Smart Contracts – Blockchains in the Wings

19

Thomas Bocek and Burkhard Stiller

Abstract

In recent years, electronic contracts have gained attention, especially in the context of the blockchain technology. While public blockchains are considered secure, legally binding under certain circumstances, and without any centralized control, they are applicable to a wide range of application domains, such as public registries, registry of deeds, or virtual organizations. As one of the most prominent blockchain examples, the Bitcoin system has reached large public, financial industry-related, and research interest. Another prominent block-chain example, Ethereum, which is considered a general approach for smart contracts, has taken off too. Nevertheless, various different set of functions, applications, and stakeholders are involved in this smart contract arena. These are highlighted and put into interrelated technical, economic, and legal perspectives.

19.1 Introduction

Technology has progressed in the past decades. However, the role of disruptive technology may have become even more prominent with "Blockchains" or "Distributed Ledgers". They pave the path for trustworthy, decentralized applications, and new stakeholder's relations. As such they have the potential to revolutionize public administration, commercial interactions, *and* scattered data – all secured, tamper-proof, and effectively useable with

T. Bocek (✉) · B. Stiller
University of Zürich UZH
Zurich, Switzerland
e-mail: bocek@ifi.uzh.ch

B. Stiller
e-mail: stiller@ifi.uzh.ch

C. Linnhoff-Popien et al. (eds.), *Digital Marketplaces Unleashed*,
https://doi.org/10.1007/978-3-662-49275-8_19

easy to set-up and fully integrated smart contracts. A ***smart contract*** was first introduced in 1994 [1], which is considered an influential work for blockchain-based ***cryptographic currencies***.

► *A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of [a] smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs* [1].

However, a smart contract alone is not "smart" as it needs an infrastructure that can run, execute, and verify the respective contract's transaction data. In combination with such an infrastructure and its interaction with the real world, the smart contract becomes "smart". Recently, smart contracts have gained dedicated attention in the context of blockchains that provide a fully decentralized infrastructure to run, execute, and verify such smart contracts.

Smart contracts can be used for financial transactions and crypto currencies. The first and currently most popular blockchain to address a crypto currency is the ***Bitcoin blockchain*** [2], which was publically introduced in the beginning of 2009 by Satoshi Nakamoto, a pseudonym leaving room for speculations about the true identity, still unknown to this date. Although the Bitcoin system uses a scripting language, it is not Turing-complete, e. g., it does not support loops. However, for smart financial transactions these scripts can create different kinds of financial contracts, such as escrow contracts, multi-signature contracts, or refund contracts.

Ethereum [3], another current blockchain approach, offers a Turing-complete scripting language, independent of any dedicated application field. The smart contract in Ethereum runs in a sandboxed Ethereum Virtual Machine (EVM) and every operation executed in the EVM has to be paid for to prevent Denial-of-Service (DoS) attacks. Without such a payment, a script with a loop could run forever and, in turn, can overload the EVM so that other scripts cannot be executed. With a general purpose blockchain, new types of contracts compared to the Bitcoin blockchain can be created, e. g., a fully distributed digital organization, such as the DAO (Decentralized Autonomous Organization) [4].

In general, smart contracts need to run on a blockchain to ensure (a) its permanent storage and (b) extremely high obstacles to manipulate the contract's content. A node participating in the blockchain runs a smart contract by executing its script, validating the result of the script, and storing the contract and its result in a block. A block stores multiple smart contracts and is typically created at a constant time interval. For instance, Bitcoin had chosen to create a block every 10 min [2], while Ethereum blocks are created every 14 s [5]. A block has always a reference to the previous block, forming a chain of blocks, hence the term blockchain (cf. Fig. 19.1). In general, a block contains an increasing block number, a hash, a reference to the previous block, a crypto puzzle's solution in case

