government to provide or accept Bitnation's claims of data integrity or conventional third-party audits of the Bitnation system. By definition, Bitnation is not following conventional KYC-AML identity verification norms, as refugees do not have the means to conventionally prove their identity.

Bitnation uses blockchain to overcome these issues of trust. All refugee's digital identities are published, for all to see, on the blockchain. As the blockchain is immutable, one cannot change the information on the blockchain, such as a person's name, place of birth, or family/trust relationships. Moreover, the web of trust assertions, such as "this is my son" or "I was the village elder and I vouch this individual was born and named as shown in the identity record" are all public. That means the individuals themselves can build up a picture of identity assertions, audit them, and third parties can also analyze the assertions to audit their validity. For example, a claimed village elder who vouches for one person in Aleppo cannot also vouch for another person in Homs on the same date.

The utility of the blockchain-based emergency digital identity in these circumstances are clear. However, the process of identity validation bypasses existing national and international governance and regulation which has been established for good reason and as a result there are broader consequences. The most serious possibility is the creation of a digital identity without lawful basis that can be used to conceal real identity and associated records. Although the digital identity created on the blockchain is justified as a short-term solution, for a person who is otherwise unable to establish identity, in effect this process creates a digital identity for the next stages of the person's life. Bitnation claims that it is unlikely that a false identity can be created because it requires collusion, it is certainly not impossible. The even more concerning aspect is that while a person's basic identity information, that is, full name, date of birth, place of birth, and gender as substantiated by consensus, may be accurate, past history including involvement in criminal and subversive activities are not known nor verifiable.

According to Templehof, the broad objective of Bitnation is "to gain recognition for Bitnation as a sovereign entity, thus creating a precedent for open-source protocol to be considered as sovereign jurisdictions." (Allison 2018) In effect this will "establish a new virtual jurisdiction with its own rules." In addition to the huge increase in stateless people in Europe from the refugee crisis, Bitnation is looking at developing markets, assisted economies and the gray economy. For example, the registry capabilities of blockchain are being considered as a means of recognizing land rights in the developing world in countries like Ghana, where 70 percent of land is reportedly untitled and land is traded peer to peer. In other words, blockchain technology is seen as the basis for a new system for a full range of commercial applications outside existing legal governance and regulation. Templehof cites the example of marriage between a same sex couple which is not recognized as legal in many countries but can be recognized on the blockchain. "[T]o get married on the blockchain would take you ten minutes between writing the contract and time-stamping it." She points out that "you could marry as many people as you want, any gender." Templehof warns, however, that "the intrinsic immutability of blockchain systems means it could be very hard to get a divorce, suggesting short term marriage contracts of four or five years at a time."

There are also broader implications. The use of blockchain in this type of situation to create an emergency, temporary digital identity to enable aid to be given to an individual who is unable to otherwise establish his/her identity may be admirable. However, it does raise security concerns particularly in the use of this means to create and new, false identity and to engage in nefarious and covert activity ranging from crimes like money laundering to activities endangering national and international security.

Although Bitnation may aspire to sovereignty, as an autonomous cyber jurisdiction, the transactions registered by Bitnation do not have legal standing. Nevertheless, the use of blockchain technology in this way can have potentially serious implications for legitimate identity and the activities it supports especially if information verified outside existing legal framework transitions into the real world. For example, depending on the rule and rigor of the checking required for registration under a particular national identity scheme, a name change as a consequence of a marriage recorded and recognized on the blockchain, may be used to register that name as part of a national digital identity scheme, thereby creating a new digital identity and in effect, a new legal identity, that is not in fact correct or legitimate. It is this potential for cross-over into the real world that is the most significant risk to the integrity of digital identity. An iteration that operates entirely outside existing law can lead to creation and use of new, false identities and illegal use of legitimate identities as ideal vehicles for fraud, tax avoidance and laundering of money that subsequently can be used to fund illicit activity ranging from organized crime to terrorist activity.

Bitnation's model of self-sovereign blockchain-based identity is problematical and is highly unlikely to gain mainstream acceptance or any kind of legal recognition. However, it is an example of using a public blockchain to record an "authoritative" digital identity for an individual outside the context of a sovereign state or proprietary platform. As such, blockchain technology has the potential to fundamentally change the way identity information is controlled and authenticated.

Blockchain and E-government

What if individuals and governments and private sector organizations could benefit from the advantages of the use of blockchain for identity within exiting legal frameworks? This is an approach which is of considerable interest to governments.

Estonia's use of blockchain concepts predates the Bitcoin blockchain. Estonia was an earlier adopter with blockchain hash publication underpinning its national identity scheme for citizens and permanent residents and for its newer international e-Residency program. Specifically, Estonia uses the concept of generating a one-way hash of the data it wants to protect, combined with prior hashes, and then publish that information publicly. In the early 2000s, that information was literally published in newspapers around the world. Today, that publication is on a blockchain-like chain of hashes.

Estonia's approach is to revolutionize traditional approaches rather than integrate blockchain into procedures such as KYC (Sullivan and Burger 2017). Other countries are seriously considering integrating blockchain technology into their identity checking protocols including the KYC requirements. The United Kingdom for example, is looking at the advantages of blockchain and in the United States, the state government of Illinois is undertaking six blockchain pilot programs including for a blockchain-based birth registry/ID system. The idea is to create "a secure 'self-sovereign'" identity for Illinois citizens during the birth registration process. The Illinois Blockchain Initiative commented, "To structurally address the many issues surrounding digital identity, we felt it was important to develop a framework that examines identity from its inception at child birth… Identity is not only foundational to nearly every government service, but is the basis for trust and legitimacy in the public sector." The site goes on to explain that in the proposed framework, "government agencies will verify birth registration information and then cryptographically sign identity attributes such as legal name, date of birth, sex or blood type, creating what are called 'verifiable claims' or attributes. Permission to view or share each of these government-verified claims is stored on the tamper-proof distributed ledger protocol in the form of a decentralized identifier… This minimizes the need for entities to establish, maintain and rely upon their own proprietary databases of identity information." This approach is notable because it applies from birth and in that regard accords with both SDG 16.9 and the fact that digital identity is based on information which is mostly established at birth. The idea is to "ta[ke] the source data from the passport office, from the DMV, from the post office, from the utility companies, and using that to prove granular things about a person's identity" (Illinois Department of Commerce and Economic Opportunity 2017).

Conventional KYC-AML laws require the enterprise validating the customer's identity to scan and store the customer's primary documentation, such as their passport or identity card. With a blockchain-based system, the source documentation can be stored off of the blockchain, the document hash can be compared to the hash on the blockchain, and the comparison can be stored on the blockchain. The benefits of this approach are that the enterprise need not store the source documents, yet the enterprise can also prove, via a ledger entry on the blockchain, they performed the KYC-AML validation. By not storing the source documents, the enterprise cannot lose them in a breach—it is impossible to lose data that one does not have.

By leveraging blockchain technology, identity providers can enable identity subjects to control the use of their information. It is true that an identity provider can promise subjects that they will contact the subject before divulging their information or verifying their identity. However, all the subject has is the provider's promise. With public blockchain technology, the subject can verify that only hashes of their personal data or encryption of their personal data with user-generated keys are stored. In that latter, more extreme version of data protection, the data user must contact the subject to obtain a decryption key to access the data. In other words, the user is directly in the loop for data retrieval, and the user can thus choose to not divulge their keys, and thus their data.

When used in this way, blockchain has clear benefits, especially in giving an individual control over his/her identity information and documentation and who has access to them. Distributed ledger technology like blockchain obviates the need for private sector organizations verifying the originals of identity documents such as birth certificate, passport, and utility bills, to copy, upload, and store a scan. Instead, a person can place his/her identity information and documents on the blockchain and use the PKI, directly authenticating the source data from the passport office or other government departments and utility companies. Security is improved because copies of identity documents are not stored on a number of databases, and are not as susceptible to erasure, loss, unauthorized access, alteration and misuse. This system also assists persons in the situation faced by Syrian refugees who unable to obtain or verify their identity information from official sources because they and the information held no longer exists. Blockchain is a comparatively more durable and enduring means of authenticating and verifying identity.

Security is improved because the identity documents are stored on, and authenticated by, the distributed ledger without the need for multiple copies to be retained on government and proprietary systems as part of the KYC process. Instead, a record of the authorization is stored in the chain. It improves security in that it eliminates multiple copies that increases the odds of them compromised and the blockchain provides a record of attribution and is generally a more accountable process. It is true that access could be tracked and proved without blockchain, but that requires much more work, trust, and integration with an infinite number of applications. Most importantly, blockchain could provide the individual with more control. The individual controls who accesses his/her identity documents and identity information and the timing of that access. The blockchain also provides the individual with timely information about who in fact accessed that information and when that occurred. Note that if implemented poorly, this model of total sunshine has a problematic feature: while it is true that anyone can validate that an individual's transactions occurred and it is impossible to erase or modify those transactions, everyone can see the individual's transactions. For example, while one could verify that an individual opened a bank account, got married, and purchased a house, one could also learn they paid a criminal debt and was admitted to a mental institution for a period of time.

Blockchain is touted as being more secure than existing systems and that appears to be borne out in its use for Bitcoin, but the security of its broader use, especially for identity documents and information is untested and is unknown. Moreover, blockchain is like any complex system in that implementation errors, as well as architectural errors, can result in undesired behavior (Price 2016). It is a new approach which may involve new security vulnerabilities. It may, for example, be found to have issues as to the authenticity of the documents and accuracy identity information placed on the blockchain and with the veracity of the identity authentication and verification process. The legal issues regarding responsibility and accountability of those who vouch for the accuracy of that information and the ensuing consequences, are also entirely undeveloped and as yet unknown. Blockchain changes the premise of established law. The applicable law depends on whether the blockchain is owned and operated by government, or whether there is an outsourcing arrangement with a private entity (the model being followed in many jurisdictions), and the location and control of the blockchain ledgers. However, for example, most data protection law is based around the data controller being a government or private organization that is processing an individual's personal information. Public blockchain challenges the balance of power so that in effect the individual becomes the data controller What is clear is that the legal implications are complex.

Blockchain, Digital Identity, E-government and a Right to Identity

The full legal implications of blockchain are not yet known but use of a distributed ledger clearly raises new legal issues regarding responsibility for the documents and information stored and accessed on the ledger and for the ensuing consequences if their accuracy, integrity, and security is compromised. While there is much uncertainty as to how current data protection and privacy law will and can apply, there is scope for development of a much more effective individual right—the right to identity.

An individual right to identity exists under international law and is poised for greater recognition in light of UN SDG 16.9 and the use of blockchain for identity. The right to identity is a fundamental human right that arises at birth under the Convention on the Rights of the Child (CRC), which was adopted and opened for signature, ratification, and accession by UN General Assembly Resolution 44/25 of 20 November 1989, entered into force 2 September 1990, in accordance with Article 49. A right to identity is expressly included in Article 8 and the CRC distinguishes the right to identity from the right to privacy in Article 16. Article 8 was included in the CRC as the result of a campaign by the grandmothers of 'The Disappeared' in Argentina for the right to identity (Detrick et al. 1992). They argued that the country's adoption laws enabled concealment of children's true identities and the creation of false identities. Their campaign led to Argentina recognizing a constitutional right to identity (Avery 2004).

Under Article 8 (1) of the CRC there is an express right to identity and although the CRC is confined to rights of minors, considering the nature of the right to identity, arguably it continues when a child becomes an adult. The argument that a right to identity for all be recognized has now been considerably strengthened by the formal adoption by the UN General Assembly of Sustainable Development Goal 16.9 which provides that member states provided a "legal identity for all, including birth registration" by 2030 (United Nations 2015).

In the EU, an international leader in the development and recognition of human rights, the European Court of Human Rights (European

Court) under Article 8 of the European Convention Protection of Human Rights and Fundamental Freedoms (ECHR) has recognized the right of both minors and adults to identity.

The right to identity can also be recognized under the International Covenant on Civil and Political Rights (ICCPR), which was adopted by the UN General Assembly Resolution 2200A (XXI) of 16 December 1966, entered into force on 23 March 1976, in accordance with Article 49, for all provisions except those of Article 41; 28 March 1979 for the provisions of Article 41 (Human Rights Committee), in accordance with paragraph 2 of Article 41, particularly under Article 1(1):

> All peoples have the right of self-determination. By virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development.

The CRC and the ECHR can provide the basis for legal action by an individual whose identity information is not accurately recorded or which has not been adequately protected on blockchain. The treaty obligations as standards may form the basis of legal action under national law or in the case of ECHR action may be taken under the treaty itself, though it should be noted that human rights claims have different objectives and standards of proof from typical damages claims. The former is designed to regulate state conduct and standards in upholding individual human rights, whereas the latter are primarily designed to compensate for damage caused, though usually the is a consequential impact on conduct and processes. As such, the ICCPR potentially has greatest impact on state conduct through the monitoring of national implementation of the ICCPR by the UN Human Rights Committee (UNHRC).

The right to self-determination under Article 1 of the ICCPR is generally considered to be in-line with the international legal meaning of self-determination, and to cover both the internal and external aspects of the right (Sullivan 2016). Note that the HRC has not clearly defined "self-determination" in Article 1. Committee on the Elimination of Racial Discrimination (CERD) has identified an internal and an external aspect. The internal aspect as defined by CERD is "the rights of all peoples to pursue freely their economic, social and cultural development without outside interference. In that respect there exists a link with the right of every citizen to take part in the conduct of public affairs at any level." CERD states that "the external aspect of self-determination implies that all peoples have the right to determine freely their political status and their place in the international community based upon the principle of equal rights." While the external aspect has in areas other than colonization not been the subject of analysis, arguably it can ostensibly apply to digital identity.

Self-determination under Article 1 of the ICCPR invokes protection of the "private sphere" as advocated by Charles Reich (Reich 1991). "The individual sector" according to Reich is the " 'zone of individual power' necessary for the healthy development and functioning of the individual" and "absolutely essential to the health and survival of democratic society." A right to identity is part of that personal sphere, and arguably it now includes the right to digital identity (Sullivan 2016). Digital identity is protected under Article 1(1) of the ICCPR because the Article protects individual autonomy and that is directly relevant to the use of blockchain for identity authentication, especially considering that it purports to give the individual control over his/her identity information and who can access it.

The UNHRC refuses to examine individual complaints based only on Article 1. Although it has been criticized for this view, the HRC considers that that only individual rights recognized in Part III of the ICCPR (articles 6–27) can be examined under the individual complaints procedure established by the Optional Protocol to the ICCPR, adopted and opened for signature and accession by General Assembly resolution 2200 A (XXI) of 16 December 1966. However, nations including Estonia must report to the UNHRC regarding implementation of Article 1 of the ICCPR and this reporting is the most effective part of overseeing compliance. Because countries that have ratified the ICCPR must report every 4 years. The UNHCR publishes its findings, identifying any areas of concern. These "concluding observations," by the UNHRC are a significant moral and political obligation for a government like that of Estonia which has committed itself to complying with the treaty.

Conclusion

Digital identity, particularly digital identity established on blockchains, is revolutionizing the delivery of e-government. Classical identity is established through government-issued paper documents, such as birth certificates, passports, and identity cards. Modern identity is established through digital identifiers such as national identity numbers and digital identity certificates. While a national identity number can identify an individual, it does not authenticate that the 'person' asserting they have that number is, in fact, that person. This is why contemporary digital identity systems use public key cryptography, digital certificates, and secure access to the private keys through the use of passphrases, biometrics, and PINs.

The point of identity, especially digital identity, is to enable the individual to conduct transactions, whether they be transactions with the government, such as receiving benefits, paying taxes, voting, and so on; or transactions with other entities, such as banking, receiving a salary, buying goods, paying rent, and so on. These transactions, particularly the commercial transactions, happen because the parties involved trust the credentials. Specifically, they trust the credentials do in fact represent the authenticated identity the claim to represent.

We have raised issues with non-governmental entities that issue digital identities, more especially those whom do not follow enrollment validation that are on a par with the various KYC regulations. One would expect that over time, such digital identities would have less and less value. However, we have outlined the mechanisms used by Bitnation in their efforts to issue digital identities for individuals for whom it would be impossible to do a full KYC validation, as their paper documents have been lost or destroyed.

For a company like Bitnation, establishing trust using conventional means, especially given their apparent antagonistic relationship with established governments, would be virtually impossible. However, by using public blockchain technology, they are able to establish trust in their crowd-sourced identity verification system. Moreover, they are able to establish trust in the veracity and integrity of their identity assertions by leveraging the immutability of the blockchain and opportunity to have the data on the blockchain publicly available.

For a country like Estonia, which has a real threat of invasion from large, hostile nation states, using the chained hash technology of blockchain enables them to build an electronic government infrastructure that can withstand electronic or kinetic attacks, as well as the seizure of computer, data, and network assets.

Acknowledgments The Army Research Office provided funding for this paper through the Minerva Initiative agreement # W911NF-15-1-0595.

References

Allison, I. (2016, September 29). *Decentralised Government Project Bitnation Offers Refugees Blockchain IDs and Bitcoin Debit Cards.* Retrieved April 8, 2018, from International Business Times. https://www.ibtimes.co.uk/decentralised-government-project-bitnation-offers-refugees-blockchain-ids-bitcoin-debit-cards-1526547

Allison, I. (2018, February 8). *Bitnation and Estonian Government Start Spreading Sovereign Jurisdiction on the Blockchain.* Retrieved April 8, 2018, from International Business Times. https://www.ibtimes.co.uk/bitnation-estonian-government-start-spreading-sovereign-jurisdiction-blockchain-1530923

Avery, L. (2004). Return to Life: The Right to Identity and the Right to Identify Argentina's "Living Disappeared". *Harvard Wonem's Law Journal, 27*, 235.

Detrick, S., Doek, J. E., & Cantwell, N. (1992). *The United Nations Convention on the Rights of the Child. A Guide to the "Travaux Préparatoires"*. Dordrecht: Martinus Nijhoff Publishers.

Hancock, K., & Rhodes, G. (2008). Contact, Configural Coding and the Other–Race Effect in Face Recognition. *British Journal of Psychology, 99*(1), 45–56.

Hancock, P., Bruce, V., & Burton, A. M. (2000). Recognition of Unfamiliar Faces. *Trends in Cognitive Science, 4*(9), 330–337.

Hardt, D. (2012). *The OAuth 2.0 Authorization Framework.* Internet Engineering Task Force, RFC 6749.

Illinois Department of Commerce and Economic Opportunity. (2017, August 31). *State of Illinois Partners with Evernym to Launch Birth Registration Pilot.* Retrieved April 8, 2018, from https://www2.illinois.gov/IISNews/14759-DCEO_Birth_Registration_Pilot_Release.pdf

Kemp, R., Towell, N., & Pike, G. (1997). When Seeing Should Not Be Believing: Photographs, Credit Cards and Fraud. *Applied Cognitive Psychology, 11*, 211–222.

Kerstholt, J., Raaijmakers, J., & Valeton, J. M. (1992). The Effect of Expectation on the Identification of Known and Unknown Persons. *Applied Cognitive Psychology, 6*(2), 173–180.

Naffine, N. (2003). Who Are Law's Persons? From Cheshire Cats to Responsible Subjects. *Modern Law Review, 66*, 346–367.

Price, R. (2016, June 17). *Digital Currency Ethereum Is Cratering Because of a $50 Million Hack*. Retrieved 8 2018, April, from Business Insider. http://www.businessinsider.com/dao-hacked-ethereum-crashing-in-value-tens-of-millions-allegedly-stolen-2016-6

Reich, C. (1991). The Individual Sector. *The Yale Law Journal, 100*(5), 1409–1448.

Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, 21*(2), 120–126.

Stevenage, S., & Spreadbury, J. (2006). Haven't We Met Before? The Effect of Facial Familiarity on Repetition Priming. *British Journal of Psychology, 97*(1), 79–94.

Sullivan, C. (2007). Who's Who—Conceptualising Identity. *International Review of Law, Computers and Technology, 21*(3), 237–261.

Sullivan, C. (2010). *Digital Identity: An Emergent Legal Concept*. Adelaide: University of Adelaide Press.

Sullivan, C. (2012). Digital Identity and Mistake. *International Journal of Law and Information Technology, 20*(3), 223–241.

Sullivan, C. (2016). Digital Citizenship and the Right to Digital Identity Under International Law. *Computer Law and Security Review, 32*, 474–481.

Sullivan, C., & Burger, E. (2017). E-residency and Blockchain. *Computer Law & Security Review, 33*(4), 470–481.

Tempelhof, S., Teissonniere, E., Tempelhof, J., & Edwards, D. (2017, April). Retrieved April 8, 2018, from Bitnation Pangea | Your Blockchain Jourisdiction. https://github.com/Bit-Nation/Pangea-Docs/raw/master/BITNATION%20Pangea%20Whitepaper%202018.pdf

United Nations. (2015). *Transforming Our World: The 2030 Agenda for Sustainable Development*. Retrieved April 8, 2018, from https://sustainabledevelopment.un.org/post2015/transformingourworld

Walker, P., & Hewstone, M. (2006). A Perceptual Discrimination Investigation of the Own-Race Effect and Intergroup Experience. *Applied Cognitive Psychology, 20*(4), 461–475.

10

Blockchain Entrepreneurship and the Struggle for Trust Among the Unbanked

Guillermo Jesús Larios-Hernández and Almendra Ortiz-de-Zarate-Béjar

Introduction

Measured as the number of bank accounts, the World Bank's Global Findex Database discovers that around 38% of the world population lacks formal financial services, the latter considered instrumental to facilitate investment and consumption among the population (Demirguc-Kunt et al. 2015). Consequently, universal financial inclusion has developed into an aspirational goal for governments, world institutions, social entrepreneurs and, in general, the whole financial system. However, the majority of persons at the Bottom-of-the-Pyramid (BoP) who possess a bank account typically do not use it and continue to recur to informal practices (Allen et al. 2012).