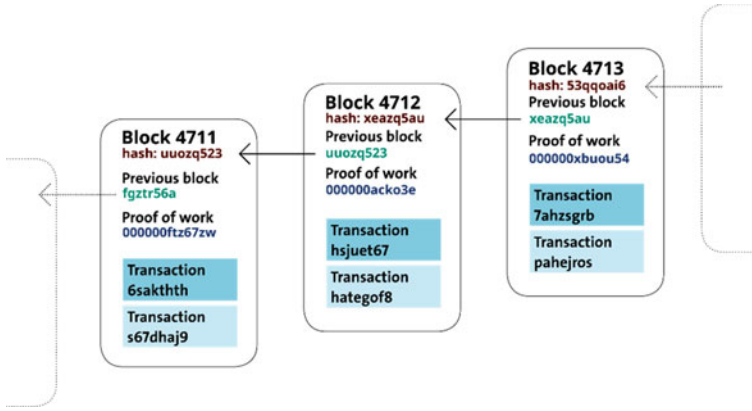

Fig. 19.1 Blockchain Example

of Proof-of-Work (PoW), and one or several transaction-related content information with encoded smart contracts.

Therefore, blockchains show the following main characteristics: full decentralization, traceability and transparency of transactions, proof of transaction viability, prohibitively high cost to attempt to alter transaction history, i. e. 51% attacks, an automated form of resolution, e. g., avoiding double spending, incentives required to participate, and trust enabling among non-trusted peers. The key advantages of blockchains are that stakeholders do not have to share a common trust basis, blockchains decentralized data storage, typically in a peer-to-peer-based network structure and replicated to all interested peers, making data loss impossible, besides act-of-god situations. Note that the terms blockchain, distributed ledger, and shared ledger are often used interchangeably [6].

The remainder of this chapter is structured as follows. Sect. 19.2 discusses Bitcoin and Ethereum, followed by current blockchain developments and limitations in Sect. 19.3. While Sect. 19.4 classifies blockchains and reviews other blockchains besides Ethereum and Bitcoin, Sect. 19.5 outlines insights into new types of applications and uses cases for the blockchain approach and highlights benefits using a blockchain. Additionally, Sect. 19.6 enlightens economic and legal challenges as well as related pitfalls. Finally, Sect. 19.7 draws conclusions.

19.2 Bitcoin and Ethereum

Once ***transactions*** are stored in a block they are considered secure after other blocks have been added to the blockchain. *E. g.*, Bitcoin suggests to wait for 3 to 6 blocks [7], Ethereum suggests to wait for 10 to 12 blocks [8]. Since blocks are created in a distributed manner, two or more blocks can be created at the same time with potentially conflicting transactions. Accepting a conflicting transaction in those blocks created at the same time could

result in "double-spending", that means the user could spend "coins" in another transaction, leaving the other user with an invalid transaction. Thus, a resolution or consensus protocol is required to discard conflicting blocks. Waiting for a certain amount of blocks practically eliminates this double-spending possibility.

The ***creation of a block*** requires the use of a scarce resource. Currently in Bitcoin and Ethereum this is processing power and electricity. This means that creating a block requires time and energy. To incentivize the creation of blocks, a reward is given to those who created a block. The reward in the Bitcoin system is currently 12.5 bitcoins for creating a block, which has at the time of writing a value of approximately 8125 €, in Ethereum it is 5 ethers with a value of 50 € for every block created. The creation of a block requires the solving of a crypto puzzle, in case of Bitcoin it is the solution of partial SHA256 hash collisions, thus, requiring to invest in processing power and energy. Those who create these blocks are termed miners, as they generate "coins", which is an analogy to the extraction of valuable minerals. Miners compete with each other to solve respective crypto puzzles, leading in the case of Bitcoin to a specialization and recently to a centralization of miners [9]. As one of the key ideas of Bitcoin is its decentralization, the centralization of miners is considered an unfavorable development. Thus, Ethereum has taken countermeasures in order to keep its system fully decentralized. One of these measures is the change of the crypto puzzle to a Proof-of-Stake (PoS) in the near future, making any hardware investment difficult to amortize, since PoS does not need a lot of processing power or electricity.