G. J. Larios-Hernández (✉) • A. Ortiz-de-Zarate-Béjar
Facultad de Economía y Negocios, Universidad Anáhuac México, Huixquilucan, Mexico

Facultad de Estudios Globales, Universidad Anáhuac México, Huixquilucan, Mexico
e-mail: guillermo.lariosh@anahuac.mx; almendra.ortiz@anahuac.mx

H. Treiblmaier, R. Beck (eds.), *Business Transformation through Blockchain*,
https://doi.org/10.1007/978-3-319-99058-3_10

The literature lists a variety of socioeconomic factors that influence individuals in the BoP in their decisions to use or reject formal financial services. Among others, the most relevant of these are low income (Beck and De la Torre 2007; Kundu 2015), lack of education (Beck and Demirguc-Kunt 2008; Lusardi 2008; Fox et al. 2005; Hastings et al. 2013; Vázquez 2015), risks related to cashflow limitations and credit traps (Collins et al. 2009), geographical barriers (Beck and De la Torre 2007; Beck et al. 2008), high transactional costs (Demirguc-Kunt and Klapper 2013), and poor financial literacy (Mandell 2006, 2008; Hilgert et al. 2003), suggesting a sort of fundamental impossibility to access financial services. Nonetheless, when scholarly research extends beyond such raw barriers, other non-monetary explanations that affect financial decision-making shed light on additional relevant factors at work around the incumbent financial system, particularly those relating to informal over formal financial practices (Keizer 2016) and lack of trust (Ennew and Sekhon 2007), which may offer other approaches for building alternative financial solutions for the unbanked.

Conceptual roots for financial inclusion originate in the study of microfinance, an endeavor that involves small credit programs for the poor (Prahalad 2005), whose business model required testing and validation to develop trust among the poor (Yunus and Weber 2007). Global expansion of the financial system and the search for economic growth inspired the world's institutional framework to plan for a more ambitious project, which would consider not only access to credit, but also the availability and use of a larger portfolio of financial products (Beck et al. 2007). However, the common sense of the institutional world appears to have ignored the process of trust creation that microfinancing originally revealed.

The Blockchain Potential

Increasingly valued by entrepreneurs, practitioners and, more recently, scholars, blockchain is conceived of today as a promising alternative for financial inclusion. Entrepreneurial ingenuity has developed blockchain-based solution proposals for the unbanked, including money transfer, financing, and proof-of-asset existence, among a variety of other applications, generating an alternative structure for persons to engage in transactions. As an Internet-based platform, blockchain not only is expected to transform the mechanisms of value exchange, but also how and whom people trust (Botsman 2017).

Blockchain is not about creating an alternative currency but rather smarter applications, as it has been found that the usage of the technology as money is not the rule but the exception (Sas and Khairuddin 2017). For the creation of new applications, entrepreneurs emphasize the technology's disintermediation features over centralized approaches. Hence, based on transactional endorsement through encrypted peer consensus, blockchain encourages a type of inclusive innovation for the unbanked, whose main expectation relies on the development of a new type of trust. Essentially, Piscini et al. (2017) define blockchain as the gatekeeper of the emerging trust economy.

Trust appears to be at the core of the adoption of blockchain solutions, particularly for financial inclusion; nevertheless, the concept has more than one definition. In this chapter, we propose that trust-creation properties, as understood by the proponents of blockchain solutions, do not necessarily correspond to the type of trust with which the unbanked are concerned. This perspective suggests an additional effort from entrepreneurs and practitioners to match blockchain capabilities with the true trust requirements of the unbanked, which tend to be contextual and based on informal practices.

Chapter Structure

The first part of this chapter deals with a concept of trust that originates in the realization of the practices of the unbanked. New financial services and the individuals using them need to be worth trusting in order to achieve an effective service adoption. This part elaborates on the key elements that build trust in informality, followed by an analysis of the role and the impact of technology. The second part reviews the concept of trust from the perspective of the blockchain, assessing and criticizing over-expectations of the technology and its decentralization properties, particularly in the context of the unbanked. After this evaluation, the third part narrows the discussion to the suggestion of situations in which the blockchain makes sense as a potential solution for financial inclusion, highlighting how the practice of the informal becomes relevant for the entrepreneur interested in blockchain solutions to the financial inclusion problem. Finally, we provide a narrative of qualitative interviews from a group of Mexican unbanked persons as empirical support for the chapter's discussion, closing this chapter with concluding remarks.

Understanding Trust in the Context of the Unbanked

Trust, merely defined as "the willingness to be vulnerable" (Sas and Khairuddin 2017), is a designation which depends on the relational and contextual elements involved in the system where trust is to be realized. There are internal factors (memory, information and perceived probabilities, resistance to change, confidence, aversion to risk, emotional state, inability to predict the future or expectations) and external elements (social environment and interdependence, access to information) that influence individuals' trust and decision-making processes (Rousseau et al. 1998; Samson 2014) (see Fig. 10.1). Another approach finds that trust depends on contextual characteristics such as temporal, social, and institutional embeddedness, and on intrinsic properties, namely motivation, integrity, and benevolence (Riegelsberger et al. 2005; Sas and Khairuddin 2017).

However, the abundance of elements in the definition of the concept renders its measurement too complex for viable application. Although scholars have developed different models that attempt to measure trust or confidence (Mayer and Davis 1999), its intangibility hinders the possibility of creating a model capable of calculating trust for all approaches. Hence, trust has been evaluated for specific contexts and usages. For instance, the Edelman Trust Barometer has been designed to evaluate people's trust in a variety of environments, such as institutions, social media, financial services, markets, and technology, among others (Edelman Trust Barometer 2018). Not surprisingly, its 2017 results emphasized the global upsurge of a crisis of trust, indicating the financial services sector as the least trustable.

In another example, the Financial Services Research Forum developed an index to measure trust in institutions, which considered four elements that constitute a vision of trust: risk, interdependence among stakeholders, vulnerability, and future expectations (Ennew and Sekhon 2007).

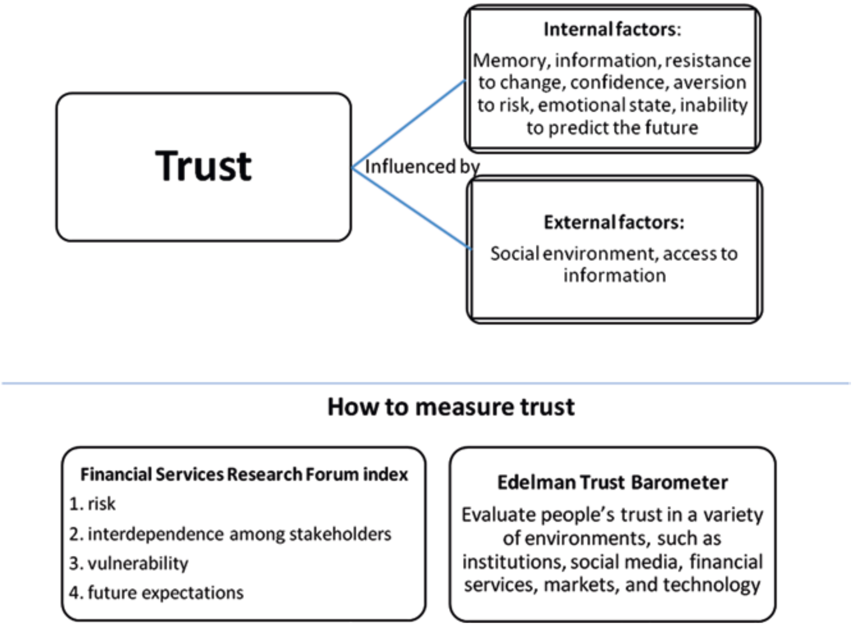

Trust
Influenced by
Internal factors:
Memory, information, resistance to change, confidence, aversion to risk, emotional state, inability to predict the future
External factors:
Social environment, access to information
How to measure trust
Financial Services Research Forum index
1. risk
2. interdependence among stakeholders
3. vulnerability
4. future expectations
Edelman Trust Barometer
Evaluate people's trust in a variety of environments, such as institutions, social media, financial services, markets, and technology

Fig. 10.1 Understanding trust in the context of the unbanked

Although the index has been specifically designed for the financial sector, it is important to consider that it only focuses on persons who already participate in financial services, without taking into account individuals who do not use these services, namely the unbanked.

If the usefulness of a multifactorial definition of trust is context-dependent, we should be more concerned about the appropriate constituents that build trust in the context of financial inclusion and the unbanked. This is particularly relevant since financial inclusion surveys indicate that trust is the most relevant factor influencing the unbanked (Shaw 2014; Allen et al. 2012).

The Building of Trust

Trust plays a decisive role in the use and offer of any type of financial services, influencing the decision-making processes that develop in the minds of people that eventually lead to the use or rejection of such services (Schul and Peri 2015). Individuals would be eligible for financial services as long as transactions make sense for both the financial offeror (the institutions, in the case of the formal financial system) and users. For instance, when banks' requirements make it inoperable for the unbanked to seek formalization, an indicator of constricted institutional-enforcement mechanisms, they encourage distrust in both parties.

Trust and enforcement mechanisms make financial transactions possible and, when enforcement is restricted, more trust is required (Christopher 2016), creating a wider gap between the financial system and the unbanked. This lack of access to financial services, specifically in poor and isolated areas, motivates a custom of low expectations regarding the formal system and low interaction with institutions. Thus, higher trust requirements by the formal financial system breeds distrust among the unbanked, prompting them to opt for alternative informal financing systems, which also generate their own trust-building structures.

These structures appear to follow a relational outline, as higher income uncertainty and risk among the unbanked engender a situation of vulnerability that makes interdependence, that is, trust, a key element of the informal system (Ennew and Sekhon 2007). Thus, informal mechanisms influence the building of trust, which does not necessarily respond to rationality (Krueger et al. 2008) and which takes place within a particular social framework (context). Trust also comes to evolve over time, since its permanence is highly volatile, as it has been shown that trust is different before and after an economic crisis (Shim et al. 2013), depending on the emotional expectations that determine people's propensity to contemplate vulnerability from a favorable perspective (Colquitt et al. 2007).

Vulnerability can be more tolerable when financial offerors and users know each other, because it has been found that geographic proximity is essential to stimulate trust between both parties, creating an environment in which individuals can resolve doubts nearly immediately and ensure that commitments are properly observed (Filipiak 2016). Additionally, the level of trust that can be created is highly dependent on the individuals' previous experiences (Shim et al. 2013), emphasizing the importance of the reputation that both the financial offeror and the user generated, as well as the context in which transactions are supposed to take place. As elements that characterize human confidence, past experiences, physical

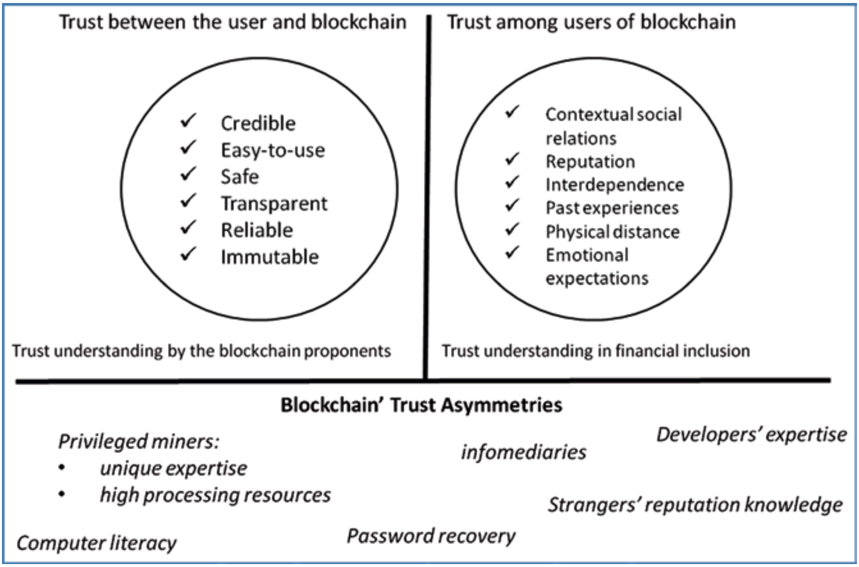

Trust between the user and blockchain
Trust among users of blockchain
✓ Credible
✓ Easy-to-use
✓ Safe
✓ Transparent
✓ Reliable
✓ Immutable
✓ Contextual social relations
✓ Reputation
✓ Interdependence
✓ Past experiences
✓ Physical distance
✓ Emotional expectations
Trust understanding by the blockchain proponents
Trust understanding in financial inclusion
Blockchain' Trust Asymmetries
Privileged miners:
• unique expertise
• high processing resources
infomediaries
Developers' expertise
Strangers' reputation knowledge
Computer literacy
Password recovery

Fig. 10.2 The blockchain trust dichotomy

distance, reputation, emotional expectations, and interdependence are some of the constituents that reside at the core of trust creation among the unbanked as well (see Fig. 10.2), which together build the systemic structures of informality. These constituents are context-dependent, and their understanding is instrumental for trust creation, especially if blockchain-based applications are to achieve effective acceptance among the unbanked.

Trust and Technology

Technology has become an important tool for boosting the use of financial services, including digital wallets, near field communication devices, peer-to-peer payments, cryptocurrencies, and others, which become instrumental in reducing transactional costs among all users, including the poorest. For successful implementation, trust in the technology is indispensable and social processes appear to be the correct mechanisms to generate such trust (Sas and Khairuddin 2017). Moreover, use of the

Internet heightens the relevance of trust for Person-to-Person (P2P) transactions; hence, identity and reputation become highly valuable and vulnerable (Piscini et al. 2017).

As negative sentiments about banks spread online, the Internet erodes trust in financial institutions, and trust correlates negatively to low income (Fungacova et al. 2016), an effect that adds to motivational reluctance to the utilization of formal services. The emergence of mobile technologies has significantly reduced transactional costs, provided that extended digital connectivity, open markets, and the development of financial alternatives constitute building blocks for an inclusive digital finance (Manyika et al. 2016). However, information networks supported by Information and Communication Technologies (ICT) have created new economic spaces of informational flows that are typically dominated by a few players (Castells 1991). Existing ICT-based efforts for financial inclusion follow this logic of control, as they remain centralized in institutions that develop asymmetrical networks aimed at connecting the unbanked.

Therefore, the task related to developing trust in the context of digital financial services for the unbanked is incomplete if financial inclusion efforts do not seek to empower users concerning the usage of technology, which requires a proper understanding of the context within which the unbanked are immersed. In the end, people's willingness and acceptance of ICT-based services determine successful financial inclusion strategies, and the increasing variety of solutions that have emerged (e.g., mobile banking) appears suitable for overcoming some of the barriers to financial inclusion (e.g., geography and cost); notwithstanding this, new trust mechanisms need to be created.

Technology cannot be trustable by itself; for financial inclusion, it needs to be trustable as a transactional mechanism, usable by the unbaked, and contextually satisfying. Even so, when technology is involved, trust can be understood from two different approaches: trust between users and the technology, which needs to be perceived as credible, easy-to-use, and safe, and trust among the people that interact with the technology (Sas and Khairuddin 2017)—see Fig. 10.2. While blockchain trust-related concerns refer to the former, the problem of financial inclusion appears to be more relevant in the latter. In other words, trust among the unbanked depends on contextual social relations, which need to be understood and leveraged by the blockchain entrepreneur in order to reach an effective appropriation of the solution. This understanding of trust mismatches the key concerns surrounding the concept expressed by blockchain technology designers, as we discuss in the following section.

Blockchain and the Demand for Trust: Insufficient but Necessary?

Proponents of blockchain technology indicate that traditional institutional trust and its associated trusted intermediaries are being put into question, especially considering that new technology gives birth to new infomediaries, including those that develop around the distributed immutable ledger (Botsman 2017). As discussed in the previous section, ICT have certainly achieved remarkable efficiencies and continue to promise the attainment of many more that lead to the elimination of several existing intermediating activities. Additionally, we must admit that there are many reasons to distrust our current institutions, which have been associated with corruption, the erosion of social values, or the inability to properly manage the pace of change, among others (Edelman Trust Barometer 2018).

However, honest advocates of the ledger depart from a paradigm that vilifies centralization and intermediation as inherently contaminated, paying no attention to the application or context, and blockchain technology's trust enabling notion is defined in terms of transparency, data integrity, and immutability (Seebacher and Schüritz 2017). These supporters propose a definition of trust that originates in cryptography and theoretical benefits resulting from the algorithmic scattering of decision power.

In fact, this common appreciation of trust has been distinguished as the key component of blockchain technology, in the belief that as long as members trust the blockchain platform, peer-to-peer trust becomes unnecessary (Leibowitz 2016), assuming that blockchain's disintermediation features would be a preferred option over the incumbents' centralized approach. Under such an asseveration, we are compelled to question, from a conceptual perspective, if trusting the blockchain platform is different from the placing of people's confidence in an institution of the current banking system.

Advocates expect blockchain cryptology to replace third-party intermediaries as the trust guarantor (Piscini et al. 2017). However, trust in the blockchain platform appears to be solely another form of institutional trust, relegating the relevance of trust in individual members (Jarvenpaa and Teigland 2017), where trust is being transferred from social confidence to a new form of algorithmic regulation (O'Dwyer 2015). This interpretation might imply that blockchain technology is not really trustless, in that trust is placed in the algorithm itself (Christopher 2016).

Expectations surrounding the ability of the shared distributed ledgers to overcome the financial intermediaries' privileged knowledge and relationships appear to ignore that new information asymmetries are generated by the blockchain business model, particularly in the form of trust (Venegas 2017). As shown in Fig. 10.2, Some of these asymmetries include privileged miners with unique expertise and high processing resources, infomediaries who deal with strangers' unknown reputation, developers' expertise, password recovery, computer literacy, and so on. As Venegas (2017) indicates, trust asymmetry is only a type of information asymmetry.

Perhaps blockchain technology is to a greater extent about systemic versus individual control power, and not about trust (Meijer 2017). Some scholars have provided valid arguments that support this line of reasoning. For instance, the proof-of-work consensus algorithm, such as that of Bitcoin, has been branded as another case of a savage, capitalistic, wasteful accumulation-seeking governance model that leads to centralization (Bacia 2018), as demonstrated by the limited number of miners that dominate the market. Another study finds that unelected developers become the decision makers behind system upgrades, acquiring a disproportionate level of control over the functioning of the platform (Scott 2016). In general, the blockchain algorithm still needs improvement and it has proven not to be as robust as its popularity indicates (Christopher 2016). Trust creation for the success of the platform becomes instrumental, as in the case of many other organizational-led initiatives around financial inclusion.

On the other hand, some centralized programs have proved to be appropriate for financial inclusion. Programs such as M-PESA in Kenya and G-Cash in the Philippines, which use technology to integrate the unbanked into the formal economy, have had great success in developing economies; other governments have sought to replicate these in other regions of the world. As branchless access mechanisms for financial services, mobile networks are also instrumental for blockchain and financial inclusion; no other access technology appears to be as available, affordable, acceptable, and appropriate for creating awareness among the poor (Anderson and Billou 2007), affecting their financial behavior (Demirguc-Kunt and Klapper 2013) by crafting new forms of value creation and capture (Santos 2012).

Therefore, to reach the unbanked with solutions to the financial inclusion problem, trust in the blockchain platform still needs to be generated, but not on the basis of its architectural design, whose featural advantages may be partly supported by the conjunctural inefficiencies and deficiencies of the incumbent financial system. Entrepreneurs would need to recognize trust far beyond what is emphasized by the proponents of the technology, whose algorithmic characteristics may be necessary for trustable platform operation and robustness, but insufficient to convince a sector of the population living in an alternative informal financial system. The building of trust between the unbanked and the blockchain platform poses important challenges, considering that the proposed financial services may appear as only another commercial service offer to the potential users. Effective appropriation of the solution would depend on how the proposed financial inclusion instrument encourages contextual trust relations among the unbanked, and between the unbanked and the offerors of financial services.

Empathizing with Informal Practices: The Task of the Blockchain Entrepreneur

As discussed at the beginning of the chapter, financial exclusion at the lowest socioeconomic levels can be explained by lack of access, the high operational costs to maintain a formal bank account, or not being able to afford sufficient money to save. As such, the unbanked distance themselves from formal financial services, because the latter make no sense to them. We also indicated previously that there are other non-monetary reasons that may exert a greater impact on the financial decision-making process, independently of the socioeconomic level, that is, non-monetary reasons explain the existence of the unbanked in terms of a variety of financial services, including those related with technology. Avoiding all sorts of naïve stigmatizations, blockchain entrepreneurs need to acknowledge the importance of context and trust-creation mechanisms that influence the financial decision-making of a particular group of unbanked persons (Larios-Hernández 2017).

Flood and Robb (2017) indicate that blockchain makes sense only if problems exist concerning fraud, intermediation services, service performance, or the stability of data applications, leaving the overexcitement surrounding blockchain as solely another case of anarchy-capitalist dreaming. In the case of the unbanked, problems associated with fraudulent situations, expensive intermediation, and deficient service performance endure, representing an interesting opportunity for the blockchain practitioner. As the intended members of the blockchain network, the unbanked would adopt financial services as long as the solution design proves its usefulness according to their contextual needs, whose familiarity with the practice would ease acceptance, beyond the disintermediation ideology of the blockchain proponents.

Certainly, blockchain entrepreneurs might be perceived by the unbanked as only another commercial organization attempting to provide them with financial services for a profit, but the former may have an advantage over closed-door policy banks, in that entrepreneurial business models can be more achievable with respect to the aspirations of persons with low income. As described by Tapscott and Tapscott (2016), the incumbent financial system has its own private blockchain proposals, which assign permissions to authorized ledgers; initiatives such as R3CEV and the Hyperledger Project are examples of banks' efforts to enforce their model for blockchain.

However, the World Bank statistics demonstrated that not all individuals excluded from the financial system respond positively to existing institutional programs for inclusion (Demirguc-Kunt et al. 2015). To some extent, these initiatives appear to implicate certain degree of wishful thinking, as they overlook the banks' refusal to place emphasis on what traditional financial judgment considers unattractive markets, given the right-end position of persons with a low income in the Pareto long tail curve (Serrano-Cinca and Gutiérrez-Nieto 2014). As indicated by Serrano-Cinca and Gutiérrez-Nieto (2014), banking systems that target this sector, such as microfinance, experience high administrative costs. Hence, a deeper characterization of financial practices and motivations for financial inclusion would provide insights that may eventually lead to the development of alternative solutions and, potentially, opportunities for entrepreneurship.

Trust in the Practice of Distributed Financing Among the Unbanked

As discussed previously, the sole fact of possessing disintermediated architecture is no indicator that blockchain-based solutions are appropriate for financial inclusion. However, there are some situations, such as those listed by Flood and Robb (2017), in which a distributed service offer may prove appropriate. Usually, decentralized local interactions increase social trust, as has been validated by existing social media and mobile technologies, which develop social capital with potential to lead toward better individual capabilities and, consequently, inclusion (Wang 2015). Blockchain is an alternative to self-organization, potentially attractive among persons in informal financing systems, since self-organization is the process behind informality and family financing, where trust relations represent strong ties among the participants.

Based on an analysis of relevant factors that are present in cases characterized by certain levels of financial exclusion, Larios-Hernández (2017) suggests a set of sensitivities for the blockchain entrepreneur to appreciate informal practices among the unbanked. Some of these factors include people's source preferences for borrowing and saving, motivations behind their need for financial services, spending and saving habits and, naturally, access infrastructure (Demirguc-Kunt et al. 2015; Larios-Hernández 2017). In some of these practices, distributed social trust mechanisms sustain the functioning of the informal financing mechanisms.

For example, informal lending is customary in nations with low financial inclusion levels. Though purposes vary, borrowing from financial institutions is usually perceived negatively by the unbanked (lack of trust), because recurring to family, friends, and private informal lenders for financing is a preferred practice. This situation appears to reinforce the negative impact of lack of access in servicing the financially excluded. In another case, cash preferences and the conditions involved in informal saving practices are preferred over bank-related services. It has been found that although, in some cases, people have accounts in banks, they do not necessarily use them, nor do they seek to expand the portfolio of bank products offered, in that informal means are perceived as more flexible and more worthy of confidence (Ranjani and Bapat 2015). Hence, informal habits for peer-to-peer interactions distributed among the unbanked can be facilitated by blockchain technology, providing its members with more efficient financing enablers, which accommodate to their context, practices, and trust-creation mechanisms, as in the case of WeTrust, a blockchain-based platform to implement trusted lending circles.

For remittances, trust in international transactions is transferred from banks to the blockchain platform. However, cost advantages would not become sufficiently appealing to remove an intermediary if trust is compromised (Venegas 2017); hence, trust needs to be created first. Distinctively, some of the blockchain solutions offer international money-transfer services without imposing a bank account as a prior requirement (e.g., Everex, a blockchain-based remittances and micropayment solution to underserved individuals), relying on existing, trusted informal local networks for currency exchange between virtual and fiat money. Blockchain may continue to capture a share of international transactions as long as settlement remains less expensive and virtual currencies are used as instant exchange media, avoiding volatility effects (Venegas 2017).

In summary, a distributed transactional architecture may provide suitable solutions for a financial dynamic that favor disintermediated peer-to-peer local transactions, which can be cultivated in existing practices that are today classified as informal. Thanks to smartphones, access is ubiquitous and blockchain can make services fast and risk-efficient, as long as settlement mechanisms are effective and loans can be available from peers at lower transactional costs. In general, blockchain entrepreneurship would be an alternative route to enhancing informal financial services, which can be designed closer to the aspirational goals of the unbanked.

Exploratory Test: Unbanked Among the Banked

In order to explore the confidence factor among the unbanked, we conducted a series of semi-structured interviews to observe the behavior of the unbanked that interact on a regular basis with the banked. All interviews were conducted in the Spanish language in a wealthy neighborhood in Mexico City, and sought for the interviewees to present opinions related to financial services practices and trust.

All of the interviews were recorded, and the audios and notes of each case were analyzed in order to arrive at the results that we present. To construct the interview, we appropriated elements of the Financial Services Research Forum survey as a base, with certain modifications that allowed achieving the objective of collecting data that explain the behavior and confidence level of individuals who do not employ formal financial services. The socioeconomic profile of the interviewees is located at the D + level, that is, individuals with an approximate monthly income of $ 350–600 dollars. These persons are found above the poverty line in Mexico, which means that they have overcome the monetary barriers that separate them from the use of formal financial services. We explored the confidence factor in the decision to use or not use formal financial services.

Findings

For ease of presentation, we reveal the responses to four questions that we have selected as the most representative of the interviews that we conducted, and that are useful to explain in a convenient manner what trust means for financial services.

When we asked the interviewees if they trusted banks, the majority of the individuals responded “no”. The next question was, *Do you consider that you need to trust a bank in order to use it?* All of the interviewees said “yes”. It was interesting to listen to the bad experiences that persons have had with banks in the past:

> *I don't trust them because at the beginning they offer many solutions, but once you become a client, they will surely abuse you.*

Would a blockchain solution be more suitable for offering clear rules for the clients with transparent mechanisms so that an environment of trust can be built?

The majority of the interviewees considered that it is a good decision to save money in a safe place; however, a bank is not necessarily safe for them:

> *You can have all of your money in the bank, and suddenly a change in politics or something like that and you can lose your life savings from one day to the next.*

The majority of the individuals whom we interviewed showed a positive attitude toward the services offered by banks, mainly, savings and credit for investments; however, the majority exhibited a lack of trust in the institutions, not in the services. Supposedly, they would prefer to save money, but not in a formal institution or a bank. Blockchain technology supports the creation of smart contracts that can be used to generate trust and transparency in rules among the unbanked.

> *I have savings, but I prefer to keep them at home, or give my money to my mom.*

We perceived that the persons that we interviewed were reluctant to use banks because they did not trust them, so we explored their financial behavior. Blockchain technology can develop decentralized platforms to manage transactions amid small groups and to strengthen trust in financial transactions.

My first option to save or to ask for credit is…

Once we distinguished that persons do not trust banks, we attempted to understand what people did with their money:

> *If I need to keep my money in a safe place, I can have it in my house. If I need to ask for credit, I would surely ask my mom or family members.*

We observed that the majority of the interviewees preferred to save their money with family members, and to ask for money from people they knew. The main reasons were related to costs and trust, considering the small or null interest value that they would pay on borrowing from family members or friends. In addition, they chose this type of informal funding, which appeared more trustable for them than a bank:

> *Sometimes, when I need money, I become part of a "tanda." It is the best way to get a credit, in a short time with no interest or surprises.*

> *The problem with banks is that you always lose: when you save your money, you have to pay for the service, and when you ask for money, you pay a lot for the services, and it is not clear how much you will pay by the end. They always have small print at the end of the page. I don't trust them.*

Do you consider banks to be fair and honest?

It was interesting to see that people do not consider banks as providers of financial services that they can use. In general, banks are perceived as something that bothers them, but sometimes it is necessary to use them. They believe that people lose more than they earn when they approach a bank.

> *No, I consider that they are not fair because they take advantage of people at their time of need.*

> *They always charge interest on interest. They (banks) should be more sympathetic.*

When you have been at a bank, have they treated you respectfully?

Trust is not a matter of respect. Mostly, all of the interviewees considered that they were treated with respect when they have been at banks; however, that does not make a difference in relation to the level of trust that they have toward banks.

> *They always treat you fine. They listen to your demands, although they don't always provide a solution.*
>
> *Some banks have very well-trained personnel, and they tend to be nice and respectful. The problem with banks is not the people who work there; they are just doing their jobs. The problem is the bank itself.*

Based on these interviews, we have found that trust is a very important variable that people consider in their financial decision-making processes. Notably, trust is understood from a perspective that does not necessarily match how blockchain evangelists appreciate the concept. For the unbanked, trust is merely about the relationship between the financial offeror and the offerees. Hence, exploratorily, we endorse the importance of trust creation between the blockchain platform and the unbanked, suggesting that entrepreneurial sensitivity to the practices of informality is the key constituent that can boost the sense of trust among people using blockchain-based services.

Conclusion

Individuals entertain different aspirational levels, and their attempts to reach them will depend on the possibility of satisfying them (Selten 1988). People in poorer countries embrace aspirations that originate in higher thresholds of formal financial inclusion (societies at the upper end), which remain valid as long as aspirations are within a reachable distance from the actual situation of these populations (Genicot and Ray 2017). According to the theory of governance and agency, communality can be an alternative governance model that influences individuals if resources are limited (George et al. 2012). When access to financial services is denied due to the lack of access infrastructure or collaterals (resources), individuals are forced to seek alternative solutions. In other words, if the current financial system cannot satisfy these aspirations, individuals will seek alternatives, which we recognize today as informal.

This chapter has reviewed the role and meaning of trust surrounding the blockchain-based services that are expected to facilitate financial demands for the unbanked, whose informal practices are familiar and customary. Low-cost access infrastructure (e.g., mobile services) is obviously essential for financial inclusion, although this fact does not necessarily denote the use of financial products such as bank accounts, credit cards, or online services, among others; monetary and non-monetary motives explain the segregation of the unbanked. Similar issues may arise with regard to other innovative transactional technologies such as the blockchain if the trust-creation process and informal practices are poorly understood by entrepreneurs, the latter a circumstance that challenges entrepreneurial thinking in terms of value proposition.

If not properly designed, blockchain may follow the fate of other potentially disruptive technologies such as VoIP and mesh networks, which never really affected the highly centralized and growing cellular telecommunications industry (O'Dwyer 2015). The technology still needs to solve several technical and scalability issues (Larios-Hernández 2017). In blockchain, reputed systems are the key factor that build trust, and the export of reputation acquired in one platform to others remains a pending improvement (Piscini et al. 2017), which would prevent platform lock-in and offer fragmentation (Pouwelse et al. 2017), increasing compatibility and trust exchange among the unbanked. Other areas of opportunity include the lack of dispute-resolution mechanisms, wallet-owner identification, the impossibility of password recovery, and users fragmented as a result of a variety of alterative platforms (Pouwelse et al. 2017; Sas and Khairuddin 2017).

For the time being, for individuals who recur to informal financial services, blockchain technology solutions can leverage the trust generated by existing local peer-to-peer transactional habits by facilitating disintermediated mechanisms that enhance interactions and lower transactional costs. With the appropriate design of the blockchain, the ledger's decentralized approach would only be an alternative for value transfer, replacing the traditional "trusted" intermediary for a type of "trusted" infomediary, whose clear value proposition would prove its effectiveness in financial inclusion, moving away from the blockchain business model that produces the artificial scarcity of a socioeconomic system (Bacia 2018).

Entrepreneurs must acknowledge at least the two kinds of trust involved in the blockchain value proposition: on the one hand, trust between the unbanked and the platform needs to be generated, which will offer an alternative attestation instrument based on a distributed architecture, replacing or complementing privileged financial intermediaries. On the other hand, entrepreneurs are expected to be sufficiently sensitive to the systemic mechanisms of social trust created in informality, whose practices can be leveraged as long as the blockchain solution assimilates the context-aware service design that grants them a clear competitive advantage over the status quo, encouraging financial inclusion at the individual aspirational level.

Given that the least developed and developing economies undergo higher levels of financial exclusion, innovative blockchain-based solutions can be tested by taking into consideration their particular contexts. In the end, it was through experimentation and proper analysis of the people's informal practices that Yunus and Weber (2007) was able to attain a sustainable model for microfinancing. Eventually, novel business models can reach the status of semi-formal financing, which can make aspirational goals attainable by the unbanked. The intention behind introducing blockchain technology into services for financial inclusion is not to bank community networks, but to socialize the financial system, making it more trustable, plural, and affordable for people.

Scott (2016) indicates that usually only social elites possess the resources to escape weak institutional environments, suggesting that participation in the blockchain communitarian network is restricted, invalidating the techno-libertarian proposals that surround the potential of blockchain. Hence, public policy should facilitate financial inclusion beyond the banking system; the existing financial system's logic hardly accommodates informal practices, and there are many circumstances in which people find it advantageous to seek peers for financial transactions. Entrepreneurs who acknowledge these facts would be better positioned to develop affordable solutions that eventually influence governments in terms of public support. These alternatives may originate from entrepreneurship and social innovation, which would also support the state government agenda through strategies that encourage freedom and protection, apart from the particular interest and motivations of the banking system.

References

Allen, F., Demirguç-Kunt, A., Klapper, L. F., & Peria, M. S. M. (2012). *The Foundations of Financial Inclusion: Understanding Ownership and Use of Formal Accounts*. World Bank Policy Research Working Paper. http://documents.worldbank.org/curated/en/348241468329061640/The-foundations-of-financial-inclusion-understanding-ownership-and-use-of-formal-accounts. Accessed 18 Dec 2017.

Anderson, J., & Billou, N. (2007). Serving the World's Poor: Innovation at the Base of the Economic Pyramid. *Journal of Business Strategy, 28*(2), 14–21.

Bacia, M. (2018). *Trust-Less Governance Is the Killer App of Blockchain Technology*. A Medium Corporation. https://medium.com/the-mission/trust-less-governance-is-the-killer-app-of-blockchain-technology-1f5881b4e6ce. Accessed 20 Feb 2018.

Beck, T., & De la Torre, A. (2007). The Basic Analytics of Access to Financial Services. *Financial Markets, Institutions & Instruments, 16*(2), 79–117.

Beck, T., & Demirguc-Kunt, A. (2008). Access to Finance: An Unfinished Agenda. *The World Bank Economic Review, 22*(3), 383–396.

Beck, T., Demirguc-Kunt, A., & Levine, R. (2007). Finance, Inequality and the Poor. *Journal of Economic Growth, 12*(1), 27–49.

Beck, T., Demirguc-Kunt, A., & Peria, M. S. M. (2008). Banking Services for Everyone? Barriers to Bank Access and Use around the World. *The World Bank Economic Review, 22*(3), 397–430.

Botsman, R. (2017). How the Blockchain Is Redefining Trust. *WIRED*. https://www.wired.com/story/how-the-blockchain-is-redefining-trust/. Accessed 28 Feb 2018.

Castells, M. (1991). *The Informational City: Information Technology, Economic Restructuring, and the Urban-Regional Process*. Oxford: Basil Blackwell.

Christopher, C. M. (2016). The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain. *Nevada Law Journal, 17*(1), 139–180.

Collins, D., Morduch, J., Rutherford, S., & Ruthven, O. (2009). *Portfolios of the Poor: How the World's Poor Live on $2 a Day*. Princeton: Princeton University Press.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, Trustworthiness, and Trust Propensity: A Meta-Analytic Test of their Unique Relationships with Risk Taking and Job Performance. *Journal of Applied Psychology, 92*(4), 909–927.

Demirguc-Kunt, A., & Klapper, L. (2013). Measuring Financial Inclusion: Explaining Variation in Use of Financial Services Across and Within Countries. *Brookings Papers on Economic Activity*, *1*(Spring), 279–340.

Demirguc-Kunt, A., Leora, F. K., Singer, D., & Van Oudheusden, P. (2015). *The Global Findex Database 2014: Measuring Financial Inclusion Around the World*. World Bank Policy Research Working Paper No. 7255. http://documents.worldbank.org/curated/en/187761468179367706/pdf/WPS7255.pdf. Accessed 8 Dec 2017.

Edelman Trust Barometer. (2018). *Edelman Trust Barometer: Executive Summary*. http://cms.edelman.com/sites/default/files/2018-02/2018_Edelman_TrustBarometer_Executive_Summary_Jan.pdf. Accessed 20 Mar 2018.

Ennew, C., & Sekhon, H. (2007). Measuring Trust in Financial Services: The Trust Index. *Consumer Policy Review, 17*(2), 62–68.

Filipiak, U. (2016). Trusting Financial Institutions: Out of Reach, Out of Trust? *The Quarterly Review of Economics and Finance, 59*(C), 200–214.

Flood, J., & Robb, L. (2017, November). *Trust, Anarcho-Capitalism, Blockchain and Initial Coin Offerings* (pp. 1–25). Griffith University Law School Research Paper No. 17–23.

Fox, J., Bartholomae, S., & Lee, J. (2005). Building the Case for Financial Education. *Journal of Consumer Affairs, 39*(1), 195–214.

Fungacova, Z., Hasan, I., & Weill, L. (2016). *Trust in Banks*. BOFIT Discussion Papers No. 7. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2782358. Accessed 7 Dec 2017.

Genicot, G., & Ray, D. (2017). Aspirations and Inequality. *Econometrica, 85*(2), 489–519.

George, G., McGahan, A. M., & Prabhu, J. (2012). Innovation for Inclusive Growth: Towards a Theoretical Framework and a Research Agenda. *Journal of Management Studies, 49*(4), 661–683.

Hastings, J. S., Madrian, B. C., & Skimmyhorn, W. L. (2013). Financial Literacy, Financial Education, and Economic Outcomes. *Annual Review of Economics, 5*(1), 347–373.

Hilgert, M. A., Hogarth, J. M., & Beverly, S. G. (2003). *Household Financial Management: The Connection Between Knowledge and Behavior*. https://www.federalreserve.gov/pubs/bulletin/2003/0703lead.pdf. Accessed 20 Feb 2018.

Jarvenpaa, S., & Teigland, R. (2017). Trust in Digital Environments: From the Sharing Economy to Decentralized Autonomous Organizations. *Proceedings of the 50th Hawaii International Conference on System Sciences*. https://pdfs.semanticscholar.org/62bf/f772aa53596fc3dc1fd8a078abcfba87330b.pdf. Accessed 12 Jan 2018.

Keizer, B. (2016). *Financial Inclusion and Characteristics of the Unbanked: A Survey Analysis*. MSc Dissertation, Erasmus University Rotterdam.

Krueger, J. I., Massey, A. L., & DiDonato, T. E. (2008). A Matter of Trust: From Social Preferences to the Strategic Adherence to Social Norms. *Negotiation and Conflict Management Research, 1*(1), 31–52.

Kundu, D. (2015). Addressing the Demand Side Factors of Financial Inclusion. *Journal of Commerce and Management Thought, 6*(3), 397–417.

Larios-Hernández, G. J. (2017). Blockchain Entrepreneurship Opportunity in the Practices of the Unbanked. *Business Horizons, 60*(6), 865–874.

Leibowitz, J. (2016). Blockchain's Big Innovation Is Trust, Not Money. C*oindesk*. https://www.coindesk.com/blockchain-innovation-trust-money/. Accessed 20 Feb 2018.

Lusardi, A. (2008). *Household Saving Behavior: The Role of Financial Literacy, Information, and Financial Education Programs*. National Bureau of Economic Research. http://www.dartmouth.edu/~alusardi/Papers/Literacy_Information_Education.pdf. Accessed 8 Dec 2017.

Mandell, L. (2006). *Financial Literacy: If It's So Important, Why Isn't It Improving?* Networks Financial Institute Policy Brief. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=923557. Accessed 8 Dec 2017.

Mandell, L. (2008). Financial Literacy of High School Students. In L. Mandell (Ed.), *Handbook of Consumer Finance Research* (pp. 163–183). New York: Springer.

Manyika, J., Lund, S., Singer, M., White, O., & Berry, C. (2016). *Digital Finance for All: Powering Inclusive Growth in Emerging Economies*. McKinsey Global Institute. https://www.mckinsey.com/~/media/McKinsey/Global%20Themes/Employment%20and%20Growth/How%20digital%20finance%20could%20boost%20growth%20in%20emerging%20economies/MGI-Digital-Finance-For-All-Executive-summary-September-2016.ashx. Accessed 8 Dec 2017.

Mayer, R. C., & Davis, J. H. (1999). The Effect of the Performance Appraisal System on Trust for Management: A Field Quasi-Experiment. *Journal of Applied Psychology, 84*(1), 123–136.

Meijer, D. B. (2017). *Blockchain Technology: Trust and/or Control?* https://pdfs.semanticscholar.org/4386/5e89dec44e9305086013c9c0999bfb8c6281.pdf Accessed 28 Feb 2018.

O'Dwyer, R. (2015). *The Revolution Will (Not) Be Decentralised: Blockchains*. http://commonstransition.org/the-revolution-will-not-be-decentralised-blockchains/. Accessed 10 Feb 2018.

Piscini, E., Hyman, G., & Henry, W. (2017). Blockchain: Trust Economy Tech Trends 2017. *Deloitte Insights*. https://www2.deloitte.com/insights/us/en/focus/tech-trends/2017/blockchain-trust-economy.html. Accessed 9 Jan 2018.

Pouwelse, J., de Kok, A., Fleuren, J., et al. (2017). Laws for Creating Trust in the Blockchain Age. *European Property Law Journal, 6*(3), 321–356.

Prahalad, C. K. (2005). *La oportunidad de negocios en la base de la pirámide: un modelo de negocio rentable, que sirve a las comunidades más pobres*. México: Editorial Norma.

Ranjani, K. S., & Bapat, V. (2015). Deepening Financial Inclusion Beyond Account Opening: Road Ahead for Banks. *Business Perspectives and Research, 3*(1), 52–65.

Riegelsberger, J., Angela Sasse, M., & McCarthy, J. D. (2005). The Mechanics of Trust: A Framework for Research and Design. *International Journal of Human-Computer Studies, 62*(3), 381–422.

Rousseau, D. M., Sim, B. S., Burt, R. S., & Camerer, C. (1998). Not So Different After All: A Cross-Discipline View Of Trust. *Academy of Management Review, 23*(3), 393–404.

Samson, A. (Ed.). (2014). *The Behavioral Economics Guide 2014*. Behavioral Science Group. https://www.behavioraleconomics.com/the-be-guide/the-behavioral-economics-guide-2014/. Accessed 10 Jan 2018.

Santos, F. M. (2012). A Positive Theory of Social Entrepreneurship. *Journal of Business Ethics, 111*(3), 335–351.

Sas, C., & Khairuddin, I. E. (2017). Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, Denver (pp. 6499–6510). New York: ACM.

Schul, Y., & Peri, N. (2015). Influences of Distrust (and Trust) on Decision Making. *Social Cognition, 33*(5), 414–435.

Scott, B. (2016). *How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?* Geneva: UNRISD. www.unrisd.org/80256B3C005BCCF9/search/196AEF663B617144C1257F550057887C?OpenDocumente. Accessed 10 Jan 2018.