Fig. 19.2 shows the big picture, how the blockchain is used by users, miners, and exchanges – the three key stakeholders in such an approach. When a user sends coins to other users, it creates a smart contract, encodes the contract in a transaction, and broadcasts the

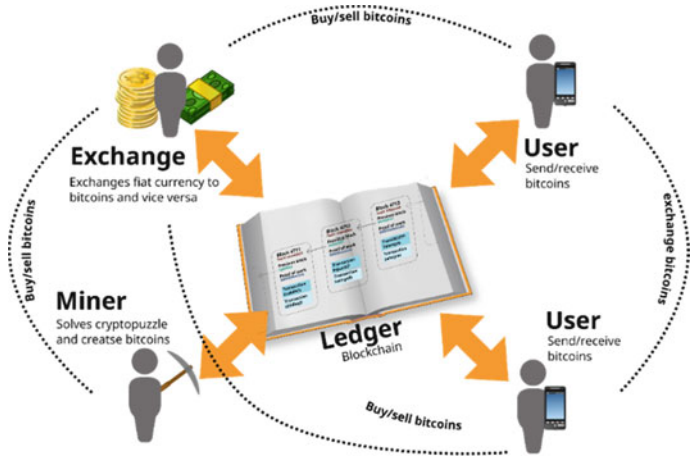

Fig. 19.2 The Big Picture of Blockchain Stakeholders with Miners, Users, Blockchain, and Exchanges

transaction. The recipient user may see the transaction broadcasted within seconds, but as this transaction is not yet in the blockchain, double spending is still possible. The miner also will receive the transaction broadcasted and will start to solve the crypto puzzle. Once a puzzle is solved by a miner, the block will be broadcasted to all peers and other miners will know that they have to restart their process and start solving another crypto puzzle.

Every block that contains a solved crypto puzzle will be added to the blockchain by each node in the system by applying the consensus mechanism in case of needs. The miner that solved the crypto puzzle gets rewarded and can use these coins or exchange them to a government-issued currency at an exchange site. This is often required as electricity bills are typically paid with "fiat" currency. Any user receiving bitcoins can also exchange these to fiat currency. Exchange sites, such as Bitstamp, the first EU-licensed Bitcoin trading site [10], require the user to register and conform to regulations such as Know Your Customer (KYC) [11]. Such regulations are not required when transferring bitcoins, however, as soon as bitcoins are exchanged to a government-issued currency (e. g., US$ or €), a user can be identified. For Bitcoin and Ethereum Table 19.1 overviews the key technical and design features as well as current statistics as of September 2016.

Table 19.1 Bitcoin and Ethereum Key Technical and Design Features

Bitcoin [2]	Ethereum [12]
A maximum of 21 million bitcoins supply, halving newly generated supply every 4 years	Unlimited ethers supply
10 min block creation time	14 s block creating time
Crypto puzzle via partial SHA256 hash collision, requiring CPU time and minimal RAM; dedicated hardware, application-specific integrated circuit (ASIC) used [9]	Crypto puzzle is variation of Dagger-Hashimoto [13], which requires besides CPU time also RAM; GPU cards currently used
Limited scripting language, not Turing complete	General-purpose scripting language, Turing complete
Started in 2009, creator unknown (pseudonym used: Satoshi Nakamoto)	Started in 2015, initiator Vitalik Buterin
Balance based on unspent transaction outputs	Balance is account-based
Transaction costs driven by transaction size	Transaction costs driven by operations in the smart contract
Max throughput: 3–7 transactions per second	Max throughput: 23–25 transaction per second
Transactions created by users	Transactions created by users or smart contracts
Market capitalization: 9.9 billion USD [14]	Market capitalization: 1 billion USD [14]
Bitcoin created: 15.8 million BTC [14]	Ethers created: 83 million ETH [14]

19.3 Current Blockchain Developments and Limitations

In general and as of today, blockchains, especially for Bitcoin or Ethereum, ***do not scale***. The ever increasing number of transactions makes the blockchain grow. Currently, Bitcoin transactions stored in the Bitcoin blockchain show a size of 75 GByte. The Ethereum blockchain, while still much younger than the Bitcoin blockchain, observes the same issue and has as of today a size of 24 GByte. While scalability is being discussed between many researchers and companies in the world and solutions are being proposed, the specific scalability solutions differ greatly for Bitcoin or Ethereum. The latter uses a general purpose blockchain, while the former is based on a specialized blockchain. This specialized blockchain offers mechanisms – typically specified to meet application demands and to make the approach scalable –, while the general purpose blockchain is much more difficult to scale for a general application.