Seebacher, S., & Schüritz, R. (2017). Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review. In S. Za, M. Drăgoicea, & M. Cavallari (Eds.), *Exploring Services Science. IESS 2017. Lecture Notes in Business Information Processing* (pp. 12–23). Rome: Springer.

Selten, R. (1988). The Equity Principle in Economic Behavior. In *Models of Strategic Rationality. Theory and Decision Library C (Game Theory, Mathematical Programming and Operations Research)* (Vol. 2, pp. 269–281). Dordrecht: Springer.

Serrano-Cinca, C., & Gutiérrez-Nieto, B. (2014). Microfinance, the Long Tail and Mission Drift. *International Business Review, 23*(1), 181–194.

Shaw, N. (2014). The Mediating Influence of Trust in the Adoption of the Mobile Wallet. *Journal of Retailing and Consumer Services, 21*(4), 449–459.

Shim, S., Serido, J., Bosch, L., & Tang, C. (2013). Financial Identity-Processing Styles Among Young Adults: A Longitudinal Study of Socialization Factors and Consequences for Financial Capabilities. *Journal of Consumer Affairs, 47*(1), 128–152.

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York: Penguin.

Vázquez, A. (2015). Determinantes para participar en el mercado formal de productos financieros: El caso del ahorro y del crédito en México. *Estudios Económicos CNBV, 3*, 73–108.

Venegas, P. (2017). *Trust Asymmetry*. A Medium Corporation. https://medium.com/@economymonitor/https-medium-com-economymonitor-trust-asymmetry-in-the-blockchain-financial-system-8ba77dbaad41. Accessed 20 Feb 2018.

Wang, R. (2015). Internet Use and the Building of Social Capital for Development: A Network Perspective. *Information Technologies & International Development, 11*(2), 19–34.

Yunus, M., & Weber, K. (2007). *Creating a World Without Poverty: Social Business and the Future of Capitalism*. New York: BBS Public Affairs.

Part IV

Legal Issues

11

Blockchains and Smart Contracts: A Threat for the Legal Industry?

Bernhard Waltl, Christian Sillaber, Ulrich Gallersdörfer, and Florian Matthes

Blockchain, as a distributed data structure ensuring trust and establishing consensus among participants that do not know and potentially do not trust each other, is expected to change businesses in many different areas. One of these areas is the legal industry. How blockchain can potentially disrupt the legal industry is in the focus of this chapter. We differentiate three pillars of legal systems, namely (i) intermediaries and notary services; (ii) courts, judges, and trials; and (iii) companies and the financial market. We explore potential disruptions for each of them. We describe multiple scenarios which allow us to elaborate on the capabilities but also the limitations of blockchain technology.

B. Waltl (✉) • U. Gallersdörfer • F. Matthes
Software Engineering for Business Information Systems, Department of Informatics, Technical University of Munich, Munich, Germany
e-mail: b.waltl@tum.de; ulrich.gallersdoerfer@tum.de; matthes@tum.de

C. Sillaber
Institute of Computer Science, University of Innsbruck, Innsbruck, Austria
e-mail: christian.sillaber@uibk.ac.at

H. Treiblmaier, R. Beck (eds.), *Business Transformation through Blockchain*,
https://doi.org/10.1007/978-3-319-99058-3_11

Introduction

The blockchain, as the most prominent representative of distributed ledger technology, is expected to have the potential to disrupt many areas of modern societies (Tapscott and Tapscott 2016). These areas cover financial, social, and economic aspects of life. The technology has already proven to be an interesting and attractive system that has great potential to ensure trust among participants who do not necessarily know and trust each other (Swan 2015). A well-known success story has been its usage as a transaction ledger for cryptocurrencies such as Bitcoin or Ethereum.

There is strong evidence that the provided properties, especially those ensuring trust and decreasing transaction cost, can be used in the legal domain and make a significant impact there (Swan 2015). In this chapter we discuss the impact of blockchain technology on the legal industry and legal practice. To structure the discussion, to subsequently derive abstract principles and to determine open research directions, the field is divided into three different branches of legal industry and their related domains:

1. *Intermediaries and notaries*: A key task of the legal industry is the provision of trusted intermediaries and notary services, which can be considered neutral roles enabling various scenarios and providing a reliable infrastructure for innovation. Currently, these intermediaries need to be compensated accordingly by the parties that consume services. For example, they frequently receive a share of the transferred assets.
2. *Lawyers, judges, and trials*: Modern legal systems need an efficient and effective structure to enforce applicable laws (including, of course, bilaterally negotiated contracts). These systems usually differentiate the power between legislative, judicial, and executive branches. These structures are often vulnerable to fraud, for example, corruption, and induce legal uncertainty. Consequently, the enforcement (execution) of law is expensive and requires manual intervention and interpretation.
3. *Companies and financial markets:* A backbone of prosperous societies are efficient companies and an efficient capital market. Therefore, structures as defined and accepted in corporate law ensure the required

stability and legal certainty. Blockchain promises to enable new means of financing projects (e.g., Initial Coin Offerings [ICOs]) and governing businesses (e.g., Decentralized Autonomous Organizations [DAOs]).

This differentiation into three layers allows for a structured approach to outline the status quo and potential impact of blockchain within the legal industry. Figure 11.1 provides an overview of the use cases that we discuss within this article. Based on the technology stack of blockchain and smart contracts, eight different use cases are presented and discussed.

The remainder of the article reflects this structure: the section "Challenges and Opportunities for Intermediaries and Notaries" opens with some fundamental remarks on the usage of the blockchain and its impact at the intermediaries and notaries level. The concrete use cases *transfer of money, tokenization, and proof-of-identity* are discussed subse-

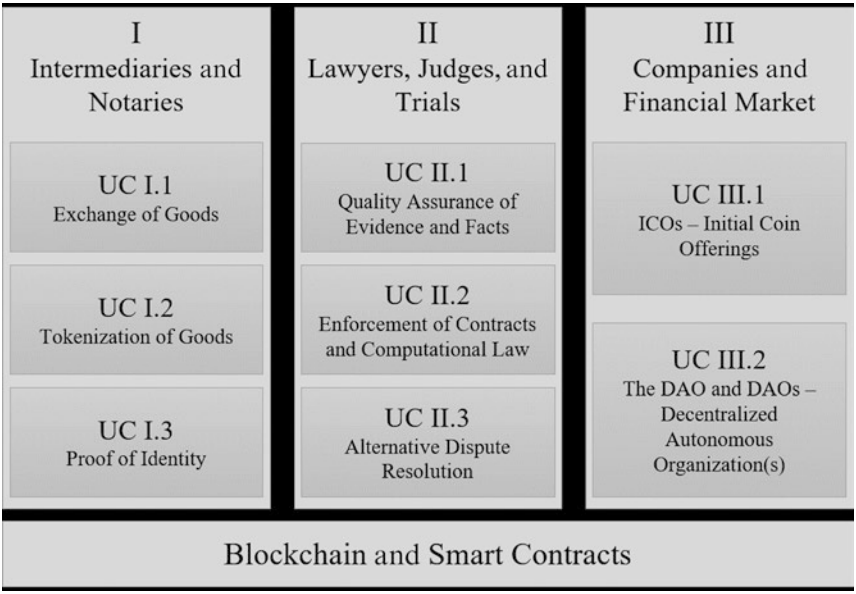

I
Intermediaries and Notaries
UC I.1
Exchange of Goods
UC I.2
Tokenization of Goods
UC I.3
Proof of Identity
II
Lawyers, Judges, and Trials
UC II.1
Quality Assurance of Evidence and Facts
UC II.2
Enforcement of Contracts and Computational Law
UC II.3
Alternative Dispute Resolution
III
Companies and Financial Market
UC III.1
ICOs – Initial Coin Offerings
UC III.2
The DAO and DAOs – Decentralized Autonomous Organization(s)
Blockchain and Smart Contracts

Fig. 11.1 Overview of the disruption scenarios on three levels of the legal industry, including "intermediaries and notaries", "lawyers, judges, and trials", and "companies and financial markets", illustrated in eight use cases (UC I.1—UC III.2)

quently. The section "Challenges and Opportunities for Lawyers, Judges, and Trials" continues with an in-depth inspection of the use cases that could make a significant impact on the work of lawyers, judges, and trials. These focus on data *provenance for evidence, the enforcement of contracts and computational law*, and *alternative dispute settlement* focusing on international arbitration. Finally, the section "Challenges and Opportunities for Companies and Financial Markets" briefly discusses the impact of blockchain technology on a systemically relevant part of our societies: corporates and financial markets. Based on the two concrete use cases, namely, *ICOs* and *DAOs*, the central role of technology as an enabler for radically new structures of corporate financing and control is illustrated.

Methodological Framework for the Analysis of Blockchain Scenarios

To structure the analysis of blockchain usage scenarios, a methodological framework is required that allows for the differentiation of the contribution of value and the level of impact accordingly. This chapter has reused and adapted the conceptual framework of Brenig et al. (2016). Brenig et al. originally proposed their framework to measure the value of a decentralized consensus system, that is, a data structure. We deviate from their original differentiation of layers but keep the distinction between three different layers. Brenig et al. do not—or only partially—take into account the interaction between the different blockchain solutions; we look at the interaction between those technological ecosystems more explicitly because the many different implementations of blockchain solutions differ heavily and are not interoperable without an additional service that allows exchanging of information. Ensuring the interoperability between smart contracts in various platforms has been identified as a research topic in recent projects.[1]

[1] For example: http://compk.stanford.edu/, last access on 03/27/2018.

Based on these considerations, the three layers that structure the analysis for the three different legal domains can be summarized as follows:

1. Ecosystem: Covers mainly technological aspects about the implementation of the blockchain. This domain also includes the parameters and design decisions that are taken into account to create the technical solution that stores the data and assures consensus among the participants.
2. Interaction: Addresses the means required to facilitate the exchange of information between blockchains and users. This includes both the interaction between blockchains and the blockchain and its users. Especially the integration of data from different blockchain solutions is relevant for a wide adoption in the legal industry as information from multiple sources will be required in various scenarios.
3. End user: Focuses on the involvement of individuals and organizations that use the technological platform to create and develop more advanced and innovative use cases.

This differentiation sets the baseline for the analysis of the blockchain scenarios that are discussed in the next sections.

Challenges and Opportunities for Intermediaries and Notaries

General Introduction

In today's society and economy, many services require the user to trust the provider. Primary examples are financial service providers providing a digital interface for the community to exchange money. The users themselves would not be able to send money digitally; therefore, they have to rely on a third party to ensure the transfer. However, these service providers represent a single point of failure (SOP); if they fail, the service itself does not work correctly anymore or is entirely unavailable. In this case, funds or other goods can be lost.

These services, called intermediaries or notaries, are likely to be disrupted by blockchain and distributed ledger technologies (DLT). Required as a third party for providing confidence among the participants, they can be replaced partially by blockchain because the technology solves the issue of lack of trust among users. The literature (Bailey and Yannis 1997) defines four different types of functions of intermediaries:

- Provide market information
- Provide trust relationships
- Integrity assurance
- Match buyer and seller

Especially to establish trust and integrity assurance, blockchain and DLT are likely to be used in the future. To understand the ways in which blockchain achieves this functionality, we have to look into the properties of blockchain technology. In general, distributed ledgers *are systems that enable parties who do not fully trust each other to form and maintain consensus about the existence, status, and evolution of a set of shared facts* (Brown 2016). Thus, a third party is likely to be redundant and will be eliminated due to cost. Furthermore, the blockchain provides transparency about all relevant processes to all involved users: besides achieving a consensus among the participants, the blockchain records all actions and steps in such a way that everyone to understand what steps taken by whom led to which outcome. Transparency is a crucial point, as processes of trusted third parties (e.g., decisions in dispute) are mostly not transparent or not comprehensible to other involved parties. This additionally increases the confidence in own choices and the results produced in such systems. Moreover, blockchain and DLT can offer significantly lower transaction fees in comparison to traditional intermediaries. Also, with the further standardization of trust processes within blockchain technology, the overall usage of such systems will increase, and intermediaries will be pushed out of the market. This implies that service providers and notaries have to restructure their business model and shift their focus to other possible value creation potentials. For example, there will be a need for all sorts of advisory services within this new ecosystem of blockchain and DLTs.

Objective variables which factor in the decision in case of disputes and the digital-only platform makes it easy to implement intermediary-like smart contracts[2] on the blockchain. In order to fully exploit the potential of the blockchain and to understand its disruptive nature, we discuss three concrete levels on which intermediaries play a significant role and possible ways they can be replaced by or supported through blockchain.

1. Exchange of goods
2. Tokenization of goods
3. Proof of identity

The design and implementation of self-governing systems always lacked a trusted infrastructure. Without an immutable, distributed system, no single entity can create a service where users can trust in the code itself, as a single entity is always able to manipulate the integrity of the software for its benefits. This of course leads to the intermediary concept itself, in which the platform provider is the trusted third party. Blockchains provide these services in a distributed and decentralized manner, and no one can modify the contents or the source code of the software running on the blockchain.

UC I.1: Exchange of Goods

Transferring assets, goods, ownership, or money requires some form of intermediary. The intermediary ensures the exchange between the participants so that no party can gain an unfair advantage. Regarding the intermediary, there are different factors to consider. In general, the trusted intermediary controls the ownership of exchanged goods. Traditionally, both transaction parties send their product or money to the intermediary which forwards them to the other participant. Of course, the intermediary benefits from a successful exchange as it wants to gain or maintain reputation, but the risk that it intentionally misbehaves or teams up with one side cannot be fully eliminated. In some cases (i.e., banks) asset ownership even remains at the bank fiduciary. In case of money, there is an additional layer of intermediaries: central banks issuing the money are

[2] A smart contract is software running in a blockchain. As long as the blockchain itself remains fully functional, the smart contract cannot be altered or stopped.

responsible for the stability of the currency. The intermediary is always involved, increasing the transaction costs and slowing down the process.

Blockchain and DLTs can partly mitigate these factors. The technology plays a vital role in transfer of ownership, assets, or money. We provide a simple example to give an insight into how blockchain increases the transaction speed and minimizes the cost and involvement of the intermediary. In cases in which an intermediary is needed still (because one good of the transaction cannot be transferred via blockchain), the monetary good could be transferred via a simple multi-signature wallet.[3] The first party (the buyer) sends the money to the wallet, the second party (the seller) sends the goods to the first party. If the goods are transferred correctly, only buyer and seller need to approve the transaction from the wallet to the seller. If the transaction fails, the intermediary has to resolve the issue and has to take sides, transferring the money to the seller or the buyer. Note, that if the transaction goes according to plan, the intermediary has no involvement at all. Using the blockchain, the seller receives the money without having to go through the intermediary, enhancing the process by reducing costs and transaction time. If all parties accept the blockchain-based virtual currencies, this process is feasible today.

UC I.2: Tokenization of Goods

However, other values or goods are not per se available on a blockchain where only a native virtual currency, such as Bitcoins or Ether[4] (Swan 2015) is usable by design. Tokenization is a new approach to use smart contracts for mapping goods onto the blockchain (Lemieux 2017). Users can create tokens with different purposes, technical foundations, legal status and underlying value. In this example, we focus on the asset-backed token, which is linked to a good in the real world. In the following example, one has to bear in mind that there are multiple layers of intermediaries. Consider buying real estate: the process of buying a house involves

[3] A multi-signature wallet is a contract which defines that n out of m parties are required to move funds from this wallet (in this case: $n=2$, $m=3$).

[4] Ether is the currency of the Ethereum Blockchain.

various intermediaries.[5] At first, real estate property is registered in a cadaster which acts as an intermediary, providing trust and the guarantee and proof of ownership. The second intermediary is the notary who functions as a witness and gatekeeper to the transaction and exchanges money for real estate, giving notice to the cadaster that the owner has changed. If the two intermediaries should be replaced with blockchain technology, first the land register has to be replaced by a distributed ledger.[6] This tokenizes the real estate. With tokenization of land, the blockchain can arguably provide a minimum level of trust among the citizens, as processes and data inside the network are transparent to all participants. As soon as the land register is fully tokenized on the blockchain, the notary becomes replaceable, too, as the blockchain handles the atomic transaction between money and real-estate-backed tokens. One of the parties sets up a smart contract which awaits both the payment and the transfer of real estate and exchanges them as soon as both goods are received. As the blockchain guarantees the execution of the smart contract, both parties trust the smart contract and execute it to carry out the trade.

Most certainly, not every asset can be tokenized on a blockchain. It can get complicated to register products of small value, as it is not cost-efficient anymore. Also, further aspects have to be considered: the notary provides other services besides trust and attestation. For example, he advises about legal consequences of transferring real estate. As the register itself has to be legally recognized as such on the blockchain, convincing the state and the public can be challenging if the traditional processes work very well.

UC I.3: Proof of Identity

Identification and authentication is daily business for many companies that operate under regulation and are required to implement KYC (know your customer) and AML (anti-money laundering) processes. This regulation applies to most banks and exchanges, because money is involved

[5] Assuming German law.

[6] Note, that different countries are testing Blockchain for land registry, e.g. Sweden (Rizzo 2016).

and the danger of money laundering or tax fraud is present. In these cases, companies have to identify the user according to the regulations that apply. This process is usually complicated and time-consuming, as the company has to make sure that individuals are who they claim to be. Verifications over the Internet often involves the usage of video-chat. A picture of an ID is not sufficient, as it could be easily stolen or faked. Offline verifications are time-consuming and not available in every city. Additionally, depending on the business, the process has to be repeated every time for regular customers. However, additional steps are time-consuming and costly. Missing standardization in authentication services (e.g., in identity documents) leads to a high effort in the industry.

Blockchain technology can support identification processes, as the blockchain has identity management built into its core. Every transaction created in the system is signed by an entity with a private key which is only known to the signing identity. All other entities can verify a transaction using the public key. Therefore, the combination of public and private key can be seen as an identity which can express its will within the network. In the core protocol, there is no linkage between a real-world identity of a user and a key-pair, users stay pseudonymous.[7] With blockchain, it is possible to link the real-world identity to a key-pair in a decentralized manner. The basic idea of many proposals and projects (Fromknecht et al. 2014; Vogelsteller 2017; Civic Technologies 2018)[8] are identical in their approach. There are three entities in the system:

- The users (who want to authenticate themselves)
- Identity partners (which attest identity of the users)
- Identity requesters.

By authenticating themselves against the identity partners, over time users gain credibility from many different partners such that identity requesters can verify the claims the user is making. This does not only

[7] The first blockchain, namely Bitcoin, only supports pseudonymous identities, as all actions of one key-pair are visible in the system. The user acts under a pseudonym. If a key gets somehow linked to a real-world identity, all actions are traceable.

[8] A list of projects and companies working on blockchain and identity can be found here: https://github.com/peacekeeper/blockchain-identity

create a standard and increases speed, but also return control over their data to users, as they only have to reveal parts of their identity to the identity requesters, such as the age for online gambling.

However, a standard has to be created first. At the moment, many platform providers are not big enough to be considered a general provider, lacking identity requesters who accept them. Many identity requesters also are very slow in adopting new methods of KYC and AML, as these processes are manifold. Nonetheless, we will see increased usage of blockchain identity providers due to the benefits for users and companies shortly.

Research Challenges

Considering all three use cases, it becomes obvious that there are many advantages, but also limitations in the usage of blockchain technology for intermediaries and notaries. These limitations have to be carefully addressed to enable a broader usage of this technology in the future. The advantages and disadvantages of blockchain technology are summarized in Table 11.1 and future research areas can be derived from it.

Based on the differentiation as introduced in the section "Methodological Framework for the Analysis of Blockchain Scenarios", we structure the main research challenges as follows:

Ecosystem and technology: In the ecosystem surrounding DLT and blockchain, the importance of software engineering increases. A key problem is the immutability of smart contracts. To guarantee that the software on top of blockchain runs as intended, software developers have to be very careful with deploying smart contracts, as bugs cannot be fixed later on. Additionally, storing smart contracts in the blockchain and the execution of smart contracts is very expensive. Therefore, software engineers have to consider how to divide up the information and business logic between blockchain and traditional server infrastructure.

Interaction: An oracle is an entity which inputs data from the real world into the blockchain. It behaves in some sense similar to an intermediary, since, in case there is only one oracle, the user has to trust that the

Table 11.1 Pros and cons of blockchain usage for intermediaries and notary services

	Pros	Cons
UC I.1	Payment between peers without trusted third party Law transactional costs High availability Lightweight approach	No trapdoor for "lost" money Currency fluctuation Trust in community and network
UC I.2	Cost reduction Simple and effective for digital assets Decentralized management of assets Direct exchange of money and goods Increased transparency	Public faith required Challenges for realizationand implementation Legislative requirementsand legal framework
UC I.3	Cost reduction High process automation Self-sovereign identity management Privacy-enhancing techniques	Reservations from users Legislative requirementsand legal framework Lack of standards

oracle inputs the correct data.[9] That said, if a good is placed or represented on the blockchain by a token, an oracle has to describe its properties (e.g., diamonds[10]) precisely. If these oracles are flawed, so is the data on the blockchain. Therefore, the linkage between the real good or information and the blockchain has to be improved. At the moment, there are different approaches to create better oracles. However, none of them provides a sufficient level of security.

End user: From the perspective of an end user, there are many open questions regarding regulation of blockchain technology. If the community wants to reach the general public with blockchain technology, these questions have to be answered—for example, how different tokens are classified in a legal sense, say, how are they treated if they represent company shares or are backed by some good. Also, from a regulatory standpoint, standards have to be created at an international level. There are already working groups standardizing blockchain and DLT, namely the ISO/TC 307 (ISO 2016).

[9] This could be anything from weather data to stock market prices.

[10] https://www.everledger.io/

Conclusion

In the end, blockchain is a technology with high potential to replace intermediaries or at least optimize their processes. Intermediaries are going to shift their business models to a more service-oriented approach, offering both sides of the transaction, enhanced and more transparent processes with additional consultation. As legislation continues to regulate blockchain and set standards, increased usage of the technology is to be expected.

Challenges and Opportunities for Lawyers, Judges, and Trials

General Introduction

Blockchain technology is expected to impact and revolutionize a large part of the legal practice dealing within litigation and transactions of the legal domain. This part includes the daily work of legal knowledge workers such as lawyers, judges, and courts. In expensive, complex, and long-lasting trials and disputes, functionalities of the blockchain could contribute significant improvements to efficiency and effectivity (Koulu 2016). However, the improvements might only be made in the most complex tasks of litigation and transactional processes but also in trivial, straightforward tasks that can easily be automated (Zheng et al. 2016). In both, the expensive, complicated tasks and the straightforward procedures, replacing or at least partially automating them using modern technology is an attractive prospect.

Legal procedures have been established as central mechanisms within modern and fair societies to ensure the enforcement of the law, avoid abuse and separate the legislative and jurisdictional power within democracies. Luhmann summarizes the necessity for these procedures based on the basic principle of legitimation by procedure (Luhmann 1983). These processes are required to ensure that the decision regarding justice does not depend on one individual and personal opinion but on a standardized and commonly accepted procedure in which individuals fulfill predefined tasks assigned to them via roles.

This separation of responsibilities and the *ex ante* definition make legal procedures well suited to be, at least partially, automated and executed via predefined routines, such as smart contracts. This section discusses the capabilities of automation with regard to three different use cases:

1. Transparency of evidence and provenance of data
2. Enforcement of the law and contracts
3. Settlement of disputes

Up to now, the digitalization of these scenarios lacks proper infrastructure services that adequately ensure trust among participants not trusting each other unconditionally (for various reasons). From a game theoretical perspective, most of the parties do have a rational argument to not act truthfully but self-interested (Jolls et al. 1998), because unilateral deviation can be beneficial (moral concerns neglected). Control instances are required to regularly check facts and procedures with regard to their correctness, immutability, and consistency. The ubiquitous penetration of technology in combination with decentralized data structures, which guarantee the correctness, immutability, and consistency of records, lower the technological barrier that has always existed and prevented innovation in the legal industry.

UC II.1: Quality Assurance of Evidence and Facts

Currently, the assessment of evidence, facts, and data quality is crucial for different legal procedures, such as litigation and transaction. As more and more analogous tasks, such as the quality assurance or provenance investigations of evidence, can be performed by technology at low, or even zero, cost, the tasks that need to be performed by humans drastically change. The digital ledger nature of blockchain technology ensures the immutability of records and also the reconstruction of the origin and flow of information. In a fully digitalized environment, such as Bitcoin, the origin of each coin in each wallet can be fully and easily be reconstructed. As there is no chance to generate new coins by any mechanism that was not intended in the conceptualization and creation of the environment from the beginning, the Bitcoin as payment system is fully transparent. The intrinsic property of transparency makes the blockchain technology ideal for tasks that are related to the provenance of data and the reconstruction of data flows within a complex organization, such as a society. Serious crimes, such as money laundry, bribery, robbery, tax evasion, or other forms of financial corruption, causing damages that easily reach billions of Euros to national and international economies could be prevented to a large degree. Public blockchain data is easily accessible and can be used by courts during trials in order to avoid costly expert reports that take a lot of time. Digital evidence is already widely used and accepted within trials but assuring the quality and reliability is done by certified authorities, such as IT-Forensics department of the Federal Criminal Police Office in Germany (BKA).[11] With immutable blockchain technology at hand, the information could be retrieved more easily and with far fewer costs.

The same mechanism can be applied to any other digital asset and is not limited to the domain of cryptocurrencies. For example, the tracing of mobility information, such as positional information of smartphones or radar and speed information in traffic, and the safe and immutable storage could be used to detect the presence or absence of someone who is accused of a crime. This could also be extended by recording not only the value data of sensors but also their configuration and certificates to ensure their proper functioning and calibration. Additionally, this mobility information must not necessarily be used to trace and monitor human beings, which would cause severe issues for data protection, but could be used to trace the life cycle of physical goods or (digital) items. A main challenge for the logging of the provenance of physical items is the transition from the real, and offline world to the digital world of the blockchain. Although there are mechanisms which increase the likelihood of reliability[12] the touchpoint of the offline and online world remains a vul-

[11] https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/ITForensik/itforensik node.html, last access on 26/03/2018.

[12] For example: PUFs—Physical Unclonable Functions.

nerable spot and can be considered to be an intrusion point for security breaches. Blockchain technology can only guarantee the consistency of the data stored within, but cannot validate whether data is inserted correctly or not.

UC II.2: Enforcement of Contracts and Computational Law

The usage of blockchain technology in combination with smart contracts to enforce legal and contractual obligations has a high potential to change the legal profession significantly. Once the formalization of legal obligations is done, which is a non-trivial task (Bench-Capon et al. 2012), the executable representation can be stored in an immutable form, which can be publicly accessed. Due to the fact that that these rules cannot be manipulated unilaterally makes it attractive to be used in laws and contracts alike. Consequently, it affects the relationship between private persons, such as civil law and contracts, and also the relationships and duties between governments and private persons, such as public law. Trivially, not every domain of the law is equally well suited to be formalized into an executable representation. Surden (2012) discusses different prerequisites that need to be fulfilled by contracts and laws in order to be processed and executed by computers. A main requirement thereby is the absence of vagueness and the existence of clear and unambiguous conditions. Consequently, different domains of the law differ in the applicability for formalization. Domains such as tax law, or service level agreements (SLAs), where numbers and values are central items of regulations and the semantics of terms is well-defined, are more suitable than very abstract legal domains, such as constitutions, or penalty law, or contracts (including international treaties).

The blockchain is an attractive medium to immutably store executable representations and keep track of changes. Ideally, smart contracts represent the will of two (or more) contracting parties by being designed and implemented such that the business requirements are properly fulfilled. Once the parties agreed on the requirements and on an implemented smart contract, it is stored and signed on the blockchain, where it cannot be changed and manipulated unilaterally. This would be an analogy to the provision of eSignatures for which software services are already established, for example, DocuSign.[13] The creation of such a contract demands additional capabilities than the creation of traditional contracts. The implementation requires the presence of software engineering skills, which cannot be expected to be provided by lawyers (Sillaber and Waltl 2017). However, once the smart contract is stored in the blockchain, it can easily be retrieved and executed at very low cost. Consequently, the enforcement of the contract is available at a very low price. In addition, the execution of consequences is performed automatically. In the analogous world, this would require an execution party, such as the police or government. Using blockchain technology the enforcement is much cheaper and faster. These scenarios could include the (temporary) disabling of user accounts, suspension of insurance coverage, freezing of bank accounts, or enabling of security measures such as locks. Again, the enforcement is constrained to measures and devices that can be accessed digitally. If changes within the offline world need to be taken, an offline enforcement party, such as police or debt collection agencies, need to be involved.

Besides the enforcement of contracts, which is in many contracts the very last measure, smart contracts allow for the easy detection of noncompliant behavior. For companies and enterprises, this is already a very valuable information which cannot be determined by lawyers as efficiently and cheaply as it could be done by algorithms executing a smart contract. Companies want to know to which degree an SLA is fulfilled and whether a service is provided as agreed within the binding smart contract. If the execution engine is constantly provided with monitoring data, the execution of the smart contract would allow to determine the compliance infringement and take adequate responses.

This enforcement and automated detection of non-compliant behavior changes the role and responsibilities of lawyers. The creation of these contracts requires additional skills and capabilities to specify the requirements of smart contracts, which are most likely implemented by computer scientists and software engineers.

[13] https://www.docusign.de/, last access on 26/03/2018.

UC II.3: Alternative Dispute Resolution

The resolution of disputes between parties is an integral part of modern legal systems. Disputes must not necessarily be resolved in lawsuits by official courts, that is, litigation, but can also be resolved outside courts, that is, arbitration. The latter is a specific form of alternative dispute resolution (ADR) and includes mediation and other types of agreements between parties and their advocates. It is highly relevant in the legal industry, especially in the field of economy and commerce. The main idea behind ADR is the definition of predefined rules that structure the procedure of resolving a conflict before the conflict actually occurs. It is important to agree on a set of rules that defines the procedure that is going to be followed by the conflicting parties. In terms of the blockchain ecosystem this can be considered as some form of smart contract that formalizes a workflow that is binding for every involved party and which cannot be changed by one party only. The formalization of these rules in the analogous world is done by prestigious institutions, which serve as trusted third parties. For example, the UNCITRAL Arbitration Rules,[14] or the International Chamber of Commerce[15] that holds the International Court of Arbitration[16] since 1923. Especially in the international arbitration related to economic affairs, ADR plays a very prominent role. The WTO also offers a dispute resolution court.[17] Also, the GATT 1947[18] contains principles for the management of disputes. What makes ADR so attractive is foremost that it addresses current problems of litigation, such as the high cost, and long duration of the process, the execution of judgments and the overall procedural complexity.

In many cases, disputes are due to *broken promises* and their resolution *requires abiding of agreed procedures*. The WTO, as many other tools and

[14] http://www.uncitral.org/uncitral/en/uncitral texts/arbitration/2010Arbitration rules.html, last access on 26/03/2018.

[15] https://iccwbo.org/about-us/who-we-are/dispute-resolution/, last access on 26/03/2018.

[16] https://iccwbo.org/dispute-resolution-services/arbitration/icc-international-courtarbitration/, last access on 26/03/2018.

[17] WTO https://www.wto.org/english/thewto_e/whatis_e/tif_e/disp1_e.htm, last access on 26/03/2018.

[18] General Agreement on Tariffs and Trades from 1947.

mechanisms for ADR, proposes a structured process with clearly defined stages during its procedure to ensure four main principles equitable, speed, effectiveness, and mutually acceptability. At least in two of these main principles, a trusted and reliable blockchain technology could provide support and add even more value at very low costs: speed and effectiveness.

Manual labor is still required to track the current process and ensure the observance of the predefined rules. Having a set of predefined rules of arbitration formalized, such as smart contract, creates trust among the conflicting parties and allows proceeding without additional input from a trusted third party, which is expensive and time-consuming. Using blockchain technology for dispute resolution has already attracted start-ups that provide technological solutions.[19,20] The benefits of the blockchain are again the avoidance of a trusted third party in executing a predefined procedure. The procedure is transparent to every party and can only be changed if both parties agree, which usually only happens before a dispute. This also allows parties to react to changes in laws or economic settings, such as a financial crisis or bankruptcy. Blockchain gives companies the tools to make (legally binding) agreements without the overhead of a trusted third party, and simultaneously provides them with enough certainty on the agreements and the structured settlement of disputes. The role of lawyers whose business model relies on time-intensive, long-lasting, and expensive court trials is competing with a set of predefined rules stored in the blockchain and that ensures a structured and fair process to settle a dispute.

Research Challenges

With respect to the three use cases as described above the usage of blockchain technology as a digital ledger comes along with limitations that need to be addressed proactively in order to enhance a wider adoption in industry. Table 11.2 summarizes the main pros and cons along the mentioned use cases.

[19] https://confideal.io/, last access on 26/03/2018.

[20] https://jury.online/, last access on 26/03/2018.

Table 11.2 Pros and cons of blockchain usage for the legal profession

	Pros	Cons
UC II.1	Immutable records Distributed access Failure tolerance Transparent data Low transactional costs	Restricted to digital assets Transparent data (privacy issue) Digitization of analogous data reward and incentive for nodes and miners
UC II.2	Low cost of execution No unilateral changes in data Transparency of decision-making process Easy to test and distributed	Assurance of validity and correctness Handling of vague terms Formalization as software implementation Handling of exceptions and errors
UC II.3	Clear rules for ADR Transparent ADR process No unilateral changes in process Low transactional costs	Handling of vague terms Structured input data required Verification of input data Handling of exceptions and errors

Based on the methodology introduced in the section "Methodological Framework for the Analysis of Blockchain Scenarios", we structure the main research challenges along this separation:

Ecosystem: A key challenge to technologically support the legal domain as an ecosystem is the diversity among different areas of the law. For example, criminal law and tax law have—at least in civil law jurisdiction—different methods for execution of rules and the apportionment of the burden of proof. From these different methods, different requirements for blockchain solutions will be derived. It is not likely that there is a one-size-fits-all blockchain solution. However, data which is contained in one blockchain might be used in the blockchains of other domains, thus interoperability becomes a central aspect (see further in this chapter). In addition, growing blockchains face the problem of efficiency and performance in terms of energy usage and transaction rates. If the system should become central for modern societies, these problems need to be solved to an acceptable level, which might differ according to domains and use cases.

Interaction: Based on the considerations for the ecosystem and technology, the main considerations for the interaction with blockchain systems can be divided into the blockchain-to-blockchain interaction and the blockchain-environment interaction. The interaction between blockchains requires interoperability between them. This does not only apply to the stored data assets but also to the formalized smart contracts. It demands compatible interfaces to properly test input and output and to safely exchange data among the different implementations. Besides these technical challenges, the interoperability between (inter-)national initiatives needs be considered. Contracts are mainly local and bilateral agreements, whereas laws are (inter-)national and interfere with the contractual agreements. Having a technological solution that allows the handling of these different levels of agreements and potentially conflicting executions is a very challenging task that is far more difficult than providing a feasible technological implementation.

End user: In order to involve end users, either as individuals or in organizations, challenges with regard to the benefits arise. End users could consider the blockchain as a data structure easily outperformed by modern databases. This requires the application of use cases in which the benefits are much higher than the actual costs, for example, dispute resolution platforms or benefits from decreasing transaction/execution costs. In order to maintain the desired properties, the involvement of miners is necessary, and the incentive for the miners needs to be clarified in advance. Outside of cryptocurrency use cases, in which money is generated, the incentive has to be attractive enough for miners to contribute their resources. Additionally, the question of what happens if one of the end users, such as an organization, does not join the blockchain ecosystem needs to be answered. How should these cases be handled? An expensive solution would be to maintain the complete legal infrastructure for the analogous parties. The involvement of end users is again a field that is much more complex than the creation of smart solutions and therefore requires an in-depth analysis and further research.

Conclusion

With regard to the potential of blockchain technology, the impact on the legal industry, especially for lawyers, judges, and trials, can be enormous. But based on the considerations above, it can be concluded that using blockchain technology does not eliminate the work of lawyers. Blockchain has the potential to change the legal profession as it operates today, and this is a great chance toward a more efficient and reliable legal system, in which lawyers and legal tasks, litigation, arbitration, dispute resolution, or others are adequately supported by technology.

The use cases discussed above will still need the justification of evidence and facts that is not a digital asset, such as human witnesses. The digitalization, the shift from analogous to digital data, is still a potential security breach for blockchain environments. Mediation and dispute settlement is and will remain a complex process that is more than just the formalization and automated execution of dispute resolving rules. These tasks will still need a high degree of human input and labor, although—or especially because—blockchain technology is used. However, legal professionals need to proactively adapt and ask themselves which services they can offer and provide to customers. This has, however, always been an intrinsic property of the legal profession and is not specifically tied to blockchain technology.

Challenges and Opportunities for Companies and Financial Markets

General Introduction

It has frequently been claimed that blockchain technology impacts how companies work, collect funding, and coordinate among themselves (Hampton 2016; Tapscott and Tapscott 2016). In current discussions, opportunities for change have been identified across the entire life cycle of companies; from their funding to managing daily operations.

Raising money in capital markets to ensure long-term success has been at the heart of the companies of any economy. While traditionally this has been driven by highly centralized market makers, today there are many opportunities to introduce blockchain technologies to remove or replace existing intermediaries (Zhao et al. 2016). A tokenization of businesses ("shares") has already happened and the buying and selling of shares has been long ongoing. The idea that tokens, managed and exchanged through blockchains, could represent a share of a company, entitling its owner to a share of the profits or giving the owner with voting rights, does not seem too outlandish. This section discusses the capabilities of automation with regard to two different use cases: raising money through ICOs and decentralized corporate governance.

UC III.1: ICOs—Initial Coin Offerings

Much of the hype behind cryptocurrencies is fueled by financial applications built on top of these currencies that stand to potentially change crowdfunding and investment markets (Adhami et al. 2018; Fenu et al. 2018). The so-called ICOs (initial token sales, token emitting events) have raised the equivalent of more than $3 billion, with individual projects collecting more than $200 million. In these offerings, entities sell cryptoassets on a blockchain in exchange for fiat currency or other cryptoassets. Most notably, the ERC20 Token implementation (Vogelsteller and Vitalik 2016) allows for the creation of tradable tokens on the Ethereum blockchain. Stakeholders willing to participate in the trade receive tokens that can be understood as cryptographically-secured coupons (Hacker and Thomale 2017) that embody a bundle of rights and obligations. Depending on the specific details of the implementation of the token and the structuring of rights and obligations, such tokens can be subject to a broad variety of rules and regulations (e.g., security regulation).

The fungibility and tradability of the tokens, combined with the potential for trading of the tokens in secondary markets, make ICOs an attractive alternative to classical crowdfunding. So, too, does the relatively low cost of an ICO as compared to IPOs, which can cost up to several hundred thousands of dollars (Ritter and Welch 2002).

This perceived ease of raising money has already attracted many malicious actors in a field where the regulators have been mostly observant.

However, as several exit and bump-and-dump schemes can be observed and have led to fraud and an increased negative perception of the crypto economy, increased regulatory enforcement can be expected.

UC III.2: The DAO and DAOs—Decentralized Autonomous Organization(s)

National and international corporate law defines the rights, relations, structuring and conduct of corporations, their stakeholders as well as the exchanges between them and other entities (Venegas 2017). These laws are the foundation on which the governance structure of a corporate entity and all additional shareholder agreements, bylaws, and other private contracts are built. Corporate rules, however, can be broken (on purpose or in negligence) or misinterpreted and their execution is rarely transparent.

This “black box” nature of corporations has been frequently abused in a variety of ways, such as for tax evasion purposes orponzi schemes (Bartoletti et al. 2017; Vasek and Moore 2018). Furthermore, a corporation leadership might be wrongfully accused of, for example, mismanagement by shareholders if the leadership’s interpretation of rules deviates from the stakeholders’ interpretation.

The ability of some blockchains to execute arbitrary programs, sometimes referred to as smart contracts, could be used to automate large parts of corporate governance structures. This would allow participants to control the organization in real-time and would require all rules to be formalized and automatically enforced. The most prominent and earliest DAO, “The DAO” (Decentralized Autonomous Organisation), was the world’s first decentralized investment fund (Jentzsch 2016; Wright and De Filippi 2015). Despite showing a high level of decentralization, in the end it set back the development of decentralization and the “code is law” principle for the recovery of stolen assets via blockchain modification.

Research Challenges

Capital market actors need to be increasingly aware of Bitcoin and other blockchain powered cryptocurrencies as their relevance for financial transactions increases.

Table 11.3 summarizes main advantages and disadvantages related to the use cases mentioned above.

A key challenge for a broader adoption of blockchain technology lies in the difficulty of aligning the scope and interests of local laws with the global blockchain system that was developed without regard for juridical boundaries. This is outlined in various discussions on the legal nature of cryptoassets (Hacker and Thomale 2017). In addition, a broad adoption of the technology in capital markets might also raise scalability, security, and interoperability issues (Karame 2016).

Furthermore, as the value of cryptoassets increases, so does the importance of keeping them save. As the technology matures, security incidents are bound to happen and many (preventable) vulnerabilities threaten broader adoption (Atzei et al. 2017).

Based on the differentiation as introduced in the section "Methodological Framework for the Analysis of Blockchain Scenarios", we structure the main research challenges along this separation:

Ecosystem: A key challenge to technologically supporting the funding and governance of businesses through blockchain-based technologies is the question of regulatory compliance. Most jurisdictions have a long history of building laws around highly centralized entities within clear jurisdictional boundaries. For example, the EU GDPR assumes centralized data processors, an assumption bound to break once decentralized, blockchain-based ecosystems emerge (e.g., Pesch and Sillaber 2017). The same decentralized nature of blockchains also (re-)enables fraud and raises regulatory issues related to AML.

Table 11.3 Pros and cons of blockchain usage for capital markets

	Pros	Cons
UC III.1	Low cost of execution Transparency of decision-making process Enhanced fairness	High impact for security incidents Formalization of business rules difficult Potential of lack of governmental oversight Potentially unwanted transparency
UC III.2	Low cost platform Transparent data	Erosion of privacy Potential for fraud and abuse

Interaction: Besides obvious issues of blockchain-to-blockchain and blockchain-to-the-real-world (e.g., fiat settlement), the use and application of blockchains raise interesting challenges for the legal system. For example, bugs and vulnerabilities in smart contracts raise yet to be answered questions of liability.

End user: As exemplified by the amounts of money raised by various ICOs, end users have already begun to embrace new forms of project financing and are willing to participate in blockchain-based services. However, due to the fast-paced nature and overall system risks attached to the ecosystem, it remains to be seen how consumer and investor protection can be enforced.

Conclusion

Although the market capitalization of cryptocurrencies is still small compared to traditional asset classes (Hacker and Thomale 2017), the technology can bring fundamental change to capital markets and the way businesses raise, use, and distribute value. The often cited de-intermediarization of capital markets has yet to be seen. Decentralized technology seems to be the layer on which new intermediaries build their business models.

Summary

This chapter discusses eight use cases and scenarios of blockchain technology and their impact on the legal industry. At first, the large field of the legal industry is subdivided into three representative pillars, namely, (I) "intermediaries and notaries", (II) "lawyers, judges and trials", and (III) "companies and financial markets". From a methodological point of view, the article differentiates into three levels of impact, of which each of the three pillars of the legal industry is going to be analyzed. These three levels of impacts, or value creation, are (i) ecosystem, (ii) interaction, and (iii) end users.

For each pillar of the legal industry, different use cases are identified and discussed. Thereby, these use cases range from very technical topics relevant for the infrastructure, such as the transfer of money (UC I.1), including other digital assets, and proof-of-identity (UC I.3) to advanced topics at the intersection of the legal domain and the financial market, such as ICOs (UC III.1).

The first contribution of this article can be considered as a methodological framework for the analysis of use cases and disruption scenarios of blockchain technology, including smart contracts, for a particular domain. The differentiation of different layers on which value proposition can be expected is suitable for a comprehensive perspective on the complex field. The second contribution is the identification and illustrative discussion of different use cases throughout the legal industry. We identified potential starting points for disruptions by blockchain technology; however, there are still open research challenges that need to be addressed and solved in prior to a broad and potentially non-threatening adoption.

References

Adhami, S., Giancarlo G., & Martinazzi S. (2018). Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings. *Journal of Economics and Business.*

Atzei, N., Massimo B., & Tiziana C. (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). In *International Conference on Principles of Security and Trust* (pp. 164–186). Springer.

Bailey, J. P., & Yannis, B. (1997). An Exploratory Study of the Emerging Role of Electronic Intermediaries. *International Journal of Electronic Commerce, 1*(3), 7–20.

Bartoletti, M., Salvatore C., Tiziana C., & Roberto, S. (2017). Dissecting Ponzi Schemes on Ethereum: Identification, Analysis, and Impact. *arXiv preprint arXiv:1703.03779.*

Bench-Capon, T., Araszkiewicz, M., Ashley, L., Atkinson, K., Bex, F., Borges, F., Bourcier, D., Bourgine, P., Conrad, J., Francesconi, E., et al. (2012). A History of AI and Law in 50 Papers: 25 Years of the International Conference on AI and Law. *Artificial Intelligence and Law, 20*(3), 215–319.

Brenig, C., Schwarz, J., & Rückeshäuser, N. (2016). Value of Decentralized Consensus Systems—Evaluation Framework. In: *24th European Conference on Information Systems (ECIS)*, 12–15 June, Istanbul, Turkey.

Brown, R. (2016). *On Distributed Databases and Distributed Ledgers*. https://www.corda.net/2016/11/distributed-databases-distributed-ledgers/

Civic Technologies, Inc. (2018). *Civic Secure Identity Ecosystem*. https://www.civic.com/

Fenu, G., Marchesi, L., Marchesi, M., & Tonelli, R. (2018). The ICO Phenomenon and Its Relationships with Ethereum Smart Contract Environment. *ArXiv e-prints* (March). arXiv: 1803.01394 [cs.CY].

Fromknecht, C., Velicanu, D., & Yakoubov, S. (2014). *Certcoin: A Namecoin Based Decentralized Authentication System*. Technical Report. Massachusetts Institute of Technology. 6.857 Class Project.

Hacker, P., & Thomale, C. (2017). *Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law*. European Company and Financial Law Review Forthcoming. Available at SSRN: https://ssrn.com/abstract=3075820 or https://doi.org/10.2139/ssrn.3075820

Hampton, N. (2016, September). Understanding the Blockchain Hype: Why Much of It Is Nothing More Than Snake Oil and Spin. *Computerworld, 05*. https://www.computerworld.com.au/article/606253/understanding-blockchain-hype-why-much-it-nothing-more-than-snake-oil-spin/

International Organization for Standardization (ISO). (2016). *ISO/TC 307—Blockchain and Distributed Ledger Technologies*. https://www.iso.org/committee/6266604.html

Jentzsch, C. (2016, November). *Decentralized Autonomous Organization to Automate Governance*. White Paper.

Jolls, C., Sunstein, C., & Thaler, R. (1998). A Behavioral Approach to Law and Economics. *Stanford Law Review, 50*, 1471–1550.

Karame, G. (2016). On the Security and Scalability of Bitcoin's Blockchain. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM. https://doi.org/10.1145/2976749.2976756.

Koulu, R. (2016). Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement. *SCRIPTed, 13*, 40.

Lemieux, V. L. (2017). A Typology of Blockchain Recordkeeping Solutions and Some Reflections on Their Implications for the Future of Archival Preservation. In *Proceedings of the 2017 IEEE International Conference on Big Data*, Boston, MA.

Luhmann, N. 2001. *Legitimation durch Verfahren* (6th ed.). Frankfurt am Main: Suhrkamp. ISBN 3-518-28043-0.

Pesch, P., & Sillaber, C. (2017). Distributed Ledger, Joint Control? Blockchains and the GDPR's Transparency Requirements. *Computer Law Review International, 18*(6), 166–172.

Ritter, R., & Welch, I. (2002). A Review of IPO Activity, Pricing, and Allocations. *The Journal of Finance, 57*(4), 1795–1828.

Rizzo, P. (2016). *Sweden Tests Blockchain Smart Contracts for Land Registry*. https://www.coindesk.com/sweden-blockchain-smart-contracts-land-registry/

Sillaber, C., & Waltl, B. (2017). Life Cycle of Smart Contracts in Blockchain Ecosystems. *Datenschutz und Datensicherheit DuD, 41*(8), 497–500.

Surden, H. (2012). Computable Contracts. *UCDL Review, 46*, 629.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. Sebastopol: O'Reilly Media, Inc.

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York: Penguin.

Vasek, M., & Moore, T. (2018). Analyzing the Bitcoin Ponzi Scheme Ecosystem. In *Fifth Workshop on Bitcoin and Blockchain Research, Financial Cryptography and Data Security 18 (FC). Springer*.

Venegas, P. (2017, August 1). *Initial Coin Offering (ICO) Risk, Value and Cost in Blockchain Trustless Crypto Markets*. Available at SSRN: https://ssrn.com/abstract=3012238 or https://doi.org/10.2139/ssrn.3012238.

Vogelsteller, F. (2017). *ERC-725 Identity*. Technical Report.

Vogelsteller, F, & Vitalik B. (2016). *ERC-20 Token Standard*. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md

Wright, A., & De Filippi, P. (2015). *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. Rochester: Social Science Research Network.

Zhao, L., Shaokun, F., & Jiaqi, Y. (2016). *Overview of Business Innovations and Research Opportunities in Blockchain and Introduction to the Special Issue*. Heidelberg: Springer.

Zheng, Z., Shaoan, X., Hong-Ning, D., & Huaimin, W. (2016). *Blockchain Challenges and Opportunities: A Survey* (Working Paper).

12

A Critical Examination of the Application of Blockchain Technology to Intellectual Property Management

Kensuke Ito and Marcus O'Dair

Introduction

Below, we set out the major challenges related to managing intellectual property in the digital era, before going on to examine ways in which supporters have suggested that blockchain and distributed ledger technologies could contribute to solving these challenges. Key technical terms are also explained.

Intellectual Property Management in the Digital Era

'Intellectual property' (IP) refers to the protection of the application of ideas and information of commercial value (Cornish et al. 2013, p. 6).

K. Ito
The University of Tokyo, Tokyo, Japan
e-mail: k-ito@g.ecc.u-tokyo.ac.jp

M. O'Dair (✉)
Middlesex University, London, UK
e-mail: M.ODair@mdx.ac.uk

H. Treiblmaier, R. Beck (eds.), *Business Transformation through Blockchain*,
https://doi.org/10.1007/978-3-319-99058-3_12

Cornish et al. (2013, p. 7) identify three central types of IP: 'patents for inventions, copyright for literary and artistic works and associated products, and trademarks and names for the goodwill attaching to marketing symbols'. This chapter focuses in particular on copyright : 'a right given against the copying of defined types of cultural, informational and entertainment productions' produced by authors, playwrights, composers, artists and film directors (Cornish et al. 2013, p. 8). Copyright is conferred automatically to literary and artistic works but only when written down or recorded: critically, 'it is the particular expression making up a work which is protected, rather than the idea behind it' (Cornish et al. 2013, 9).

While digital technology is far from the first challenge to copyright, it may prove the most significant, since 'digitisation has made unauthorised access and distribution of copyrighted work easy and ordinary' (Klein et al. 2015, p. 3). Indeed, some scholars have suggested that IP, as currently understood, may not survive the current era (Cornish et al. 2013, p. 11). As Cornish et al. (2013) assert, IP is essentially negative: although there may be positive entitlements, IP rights are primarily an attempt to prevent particular activities, such as piracy. In practical terms, however, lawsuits and threats have achieved limited results (Klein et al. 2015, p. 31), since peer-to-peer file-sharing sites, for instance, have proved difficult to shut down. Digital technology has stretched copyright 'to breaking point', resulting in 'a gulf between copyright law and everyday practices' (Klein et al. 2015, p. 1). There are problems with royalty payments, which are slow, inefficient and opaque, and it is difficult to assess whether labels, publishers or collection societies are processing payments efficiently (O'Dair et al. 2016).

The Possible Role of Blockchain Technology

Some have suggested that a solution could lie in distributed ledger technologies (DLTs), such as blockchain technology. A 'distributed ledger' can be understood as a type of distributed database; its aim is to overcome the presence of malicious users or nodes (Hileman and Rauchs 2017, p. 11). A blockchain is a particular type of distributed ledger: one that is 'composed of a chain of cryptographically linked "blocks" contained in batched transactions' (Hileman and Rauchs 2017, p. 11).

For reasons of space, we do not include a detailed discussion of the technical aspects of DLT in this chapter; such information is readily available elsewhere (Nakamoto 2008; Buterin 2014; Antonopoulos 2015; Swan 2015; Narayanan et al. 2016). The pertinent point for this chapter is that Bitcoin, proposed in 2008 and implemented the following year, was radical in its removal of third parties (in that instance, banks). Crucially, this disintermediation was achieved not only through technology but also through a deep understanding of game theory and incentives. However, Bitcoin can be understood as simply the first innovation in this space. Gupta (2017, p. 2) identifies subsequent innovations, of which the first is 'the realisation that the underlying technology that operated bitcoin [the cryptocurrency] could be separated from the currency and used for all kinds of other interorganisational cooperation'. With this innovation came the understanding that blockchain technology, which, if not quite immutable, is certainly extremely robust since it has no single point of failure, could be utilised for more than Bitcoin transactions. With 'metacoins' came the notion that Bitcoins could be augmented, its functionality extended; with 'altcoins' came entirely new cryptocurrencies, and new blockchains. The subsequent innovation identified by Gupta, closely linked to one of these new blockchains, is the 'smart contract', 'embodied in a second-generation blockchain system called Ethereum, which built little computer programs directly into blockchain that allowed financial instruments, like loans or bonds, to be represented', rather than only Bitcoins (Gupta 2017, p. 2). A 'smart contract', then, is a self-executing computer programme that automatically performs a given function (Hileman and Rauchs 2017, p. 11). Smart contracts have enabled the emergence of DApps, or decentralised applications with backend code running on decentralised, peer-to-peer networks.

While it is the global prominence, and fluctuating value, of Bitcoin that hits media headlines, Morabito (2017, p. vii) suggests we should understand blockchain as more than a financial technology or 'fintech' phenomenon; it is being deployed in a range of domains and across a number of industries. Blockchain technology, in other words, can be used to as a register of intellectual property. In essence, this works through the use of 'hashes'. A 'hash' is a unique string of alphanumeric characters that represents a given content file; it can be understood as a kind of 'digital fingerprint' (Antonopoulos 2015, p. xx). Crucially, it is short enough to be included in a blockchain transaction; 'via the hash, the original file content has essentially been encoded into the blockchain' (Swan 2015, p. 39).

Proponents identify three advantages of blockchain technology for creating a distributed IP database (O'Dair and Beaven 2017). Firstly, they claim that it guarantees *authenticity*: metadata can be inextricably bound to the relevant data file, be it a song or a film. Secondly, proponents state that blockchain technology allows for *provenance*: usage and ownership can be recorded. Thirdly, champions of the blockchain state that it can facilitate the faster and more efficient payment of royalties, in some cases by removing trusted intermediaries and facilitating a direct-to-fan model. These advantages may seem compelling, and they are propounded by a number of start-ups, funded either by traditional venture capitalists or by means of token sales, also known as initial coin offerings or ICOs. A token sale can be akin to a Kickstarter-style crowdfunding campaign, which allows the general public to participate in an early-stage project; the important difference, however, is that most tokens are tradeable (Chen 2017). Token sales offer the possibility of raising significant sums of money at speed: millions of dollars can be raised in seconds, even by companies yet to produce a product (Sahdev 2017). At the same time, it is important to recognise that token sales vary wildly, with only a minority of tokens offering fractional ownership in the value of the underlying organisation (Conley 2017, p. 1).

Having examined both the challenges of contemporary intellectual property management and the claims made for blockchain and DLT as a solution to these challenges, we now go on to critically examine limitations of the technology—first from an operational perspective, sub-divided into authenticity, provenance and royalty stability, and then from the perspective of implementation, sub-divided into files, metadata and licensing.

Review from an Operational Perspective

This section covers potential problems of using blockchain technology for IP management from an operational perspective. Specifically, we here examine each use case in order, from simple to complex, and classify their limitations in terms of authenticity, provenance and royalty stability. Having identified a number of challenges, we then go on to suggest possible solutions which we could consider under a current environment.

Authenticity Problem

In almost all blockchain-based intellectual property management systems, we first have to convert some IP information into a hash and record it in a distributed ledger. This is a relatively simple task but it is valuable in providing assurance that a protected work existed at a certain point in time (Proof of Existence) because blockchains are robust—even 'immutable'.[1] By adding information on rights holders, it would be possible to go a step beyond proof of existence—to what we might call proof of ownership.[2] A number of related services have already been proposed, such as a digital certificate that makes use of blockchain 'timestamping' (e.g. Binded) and a common protocol for IP metadata (e.g. Coala IP, SPOOL on Ascribe). However, a fundamental problem in this first step is that, for information that is not native to the blockchain we cannot guarantee its authenticity at the moment of registration: this is sometimes referred to as the 'garbage in, garbage out' problem. If copyright ownership information is entered incorrectly, either deliberately (by a bad actor) or mistakenly (due to human error), it is unclear how conflicts would be resolved without a trusted third party (TTP). Although it can store information in a robust and immutable manner, blockchain technology alone cannot confirm the authenticity of the registered information.

Unless and until we can address this authenticity problem, practical operations will be restricted to a public but permissioned network that can contain only information authorised by a TTP. This corresponds to the example of the academic journal where the process of reviewing

[1] More precisely, blockchain is pseudo-immutable because the accumulation of sequential blocks just makes tampering difficult (not impossible) through computational complexity, and we can roll back the stored record when blockchain is managed by a TTP.

[2] This extension has a novelty in that we can prove existence or ownership without disclosing the data on the contents by adopting a hash function.

submitted papers is recorded on a blockchain, rather than a centralised pre-print server (e.g. Ledger). In this case, even though the data can be preserved in a secure environment, only the authorised editors are responsible for its input. If a solution requires governance by a TTP, it is not based on the innovation achieved by Bitcoin, and it also contradicts our goal of facilitating IP management by disintermediation.

Provenance Problem

If, for the sake of argument, we assume the authenticity problem is somehow solved, the next challenge concerns recording transfers of ownership. There is an expectation that blockchain can facilitate the transfer of IP without requiring a TTP, and that it can overcome the problem of 'piracy' through issuing a digital certificate or a secret key to access digital contents (e.g., Ascribe, CopyrightBank). Here, however, we face another problem related to provenance: blockchain cannot prevent 'double-spending' and unauthorised replication outside the network (O'Dwyer 2017, p. 306). Physical assets such as paintings, for example, can easily be transferred between owners without updating the information stored in a ledger; moreover, even digital assets are replicable for a temporal owner who has the private key. Needless to say, once IP is transferred outside the network, records in the ledger no longer provide a reliable certificate of ownership.

Until this provenance problem is solved, practical operations will be restricted to issuing transferable ownership certificates, where the rights to exclude unauthorised use depends not on blockchain but on the power of TTPs such as government representatives or collection societies. This corresponds to the example of the digital certificate (e.g. Ascribe) that embeds terms of service compliant with local laws in order to be used as evidence in court to resolve ownership disputes. As with authenticity, this solution would not contribute to the disintermediation and efficient IP management because it is costly to settle ownership disputes after the fact, by relying on a TTP, rather than preventing such problems beforehand by incentive design.

Royalty Stability Problem

If we assume both the authenticity and the provenance problems are solved, then disintermediated IP management would finally become feasible. As stated above, a number of intermediaries currently exist to monitor the secondary use of intellectual property, as manifest in both physical and digital works, and their high management costs diminish royalty payments to creators. In order to improve such a situation, a variety of online platforms are being developed that aim to directly connect artist and consumer by using blockchain to store royalty payment records in addition to contents transaction. This is evident especially in the music industry, where monitoring costs are high (e.g. Ujo Music, Peertracks, Bittunes).[3] However, one final challenge remains: we cannot use stable payment methods for decentralised royalty management. Although cryptocurrencies provided a new payment method that does not rely on a TTP, their price has thus far not been sufficiently stable as to use as a store of value. Instead, many cryptocurrencies are volatile in the extreme. It would be more practical for intellectual property management to use DApps,[4] for instance on Ethereum; specifically the DApp could circulate internal reward tokens associated with ownership transfer and thereby manage the transactions of both IP ownership and royalty payments on the same network. However, this would make the royalties paid to artists even more unstable, because there is fluctuation in the value of reward tokens within the DApp, as well as at the Ethereum network level.

As long as we cannot solve this royalty stability problem, practical operations will be restricted to a service whose royalty payment confronts the trade-off between efficiency and stability; we must accept significant price fluctuations in return for efficient payment with no intermediaries, or, conversely, must rely on costly intermediaries and legal currencies in return for stable royalty payments. Therefore, even if we could solve the

[3] At the time of writing, the authors are not aware of platforms that have decentralised all three service layers identified in the implementation section below.

[4] Decentralised applications: an app with the backend code running on a decentralised peer-to-peer network, rather than a centralised server.

problems of authenticity and provenance, the system needs to set an optimal boundary on to what extent royalty management should be decentralised in order to maximise royalty payments to creators.[5]

Tentative Solutions

We have thus far investigated several use cases concerning IP management by blockchain technology, and have discussed three cumulative obstacles: authenticity, provenance and royalty stability. The consistent challenge is that IP is not native to the blockchain, and can have an independent value even outside the network.[6] In the case of cryptocurrencies represented by Bitcoin, we can trace the precise history of transaction and issuance because the numbers recorded in the ledger serve as the only evidence of asset value. In the case of intellectual property, by contrast, we face a number of challenges in keeping IP data consistent with the actual asset, because the value of the asset exists separately from the ledger. In other words, DLT can make the data robust and immutable, but only once it is correctly registered —and it cannot accurately validate the condition of external entities. IP management may, then, need a new technology or incentive design which addresses assets with independent value, rather than simply applying to IP management a system developed for cryptocurrencies. How, then, can we overcome these challenges? Below, we consider some tentative solutions for each challenge in turn.

In regard to the *authenticity* problem, similar discussions have already been made in Oracle, a system that acquires information outside the blockchain network as a condition for executing smart contracts. If we consider the example of a prediction market, one of the most common applications of Oracle, users need to reach consensus on the outcome of predicted events (about weather, the stock market, sports matches and so on) in order to trigger payments. Thus, this shares the same challenge as

[5] Note also that the realisation of decentralised payments needs additional fees as an incentive to the validators, such as transaction fees on Bitcoin and GAS on Ethereum. Thus, more precisely, we need to consider this cost as well as the price fluctuation risk in order for artists' royalty maximisation.

[6] We therefore can apply the three problems to other assets that have similar characteristics, such as real estate, jewellery and even supply chain management.

intellectual property management: how to prove the input data are truly correct. While most of the implemented oracles adopt a centralised solution relying on a TTP (typically information providers), some propose a decentralised solution to the problem. For example, Peterson et al. (2018) describes a unique Oracle for Augur that delegates the outcome determination to some internal users named ‘reporters’. Reporters in this system are incentivised to act honestly by the mechanism that each reporter stakes tokens against an option they believe as most likely and then all staked tokens are redistributed to those reporters who chose the option consistent with consensus.[7] In addition, Brey (2017) deals with an attempt to design a decentralised reputation network formed through token-based incentives and to trade the reputation data in its own Oracle for Tru. These approaches, namely token staking and reputation systems, will also be useful in addressing the authenticity problem for IP management, by helping to achieve decentralised consensus.

The *provenance* problem could in part be solved by the fact that we have an incentive to maintain the chain of provenance to avoid decreasing the value of a given asset (De Filippi et al. 2016, p. 5). Furthermore, the provenance problem could be addressed through tokenisation, a method that divides the value (or associated rights) of a work into tokens whose management can be internalised in the ledger. Unfortunately, effective tokenisation is currently limited to goods with a source of value that is traceable on the ledger or transferrable by tokens; the former corresponds to an example of online ticket (e.g. Aventus), while the latter corresponds to tokens issued in a creator’s name (e.g. Tokit on SingularDTV). In other words, even if an asset is tokenised under the status quo, this will not overcome the provenance problem without the existence of TTP, because IP can still be copied or double-assigned behind the token holders’ back. Nevertheless, tokenisation has a great potential to solve this problem, in two broad ways. In the first scenario, which we might call the internal method, the tokens denote IP rights; this method represents an attempt to make IP rights traceable, and could be successful as long as we can prove the connection of value between tokens and cre-

[7] See Peterson et al. (2018) for more details of the consensus-building. Although it is not explicitly mentioned in the original paper, Augur’s Oracle is often called ‘distributed fact stream’.

ative works.[8] The second scenario is the external use of tokens, in which tokens are a form of compensation, or reward, for creators of IP. This is an approach to mitigate the provenance problem by incentivising creators even when works are not protected by exclusive copyright; anyone can freely access and copy them. Externalisation therefore has a synergy with digital content which we can duplicate with almost no additional costs. For example, Everpedia, a kind of decentralised Wikipedia, already issues tokens to users who contribute by editing articles, and Steemit adopts a similar reward system towards blog posts and their evaluation.

Regarding the *royalty stability* problem, a straightforward but effective solution would be to adopt 'pegged cryptocurrencies', whose value is backed by stable assets. Tether, Nubit and BitUSD, for example, are examples of cryptocurrencies pegged to US dollars, and there is also a project to issue the tokens pegged with gold such as DigixDAO. These attempts can bring both value stabilisation and efficiency to payment methods. In particular, the Dai Stablecoin System by MakerDAO is noteworthy in that it aims to stabilise token prices in a decentralised manner. The system uses two main protocols in order to achieve stabilisation without a TTP holding vast amounts of US dollars in reserve: users have to deposit an appropriate amount of ether as collateral before issuing a token, and the amount is calculated based on the price of US dollars acquired from the outside by the distributed Oracle. Since this token allows an integrated application to maintain the characteristics as DApps, the Dai Stablecoin System will be effective on the stable and disintermediated IP royalty management.

Review from an Implementation Perspective

In this section, we investigate the methods and challenges of blockchain-based applications for IP from an implementation perspective. This is important because a system for efficient IP management generally requires

[8] Note that some projects try to tokenise the external (non-native to the blockchain) assets by assuming a TTP responsible for custody of the assets (e.g. Latoken). Although this is partially contrary to the elimination of intermediaries, it will make a certain contribution to the provenance problem and the liquidity on the registered assets.

the implementation of multiple service layers, each with a different method for decentralisation. For simplicity, we here divide the layers into three: files, metadata and licensing. We examine these three layers in turn, in each case analysing examples of existing services.

Files Layer

When implementing a system aiming for disintermediation of IP management, the most fundamental layer we can consider decentralising would be file storage: the layer that contains original digital content such as music, movies and images. Before the emergence of blockchain technology, decentralisation of this layer can be understood as essentially an extension of the use of peer-to-peer file sharing systems for the high-speed transfer of large volume data. Resilio Sync (formerly BitTorrent Sync), for example, provided a system to synchronise files in local storage among multiple devices based on BitTorrent—one of the most popular peer-to-peer file transfer protocols. More recently, Benet (2014) extended this idea to a browser-based file system named IPFS (InterPlanetary File System) and proposed a web page that works even without a server. However, these systems themselves lack Bitcoin's unique incentive design—only more recently have they started to integrate token-based rewarding to promote the autonomous working of the distributed storage network. Nodes in these new systems all lend and borrow their storage space via tokens and store the hash values of segmented data as Merkle tree format along with the original data, but the methods are slightly different to prove without a TTP that the data are correctly stored.[9] For example, Storj is designed to reward storage providers if they can return a hash value consistent with the regular requests by clients, and the Merkle tree of hashes is preserved in the Ethereum blockchain (Wilkinson et al. 2016).[10] In Sia, while storage providers similarly obtains reward tokens when they successfully return a valid hash list of a part of the

[9] Additionally, the approaches for redundancy (a design to handle the situation that a part of nodes is offline) are also slightly different. See each whitepaper for detail.

[10] Storj changed its underlying blockchain from Bitcoin to Ethereum in 2017.

stored data in predetermined frequency, the Merkle tree is preserved in its original proof-of-work blockchain (Vorick and Champine 2014). Furthermore, Filecoin, proposed for usage with IPFS, links storage proof and the influence over its original blockchain: a node can generate the next block with a higher probability if it is proved to store the client's data for a specified time (Protocol Labs 2017).

With these systems, creators will be able to store original IP data in an environment that is neither entirely self-contained nor dependent upon a TTP. On the other hand, we can point out two main problems with regard to decentralising the files layer. Firstly, the decentralisation of the files layer does not make a very significant contribution to the goal of efficient IP management through disintermediation. Most of the argument on inefficiency has been made against a number of intermediaries for the management of IP rights and royalties, not for the storage of original files. Considering that we also need additional costs (tokens) in order for the file storage to function autonomously, it would be more reasonable in many cases to use existing services relying on TTP such as cloud storage, rather than attempt to decentralise this layer.[11] Secondly, as far as the authors know, all peer-to-peer storage systems with Bitcoin-inspired incentive design (e.g. IPFS with Filecoin) are currently under development, so that there are no practical applications for IP management based on them. Although implementation plans have often been announced in the music industry, for instance, we are not aware at the time of writing this chapter of any projects that have successfully achieved decentralisation of the files layer.[12] The risks and benefits of using such new file storage systems, therefore, remain uncertain.

Metadata Layer

Many applications use the database management system (DBMS) for efficient data control. Unlike storage and file systems, such a database generally stores the structured metadata which correspond to the original data,

[11] It should also be noted that while the decentralisation of storage layer will reduce the risk of data loss, it does not solve the problems of authenticity and provenance.

[12] For example, Ujo Music is now using Amazon S3 while developers mentioned future implementation of decentralised (and autonomous) storage systems.

and DBMS frees us from the programming task for stipulating data location and access authority. This convenient middleware is adopted for IP management as well—for example, the metadata of registration rights such as trademarks and patents are all published on the database by management authorities (e.g. EUIPO, EPO). Decentralisation of this layer has already been popular as distributed databases which were implemented for the main purpose of resolving the large-scale data management problems by making distributed processing easier and more efficient (Özsu and Valduriez 2011, p. 3). Blockchain technology is, as Hileman and Rauchs (2017, p. 11) stated, often referred to as DLT while being treated as a kind of distributed database. This is to emphasise several different aspects of blockchain, such that it is decentralised for robustness, rather than efficiency, and is proposed originally as a component of the peer-to-peer system that did not assume central management (Nakamoto 2008; Pinna and Ruttenberg 2016). It would be a natural approach to apply such blockchain-specific characteristics to existing distributed database management system (DDBMS). For example, BigchainDB aims to balance scalability and decentralised management through a hybrid method that the system uses DDBMS for both data storage and transaction recording,[13] while the communication between them requires the voting by the group of assigned nodes.[14] BigchainDB has especially a potential to have an influence on the future of IP management since it is being developed by many of the same individuals who developed Ascribe, a company dealing with digital certificates for IP ownership.[15]

The point we would like to emphasise here is that existing distributed databases can achieve much of what can be achieved by blockchains. For example, as with other append-only databases, CouchDB can make data uneditable once inputted, while Apache Cassandra eliminates single points of failure from its network by peer-to-peer data management based on consistent hashing.[16] Considering that we can ensure something

[13] The latter has a similar structure to blockchain.

[14] See McConaghy et al. (2016) for detail. Note that this whitepaper is no longer a living document according to the project members, and they are now writing a new updated version which is unavailable at the time the authors are writing this chapter in March, 2018.

[15] McConaghy and Holtzman (2015), the whitepaper of Ascribe, already mentioned the outline of BigchainDB.

[16] See Lakshman and Malik (2010) for detail.

approaching immutability and a reasonable degree of robustness even in existing mechanisms, the new achievement by blockchain (in combination with proper incentive design) would be limited to the decentralised and autonomous management of the data recorded on the ledger by people with different interests. However, this has not yet been completely realised in a general-purpose DBMS. Even in BigchainDB, clients need to trust the nodes and the consortium as long as its consensus depends on the voting system. Other barriers to creating a decentralised autonomous management still remain too, such as the aforementioned authenticity problem and the Sybil attack problem, a risk typically faced by online voting. Therefore, we need to be cautious in claiming blockchain technology can transform the metadata layer—not only in the case of IP management.

Licensing Layer

A significant proportion of the blockchain-based IP management applications we introduced in the previous section intend to record the transfer of the rights and values accompanying the registered contents. Such a layer for storing the history of status transition of the target files or metadata is referred here to as the licensing layer. A number of applications are being developed in this layer, because licensing is one of the most explicit extensions to the core concept of Bitcoin—a peer-to-peer transfer of the data stored in the ledger. In case of performing a simple proof of existence and certificate transfer, it would be sufficient to store the hash value corresponding to creative work in the Bitcoin blockchain (e.g. Ascribe, poex.io).[17] However, in order to execute wider and more flexible functions, including licensing and payment, we need to use blockchain as a platform which is able to develop DApps. In Ethereum, for instance, we can realise behaviours much more diverse and complicated than those required for a coin transaction by the following two sequential methods: creating a transaction to define and deploy a 'contract account' equivalent to an object in the context of programming, and sending another type of

[17] See Roselfeld (2012) for further detail of this approach called 'colored coin'.

transaction containing the variables necessary for contract execution to the defined account (Buterin 2014, pp. 13–17). It should be emphasised that Ethereum blockchain is not designed to hold the files or metadata; it recorded only the state transition of both user and contract accounts.[18] Accordingly, at least under the existing circumstances, a single blockchain cannot manage IP consistently from original file storage to licence transfer.

The fact that a number of projects are being developed on the licensing layer suggests a confidence that implementation challenges can be overcome; certainly, the challenges are mild compared with those presented by the files and metadata layers. The real challenge in decentralising royalty management is to integrate licensing with these files and metadata layers—yet existing DApps focus on the licensing layer alone. In IP management, Ujo Music is an example of a platform attempting to address this issue: the company plans to decentralise multiple layers, including the licensing layer. In addition, needless to say, the problems from the operational perspective that we have discussed in the previous chapter still remain. Provenance and royalty stability are especially critical issues that should be dealt with through the design of the licensing layer, since we cannot solve them even if original files or metadata guarantee authenticity. Despite these challenges, licensing is the layer where application development is so active as to have a high possibility of making useful DApps for IP management ahead of other layers.

Conclusion

The excitement surrounding the potential of blockchain technology for managing IP is understandable. Yet existing blockchain design, which is optimised for cryptocurrencies, should not and cannot be simply applied to the management of IP, since assets are not native to the blockchain. Significant operational challenges remain. In respect of authenticity, we must address the 'garbage in, garbage out' problem. In respect of provenance, we must consider our inability to prevent off-chain transfers. In

[18] User is defined as 'externally owned account' in the context of Ethereum.

respect of royalty stability, finally, we must face the challenge of cryptocurrency volatility. Tentatively, we have suggested ways in which the various operational challenges might be overcome—for instance through the use of token-based incentives, and through pegging cryptocurrencies to fiat currencies. There are also, however, challenges from an implementation perspective—at the file, metadata and licensing layers. We are, as yet, not aware of use cases for the decentralisation of the file layer, so talk of using blockchains for managing actual files remains somewhat abstract. In regard to metadata, the case for the use of blockchains as opposed to other forms of distributed database has yet to be made. In regard to licensing, finally, we are not as yet aware of a single blockchain that can manage IP consistently from original file storage to license transfer.

It is also important to note that, even if we overcome the barriers to adoption identified in this chapter, not to mention additional concerns relating from the technical (scalability) to the legal and regulatory, the use of blockchains for IP management is not without risk: 'smart contracts' could replicate the worst aspects of digital rights management (De Filippi et al. 2016, p. 3), while the censorship-resistance of distributed systems could make it very difficult to remove illegal content (O'Dair 2017, p. 22). Finally, not all commentators agree that the use of distributed ledgers for the management of IP necessarily results in a decentralisation of power in the interests of creators: for Zeilinger (2016), decentralised technologies will, on the contrary, simply reinforce models of centralised finance. Further examination of such risks is beyond the scope of this chapter, but the need for further research is clear.

The conclusion of our own research is that blockchain is a highly innovative technology that could transform the management of IP. A narrow focus on the technology itself, however, can result in a tech-utopian 'solutionism' that ignores significant challenges from both operational and implementation perspectives. The effective use of blockchain technology for IP management will be dependent upon the proper design of incentives, at both operational and implementation layers. The incentive structure, after all, is precisely what was so innovative about Nakamoto's original proposal back in 2008. We should not forget that history.

References

Antonopoulos, A. (2015). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Beijing: O'Reilly.

Benet, J. (2014). *IPFS – Content Addressed, Versioned, P2P File System (DRAFT 3)*. Available at: https://arxiv.org/pdf/1407.3561.pdf. Accessed 24 Mar 2018.

Brey, I. (2017). *Tru Reptation Protocol—Establishing Persistent Reputation via the Ethereum Blockchain*. Available at: https://tru.ltd/Tru_Reputation_Protocol_White_Paper.pdf. Accessed 25 Feb 2018.

Buterin, V. (2014). *A Next-Generation Smart Contract and Decentralised Application Platform*. Available at: https://whitepaperdatabase.com/ethereum-eth-whitepaper/. Accessed 25 Mar 2018.

Chen, Y. (2017). *Blockchain Tokens and the Potential Democratisation of Entrepreneurship and Innovation*. Stevens Institute of Technology School of Business Research Paper. Available at: https://ssrn.com/abstract=3059150. Accessed 24 Mar 2018.

Conley, J. (2017). *Blockchain and the Economics of Crypto-Tokens and Initial Coin Offerings*. Vanderbilt University Department of Economics Working Paper Series. Available at: http://www.accessecon.com/Pubs/VUECON/VUECON-17-00008.pdf. Accessed 24 Mar 2018.

Cornish, W., Llewelyn, D., & Aplin, T. (2013). *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* (8th ed.). London: Sweet and Maxwell.

De Filippi, P., McMullen, G., McConaghy, T., Choi, C., de la Rouviere, S., Benet, J., & Stern, D. J. (2016). How Blockchains Can Support, Complement, or Supplement Intellectual Property: Working Draft, Version 1.0. *COALA IP*. Available at: https://github.com/COALAIP/specs/blob/master/presentations/COALA%20IP%20Report%20-%20May%202016.pdf. Accessed 24 Mar 2018.

Gupta, V. (2017). A Brief History of Blockchain. *Harvard Business Review*. Available at: https://hbr.org/2017/02/a-brief-history-of-blockchain. Accessed 24 Mar 2018.

Hileman, G., & Rauchs, M. (2017). *Global Blockchain Benchmarking Study*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224. Accessed 24 Mar 2018.

Klein, B., Moss, G., & Lee, E. (2015). *Understanding Copyright: Intellectual Property in the Digital Age*. London: Sage.

Lakshman, A., & Malik, P. (2010). Cassandra—A Decentralised Structured Storage System. *ACM SIGOPS Operating Systems Review, 44*(2), 35–40.

McConaghy, T., & Holtzman, D. (2015). *Towards and Ownership Layer for the Internet*. Available at: https://d1qjsxua1o9x03.cloudfront.net/live/trent@ascribe.io/ascribe%20whitepaper%2020150624/digitalwork/ascribe%20whitepaper%2020150624.pdf. Accessed 24 Mar 2018.

McConaghy, T., Marques, R., Müller, A., De Jonghe, D., McConaghy, T. T., McMullen, G., Henderson, R., Bellemare, S., & Granzotto, A. (2016). *BigchainDB: A Scalable Blockchain Database*. Available at: https://github.com/bigchaindb/whitepaper. Accessed 20 Mar 2018.

Morabito, V. (2017). *Business Innovation Through Blockchain: The B3 Perspective*. Cham: Springer.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at: https://bitcoin.org/bitcoin.pdf. Accessed 24 Mar 2018.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton/Oxford: Princeton University Press.

O'Dair, M. (2017). *How Blockchain Is Transforming the Creative Industries: Copyright and Rights Management in the Second Era of the Internet*. Toronto: Blockchain Research Institute.

O'Dair, M., & Beaven, Z. (2017). The Networked Record Industry: How Blockchain Technology Could Transform the Record Industry. *Strategic Change, 26*(5), 471–480.

O'Dair, M., Beaven, Z., Neilson, D., Osborne, R., & Pacifico, P. (2016). *Music on the Blockchain*. Available at: https://www.mdx.ac.uk/__data/assets/pdf_file/0026/230696/Music-On-The-Blockchain.pdf. Accessed 24 Mar 2018.

O'Dwyer, R. (2017). Does Digital Culture Want to be Free? How Blockchains are Transforming the Economy of Cultural Goods. In R. Catlow, M. Garrett, N. Jones, & S. Skinner (Eds.), *Artists Re:Thinking the Blockchain*. Liverpool: Liverpool University Press.

Özsu, M. T., & Valduriez, P. (2011). *Principles of Distributed Database Systems* (3rd ed.). New York: Springer.

Peterson, J., Krug, J., Zoltu, M., Williams, A. K., Alexander, S. (2018). *Augur: A Decentralised Oracle and Prediction Market Platform*. Available at: http://www.augur.net/whitepaper.pdf. Accessed 8 Jan 2018.

Pinna, A., & Ruttenberg, W. (2016). *Distributed Ledger Technologies in Securities Post-Trading—Revolution or Evolution?* European Central Bank Occasional Paper Series, No. 172. Available at: https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf?13905018ccb56b34472f00d25c1be0d8. Accessed 20 Mar 2018.

Protocol Labs. (2017). *Filecoin: A Decentralised Storage Network*. Available at: https://filecoin.io/filecoin.pdf. Accessed 16 Mar 2018.

Roselfeld, M. (2012). *Overview of Colored Coins*. Available at: https://bitcoil.co.il/BitcoinX.pdf. Accessed 24 Mar 2018.

Sahdev, N. (2017). *The Tokenization of the Economy: ICOs and the Implications for Cryptoeconomics*. Available at: https://ssrn.com/abstract=3057083. Accessed 24 Mar 2018.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. Beijing: O'Reilly.

Vorick, D., & Champine, L. (2014). *Sia: Simple Decentralised Storage*. Available at: https://sia.tech/sia.pdf. Accessed 16 Mar 2018.

Wilkinson, S., Boshevski, T., Brandoff, J., Prestwich, J., Hall, G., Gerbes, P., Hutchins, P., & Pollard, C. (2016). *Storj A Peer-to-Peer Cloud Storage Network*. Available at: https://storj.io/storj.pdf. Accessed 16 Mar 2018.

Zeilinger, M. (2016). Digital Art as 'Monetised Graphics': Enforcing Intellectual Property on the Blockchain. *Philosophy & Technology, 31*(1), 15–41.

Part V

Appendix

13

Blockchain: Basics

Aljosha Judmayer, Nicholas Stifter, Philipp Schindler, and Edgar Weippl

Over the last decade, the principle of *blockchains* has risen from relative obscurity in what was at the time a comparatively small community of Bitcoin users to worldwide prominence. The recent success of Bitcoin has led to extensive news coverage in mainstream media and widespread interest from the general public. Reports, videos and myths surrounding Bitcoin show how difficult the fundamentals are to understand for non-expert users, not to mention the fact that there is still very little awareness or understanding of systems other than cryptocurrencies that rely on the principle of blockchains. We hope this chapter will help demystify the concept and provide a sound introduction to the underlying

A. Judmayer • P. Schindler
SBA Research, Wien, Austria

N. Stifter
TU Wien, CDL-SQI, Wien, Austria

E. Weippl (✉)
TU Wien, FH St. Pölten, Wien, Austria
e-mail: EWeippl@sba-research.org

H. Treiblmaier, R. Beck (eds.), *Business Transformation through Blockchain*,
https://doi.org/10.1007/978-3-319-99058-3_13

technologies and consensus mechanisms of the blockchain. Although the term blockchain is closely linked to Bitcoin (to the point where many laypeople consider them quasi-synonymous), the term was not introduced by Satoshi Nakamoto in the original paper that presented Bitcoin (Nakamoto 2008) as a prototype for a decentralized cryptocurrency.[1] The term emerged in the Bitcoin community to describe the principle of the new cryptocurrency, and is therefore not standardized terminology. Therefore, there are two common spelling variants: blockchain and block chain. Although the latter was used by Satoshi Nakamoto in a comment in the original source code,[2] the former is more frequently used in academic literature, for example, in publications such as Croman et al. (2016) and press reports, and can be regarded as a de facto standard. Therefore, we will use the spelling *blockchain*.

Although the wider public generally associates the term blockchain with cryptocurrencies (especially Bitcoin), and it is true that most cryptocurrencies use mechanisms and principles derived from the originalBitcoin protocol, distributed consensus approaches like the blockchain or other proof-of-work (PoW) algorithms have a much wider area of application.

The fundamental objective in the creation of Bitcoin was that it should function as a decentralized virtual currency that is not dependent on trusted third parties. This was achieved by combining an innovative distributed consensus approach with incentive engineering and suitable cryptographic primitives—an approach whose feasibility has been demonstrated by the success of Bitcoin and other cryptographic currencies. However, the principle has applications far beyond cryptocurrencies, in such diverse domains as the energy sector or the music industry. The underlying technology, generally referred to as blockchain, is being increasingly studied in the scientific community, along with increased research into other security problems of distributed systems, such as secure timestamping, distributed name spaces, and so on. As Bonneau

[1] The Bitcoin whitepaper was self-published by Nakamoto in 2008, and soon followed by the creation of the genesis block of theBitcoin protocol on January 3, 2009.

[2] https://github.com/trottier/original-bitcoin/blob/master/src/main.h##L795-L803

et al. (2015) see it, "Bitcoin is a rare case where practice seems to be ahead of theory. We consider that a tremendous opportunity for the research community to tackle the many open questions about Bitcoin …". Despite the growing interest in academia, the private sector, and the general public, there are still many unsolved problems in terms of finding a balance between performance, scalability, security, decentralization, and anonymity in such systems. This chapter will first look at the fundamentals of blockchain technology through the lens of an analogy. The example introduces the main concepts of blockchains and can explain the functioning of Bitcoin and other blockchain systems to people with no technological background. This will be followed by a brief discussion of the cryptographic primitives that are the building blocks of the technology.

The Analog Stone Block Chain

It can be difficult to explain the fundamental principle of Bitcoin and other blockchain applications to novices, especially if they have no technical background. Many explanations for laypeople, which have proliferated with the rise of Bitcoin, falter when it comes to explaining the ideas behind complex concepts and terminology like consensus algorithms and cryptography. We have therefore attempted to create a fully analog example that may be helpful in trying to explain the basic mechanisms of blockchain technologies to people lacking the necessary technological background. Our example of a stone block chain uses simple analogies that are easy to visualize. While it may not be able to explain every detail, it should be able to present the basic ideas behind Bitcoin's complex components in a way that makes it easy to understand without technological knowledge. We hope that this—admittedly not entirely practical—example will help illustrate the fundamentals of blockchains. In the example, the blockchain is used to create a currency, but the general principles apply to other uses of blockchain technology as well.

Our setting is a prehistoric village called *Nakamotopia*. Much of the life and culture of this village revolves around stone: the Nakamotopians' love of stone blocks borders on obsession, and the town is famous for its stonework and is home to numerous skilled stonemasons. Until recently, they used small, intricately carved round rocks as a kind of currency. This came to an end when it was discovered that someone had found a way to carve new rocks much easier and faster than previously. The new rocks flooded the market, the currency lost its value, and the villagers lost their trust in it. In view of the damage this was doing to trade, the village council met to discuss what could be done. The solution was elegant, combining the villagers' love of stone blocks with their enthusiasm for lotteries. They decided to involve the entire community in the creation and management of the new currency system. The block creation ceremony, as they call it, has three steps:

Miner Selection Every morning, all Nakamotopians assemble next to the quarry outside their village. Each of them places a small stone token, engraved with their (unique) name, into a large wooden box. The box is placed on top of a geyser located there, which erupts at regular intervals. When the hot stream of water shoots from the geyser, the wooden box is propelled into the air and scatters its contents on the ground. The villager whose stone lands closest to the geyser is the winner: they become the *miner* of the next block. If the result is not clear, the stones that are closest are placed back into the box and the process is repeated until one miner has been chosen.

Transaction Processing In the second step of the block creation ceremony, the person selected as miner for the day sets out their tools next to an enormous stone block. All the villagers who want to make a transaction queue up to inform them of the transactions so that they can be included in the stone block chain. With each transaction, a certain amount of virtual currency units is transferred from one person to another. The miner carves this information into the stone block, thereby transferring ownership of the currency to the recipient. Of course, this is only possible if the sender actually has at least as many units as they want to transfer (that information is available on the previous stone blocks). There is only one exception to this rule: the very first transaction engraved into the block credits the miner with a certain number of currency units as reward for their work. This is also the only way of creating new currency units. This means that all information about currency units in circulation is recorded on a block. The miner adds all transactions they want to include onto the stone block. They may decide not to include a particular transaction. If that happens, the person who wanted the transaction to be recorded has to wait for the next day when a new miner is chosen and hope they will include it. At the end of the day, the stone block contains all the transactions the miner has included, each with the name of the sender, the name of the recipient, and the number of currency units transferred. Finally, the miner engraves the holy termination symbol 0x00 in the remaining space underneath the last transactions. This way, nobody will be able to sneak to the village square at night to engrave additional transactions onto the block: it would be easy to detect. Because all stone blocks have exactly identical dimensions, it is also not possible for someone to polish off the surface of the stone block and engrave a new set of transactions—everyone would notice the block had been tampered with, and they would reject it.

Chaining Once the stone block has been completed and terminated with the holy termination symbol, it is taken to the village square. Due to its enormous weight and size, moving it even a short distance requires the combined effort of a large number of villagers. The villagers have a vested interest in the stone block being correct, and make sure it is. Should the miner have incorporated invalid transactions or in any other way violated the rules of the elders, no honest villager would help them move the block, and the miner would not receive their mining reward, because they only get it if their block becomes part of the chain as proof of their work. If the villagers decide the transactions on the stone block are correct, they move it into the town center and lift it on top of the towering stack of blocks already located there. Only once it is placed onto this stack is it considered valid, and the transactions take effect. The stacking process ensures that transactions are in chronological order, but it also makes it much harder to tamper with blocks that are further down the chain. If someone wanted to modify a block further in the past, for example, to engrave a transaction on it that would credit them with a large amount of currency units, they could not do it on their own. They would need the help of a large number of Nakamotopians to start removing the blocks from the top with significant effort. This would take a long time and would not remain unnoticed by honest villagers for long. However, if a sufficient number of villagers realize that there has been a mistake or an attempt at fraud, and they conclude that a block should not be part of the chain, they can get together to remove that block and replace it. In this way, the majority consensus decides what is a valid part of the stone block chain.

Security Features of the Stone Block Chain

This subsection examines the security guarantee of the stone block chain in our analogy and how they relate to the security features of cryptographic currency and other blockchain technologies.

Public Transaction Ledger All transactions that take place in Nakamotopia can be viewed at any time in the chain of blocks in the village square. This public transaction ledger, or public record of transactions, also exists in actual blockchain systems. The main difference is that the Nakamotopians use their real identities in their transactions, while-Bitcoin uses pseudonyms.

Proof-of-Work A Proof-of-Work (PoW) is a way of proving that you have invested (computational) resources into a task. The requirements for a PoW are that it should be difficult to generate but easy to verify.

In Nakamotopia, stone blocks are difficult to generate: you have to create the blank blocks to exact measurements, inscribe transactions into them, and then transport them to the village square and place them on top of the stack. The stone blocks are easy to verify: once they have been placed onto the stone block chain in the village square, anyone can verify them by reading the transactions inscribed on them, and measure them to make sure they have the right dimensions.

In Bitcoin, PoW also functions as a mechanism that randomly selects a new creator for the next block. In Nakamotopia, this function is fulfilled by the geyser.

Immutability The data in the blockchain must be immutable. In Nakamotopia, this is achieved by means of enormous stone blocks with precisely defined dimensions: attempting to polish a correct transaction off a block's surface to replace it with a fraudulent one would easily be noticed—either during the process or when verifying the dimensions of the blocks. If someone were to create a new stone block with the exact right dimensions that includes fraudulent transactions, the effort of removing the previous blocks, replacing an older block with the fraudulent one, and putting the other blocks back would require so much effort it is highly unlikely to go unnoticed by several honest villagers—not to mention the effort of moving the stone blocks would require the help of too many dishonest villagers to be in any way feasible.

In Bitcoin and other blockchain systems, the blocks are chained together by including a cryptographic hash of the previous block in each new block's header. A client can check the previous blocks and verify the final block hash.

Honest Majority For the stone block chain to work, there has to be an honest majority of villagers who agree on each block of the chain. If we assume that is the case, then a majority of the blocks in the chain will have been made by honest villagers, and there is little risk of them being changed by dishonest villagers. If none of the honest villagers are paying attention (e.g., because they are out hunting for mammoths for the community), dishonest villagers could have an opportunity to add fraudulent blocks to the chain or replace blocks. Moving the blocks takes a lot of time and effort, so if previous blocks were to be replaced, they could only be ones near the top, because the process would have to be completed before the others come back from the hunt to avoid discovery. But even if enough dishonest villagers were to get together to add or replace a block, the honest majority would quickly notice that something was wrong when they verified the chain. They could then set about removing the invalid blocks and replacing them. The more stone blocks are stacked on top of a particular block, the longer it would take to remove them. As the dishonest villagers would need days or even weeks, such an attack would be unlikely to succeed. This means that if a stone block is far enough down the chain (i.e., has been in the chain long enough), it can be considered agreed upon: it cannot have been placed there recently by an attacker, and enough honest people have seen it and confirmed its validity by continuing to place blocks on top of it.

If a large number of Bitcoin blocks has been appended to a given block, it is considered to have a high number of confirmations. It is unlikely that changes will be made after a certain point, so the block is then considered agreed upon. While the number of confirmation blocks depends on the value of the transaction in question, six confirmation blocks are generally sufficient to consider a past transaction valid and secure (Eyal and Sirer 2014).

Proof-of-Stake

To address the issue of very high resource demands in PoW-based blockchains as well as other concerns such as scalability, latency, throughput and centralization risks (Gervais et al. 2014), alternatives to PoW are proposed. In this thesis, we focus on one of the most promising ones called *Proof-of-Stake* and refer the reader to, for example, Bentov et al. (2016) for a more general discussion. Proof-of-Stake aims to establish similar security guarantees as PoW, but in comparison uses only a negligible amount of computational resources.

As a key difference, Proof-of-Stake does not rely on solving cryptographic puzzles as part of its consensus algorithm. Instead of consuming electricity as a physical resource, virtual resources in form of digital coins are used. Leaders, which produce new blocks in Proof-of-Stake based systems, are typically selected *at random* based on the amount of coins they stake. Unfortunately, obtaining and agreeing on the involved randomness is a difficult problem by itself, as any introduced entropy is subject to potential manipulation by an adversary (Kiayias et al. 2016).

The idea of Proof-of-Stake was first discussed in Bitcoin forums in 2011,[3] later independently discovered and described with Peercoin (King and Nadal 2012), and is already used in various other cryptocurrencies

[3] https://bitcointalk.org/index.php?topic=27787.0

such as BlackCoin, Nxt and ShadowCash. Moreover, there is ongoing discussion to consider Proof-of-Stake as a replacement for PoW in Ethereum[4] which is the second largest blockchain system with a market capitalization of about 700 Mio. USD (approx. 6% of Bitcoin)[5] in 2016.

In a PoW-based system the creator of the next block to be added to the blockchain is selected in a race finding a solution to a cryptographic puzzle. The more computational power a miner has, the more likely it is to be elected for him. Proof-of-Stake proposes an alternative, where the nodes run a random selection process which is not based on the computational power of the nodes. Instead this process depends on the share of coins a participating node possesses. In this way, the drawback of the high power consumption required by mining in PoW-based systems can be eliminated. As a further consequence, the group of stakeholders and miners collapses into a single group maintaining the blockchain (Kiayias et al. 2016; King and Nadal 2012).

Proof-of-Stake in Peercoin

As an early example, we now introduce Peercoin as the first cryptocurrency implementing Proof-of-Stake. In fact, Peercoin uses a hybrid system of PoW and Proof-of-Stake. The initial distribution of coins is based on PoW similar to Bitcoin. In order to sustain the network and to cover the miner's expenses for electric current, as soon as the mint rate slows down and transaction fees increase, the creation of new blocks is more and more shifted toward the Proof-of-Stake approach (King and Nadal 2012). The concept of a hybrid approach is already considered in an increasing number of research work such as Bentov et al. (2014); Mackenzie (2014); and Duong et al. (2016).

Although Peercoin's approach shares many ideas with Nxt, Peercoin is based on the concept of coin age which is not used in Nxt. Coin age is defined as the amount of coins one possesses times the holding period.

[4] https://www.reddit.com/r/ethereum/search?q=proof+of+stake&restrict_sr=on&sort=relevance&t=all

[5] https://coinmarketcap.com

The holding period is simply the amount of time a set of coins has not been spent. For example, if Bob received 10 coins and does not spend it for a period of 90 days, this can be seen as an accumulation of 900 coin-days of coin age. The calculation of coin age is made possible by introducing a timestamp field for each transaction (King and Nadal 2012).

A Proof-of-Stake block in Peercoin includes a special transaction, called a coinstake transaction. The creator of the block consumes his coin age by this transaction and gets to pay himself a block reward. The privilege of being selected to generate a block depends on a part of the coinstake transaction called the kernel. This kernel has to meet a certain hash target. This is similar to Bitcoin, where block hashes have to be lower than a difficulty target. Coinstake transactions with a higher coin age are proportionately more likely to match the hash target. However, there is an important difference: in Bitcoin the search space for the hash is only bounded by the amount of resources a miner is willing to invest, while in Peercoin the protocol only permits one hash per second per unspent transaction output. As a consequence, the resource usage in Peercoin is insignificant (King and Nadal 2012).

Conflict resolution between two competing blocks is achieved by the rule that the block containing more coin age is to be included in the main chain. A block's coin age is simply calculated by the sum of the coin age of its transactions. Furthermore, a centralized checkpointing mechanism is introduced to protect the blockchain history (King and Nadal 2012).

Proof-of-Stake: Casper

One of the newest ideas for a Proof-of-Stake consensus mechanism is currently researched and developed for the second largest blockchain system Ethereum. The consensus mechanism is named "Casper" as it adopts some principles previously described in the GHOST protocol (Sompolinsky and Zohar 2015). As of April 2018, Casper is not implemented as part of the Etherium protocol yet. Currently, Casper is considered work in progress. Different variants have been proposed by Vitalik Buterin (2017) ("Casper the Friendly Finality Gadget") and Vlad Zamfir (2017) ("Casper the Friendly Ghost: A Correct-by-Construction Blockchain Consensus Protocol").

Today Etherium is running on top of a PoW-based consensus algorithm. Different reasons why a switch to a new system is desirable have been stated[6,7,8]:

- lower costs: In Bitcoin the costs of attacking the system are equal to the expenses to run the system. In Proof-of-Stake, honest participants have low costs compared to attackers.
- improved scalability.
- reduced vulnerability to selfish-mining attacks.
- reduced centralization risks.

However, those arguments and in particular the argument of a higher degree of security for a given amount of money in a Proof-of-Stake based system in comparison to, for example, Bitcoin is subject to different opinions.[9,10]

Challenges for Proof-of-Stake

We now discuss one of the most fundamental issues that need to be addressed by any Proof-of-Stake-based system: a problem called Nothing at Stake. The Nothing at Stake problem can be summarized as the fact that a node might choose to build new blocks on top of every fork he sees. There are two incentives for this approach:

- no additional costs
- additional chances for mining rewards

First, in contrast to PoW, where an attacker actually has to spend computational power on each fork he chooses to mine on, there are no addi-

[6] https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ

[7] http://ethereum.stackexchange.com/questions/9/why-does-ethereum-plan-to-move-to-proof-of-stake

[8] https://blog.ethereum.org/2014/07/05/stake

[9] http://www.truthcoin.info/blog/pow-cheapest

[10] https://www.youtube.com/watch?v=rsLrJp6cLf4

tional costs involved in a Proof-of-Stake-based system. And second, building blocks on all forks increases the opportunity of getting mining rewards independent of the fact which fork becomes the main chain.[11,12,13]

In the original Peercoin paper, the Nothing at Stake problem is not addressed. However, a centralized checkpoint mechanism was already introduced with the first Peercoin version. Centralization in this case is considered acceptable until a distributed solution is available (King and Nadal 2012). More recently, the problem is addressed at the Peercoin Wiki.[14] The event of a successful attack is considered very unlikely. In addition to a similar economic argument, the concept of coin age protects against ongoing attacks due to the fact coin age is consumed by an attacker.[15]

The Casper consensus mechanism is designed to protect against Nothing at Stake attacks. Although the same economic argument might apply, Casper's protection is built into the protocol. Betting on multiple forks of the same height in Casper results in loses, as upon detection of this equivocation the node's staked funds are destroyed (slashed) (Buterin 2017).

Cryptographic Primitives

Although the example of the stone block chain is a good analogy for the fundamentals of blockchain technology, a more concrete understanding of the principles of PoW-based cryptocurrencies requires some discussion of the cryptographic primitives used. The two most important primitives for PoW-based cryptocurrencies are **cryptographic hash functions** and **asymmetric cryptography**. We will look at the basic properties that cryptographic hash functions must have and the constructions that can

[11] http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt

[12] https://wiki.peercointalk.org/index.php?title=Myths\#Nothing-at-stake

[13] https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/

[14] https://wiki.peercointalk.org/index.php?title=Myths\#Nothing-at-stake

[15] https://wiki.peercointalk.org/index.php?title=Myths\#Nothing-at-stake

be built on them, for example, *Merkle trees*, but not go into much detail regarding the security behind them. We also assume that the reader has a general understanding of public key cryptography, as most cryptocurrencies rely on established algorithms and parameters. For further details as well as the mathematical foundations of the topics mentioned here, please refer to Hoffstein et al. (2008); Katz and Lindell (2014); Menezes et al. (1996); Bos et al. (2014); Hankerson et al. (2006); and Cohen et al. (2005).

Hash Function A hash function H takes data x of arbitrary (but finite) size and returns a value h of a fixed size, called hash, hash value, or digest.

Cryptographic Hash Function To be considered a *cryptographic* hash function, a hash function has to have four additional properties (Menezes et al. 1996).

1. **Easy to compute**: It must be easy to compute the hash of any given finite message.

$$h = H(x), Where\, h \text{ is of fixed length} \tag{13.1}$$

2. **Preimage resistance:** It is infeasible to generate an input value that has a given hash value. Infeasible in this context means that it cannot be achieved by an adversary during the time that the message must remain secure. In terms of complexity theory, this equates to not being possible in polynomial time. As a result of this property, cryptographic hash functions are also called one-way functions.

$$\text{Given a hash } h \text{ it is infeasible to find any message } x \text{ such that } h = H(x) \tag{13.2}$$

3. **Second preimage resistance:** It is infeasible to find a second input that produces the same output as a specified first input (referred to as *collision*).

$$\text{Given a message } m \text{ it is infeasible to find another message } m' \\ \text{such that} m \neq m' \text{ and } H(m) = H(m') \tag{13.3}$$

4. **Collision resistance:** It is infeasible to find *any* two different inputs that produce identical hash values.

$$\text{It is infeasible to find any two messages } m, m' \\ \text{where } m \neq m' \text{ and } H(m) = H(m') \tag{13.4}$$

Merkle Tree *Merkle trees*, or *hash trees*, allow the verification and authentication of large sets of data. They are binary trees in which each leaf node is labeled with a value to be authenticated, and each non-leaf node is labeled with the hash value of the labels of its child nodes. The concept was introduced by Merkle in 1987 as a one-time signature scheme based on an *"infinite tree of one-time signatures."* Later, it became known as a *Merkle tree*, *hash tree* or *authentication tree* (Menezes et al. 1996). Figure 13.1 gives an example of a Merkle tree with $n = 4$ values and the resulting *root hash* or Merkle tree root r. To authenticate a value v_1 and prove that it was part of a Merkle tree with a root hash r, the values h_2 and h_6 are needed. For more information on Merkle trees see Becker (2008).

Some properties of such a tree structure are as follows:

- The distance from any leaf to the root of a (balanced) binary tree with n leaves is approximated by $log_2(n)$.

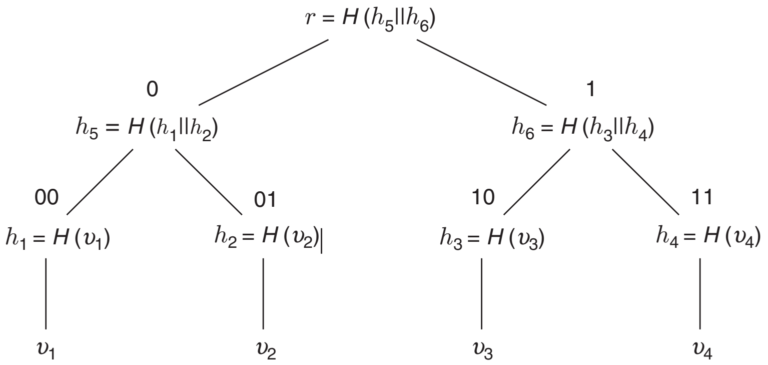


Fig. 13.1 Merkle tree with $n = 4$ values. Nodes are labeled with a binary string referencing their position, for example, node h_2 is labeled 01

- Given a root hash r and a value v, approximately $log_2(n)$ hash computations are required to prove whether v is a leaf of a (balanced) binary tree.

References

Becker, G. (2008). *Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis.* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.392.7879&rep=rep1&type=pdf

Bentov, I., Charles, L., Mizrahi, A., & Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. *ACM SIGMETRICS Performance Evaluation Review, 42*(3), 34–37.

Bentov, I., Pass, R., & Shi, E. (2016). Snow White: Provably Secure Proofs of Stake. *Cryptology ePrint Archive, Report 2016/919.* https://eprint.iacr.org/2016/919.pdf

Bitcoin Forum. (2011). *Proof of Stake Instead of Proof of Work.* https://bitcointalk.org/index.php?topic=27787.0. Accessed 8 Dec 2016.

Bonneau, J., et al. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *2015 IEEE Symposium on Security and Privacy.* https://www.ieee-security.org/TC/P2015/

Bos, J. W., et al. (2014). Elliptic Curve Cryptography in Practice. *International Conference on Financial Cryptography and Data Security 2014.* https://www.

amazom.de/Financial-Cryptography-Data-Security-International/dp/3662454718

Cohen, H., et al. (2005). *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Boca Raton: Chapman & Hall/CRC.

Croman, K., et al. (2016). On Scaling Decentralized Blockchains. *International Conference on Financial Cryptography and Data Security 2016.*

Duong, T., Fan, L., & Zhou, H.-S. (2016). *2-Hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely*. https://eprint.iacr.org/2016/716.pdf

Etherium Forum. *Proof of Stake*. https://www.reddit.com/r/ethereum/search?q=proof+of+stake&restrict_sr=on&sort=relevance&t=all. Accessed 8 Dec 2016.

Eyal, I., & Sirer, E. G. (2014). Majority Is Not Enough: Bitcoin Mining Is Vulnerable. *International Conference on Financial Cryptography and Data Security* 2014.

Gervais, A., et al. (2014). *Is Bitcoin a Decentralized Currency?* http://www.syssec.ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/research/publications/pub2014/spmagazine_gervais.pdf

Hankerson, D., Menezes, A. J., & Vanstone, S. (2006). *Guide to Elliptic Curve Cryptography*. New York: Springer.

Hoffstein, J., Pipher, J., & Silverman, J. H. (2008). *An Introduction to Mathematical Cryptography*. New York: Springer.

Katz, J., & Lindell, Y. (2014). *Introduction to Modern Cryptography*. Boca Raton: CRC Press.

Kiayias, A., Konstantinou, I., Russell, A., David, B., & Oliynykov, R. (2016). A Provably Secure Proof-of-Stake Blockchain Protocol. *Cryptology ePrint Archive,* Report 2016/889. http://eprint.iacr.org/2016/889.pdf

King, S., & Nadal, S. (2012, August 19). Ppcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Self-Published Paper.

Mackenzie, A. (2014). *Memcoin2: A Hybrid Proof of Work/Proof of Stake Cryptocurrency.* http://mc2.xwebnetwork.com/storage/mc2%20draft%20v0.04.pdf

Menezes, A. J., et al. (1996). *Handbook of Applied Cryptography*. Boca Raton: CRC Press.

Merkle, R. C. (1987). A Digital Signature Based on a Conventional Encryption Function. *Conference on the Theory and Application of Cryptographic Techniques* 1987.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

Sompolinsky, Y., & Zohar, A. (2015). Secure High-Rate Transaction Processing in Bitcoin. *Financial Cryptography and Data Security* (pp. 507–527). New York: Springer. http://www.cs.huji.ac.il/ avivz/pubs/15/btc_ghost_full.pdf

Zamfir, V. (2017). *Casper the Friendly Ghost a "Correct-by-Construction" Blockchain Consensus.* https://github.com/ethereum/research/raw/master/papers/CasperTFG/CasperTFG.pdf

Index[1]

[1] Note: Page numbers followed by 'n' refer to notes.

H. Treiblmaier, R. Beck (eds.), *Business Transformation through Blockchain*,
https://doi.org/10.1007/978-3-319-99058-3