Specifically, Bitcoin is introducing a mechanism termed "segregated witnesses" [15], which removes besides transaction malleability also signatures in the transaction resulting in smaller transactions. As of today and in the long term other solutions are discussed, such as snapshots or pruning of spent transactions. For Ethereum, "sharding" has been proposed, where an Ethereum node stores only parts of the blockchain, while other nodes host other parts. However, as of today sharding exists only in theory and shows other unresolved issues, such as rogue validators, communication across multiple shards, and reaching global consensus, while working on partial data only. The key future challenge is to design and build scalability mechanisms for general purpose blockchains, without trading their inherent advantages discussed above.

Currently the debate in the Bitcoin system either to increase the block size or to make the protocol more efficient with segregated witnesses will not solve scalability in the long term. Also with segregated witnesses, which is planned to be integrated soon, the Blockchain is only growing slower by a constant factor. Scaling to the volume to VISA credit card transaction numbers, which show around Christmas 57,000 transactions per second, is not feasible anytime soon, as the Bitcoin system currently allows for only 3–7 transaction per second. Ethereum has a similar low number of 25 transactions per second and adopting Ethereum- or Bitcoin-based products may suffer from increased transaction fees when the limit is reached. It is expected that Ethereum reaches a much higher transaction per second rate, once the switch from PoW to PoS has been performed.

Smart contracts execute based on their input and contract code. If the smart contract was not properly designed, e. g., allowing to withdraw funds from an unauthorized address, such a withdrawal may be unintentional, although the smart contract executed correctly. To reflect the intention of the smart contract creator, a language is used to specify the contract. Ethereum offers the language Solidity, a typed JavaScript dialect. However, Solidity it is not concise and easy to use as seen with the DAO disaster [4], although the DAO smart contract code was written by Ethereum experts. Yet, a security problem allowed to withdraw funds. Current best practices recommend to keep the contract as simple as possible, which may not be doable in all situations, since some contracts are complex

by design. Ethereum runs smart contracts in the EVM. To produce respective code, a language needs to compile Solidity-based smart contracts written to EVM byte code. Future language research may reveal better alternatives, such as using a functional language for the EVM or adding functional elements to improve Solidity.

Lastly, while many factors affecting a blockchain's security, either permissionless or permissioned (cf. Sect. 19.4 below), such as block size, network size, or end-to-end delay, have been evaluated in the recent past, a comprehensive approach to a blockchain ***security and performance evaluation*** is still missing. Thus, the need for (a) a comprehensive threat model, (b) an impact model of the infrastructure (either the public network, separate clouds, or cross cloud-based alternatives), (c) a Service Level Agreement for a blockchain's performance, and (s) a suitable testing as well as management framework has emerged.

19.4 Classification, Related Work, and Key Characteristics

As of today major observations on smart contracts in general and blockchains specifically are summarized here to establish a basis for future application evaluations and to benefit investigations with respect to technology, economics, and regulation/law. Thus, blockchains can be classified using the following dimensions: (a) accessibility, (b) consensus mechanisms, and (c) its crypto currency.

The first dimension determines how the blockchain can be accessed (***accessibility***), whether it is publically available or if it requires permission to access it. The two main categories in the accessibility dimension cover: public blockchains (permissionless) and private or private group-based (consortium [3], permissioned) blockchains as shown in Table 19.2.

The second classification dimension is the ***consensus mechanism***. A consensus mechanism is one of the key features in a distributed system in order that all nodes will reach eventually the same state. Distributed systems can use Byzantine Agreement Protocols such as Paxos [16] or Raft [17] as a consensus mechanism, however, Sybil attacks [18] can

Table 19.2 Accessibility

Public Blockchain (PUB)	Private or Private Group-based (Consortium) Blockchain (PRIV)
A public blockchain can be accessed and used by anyone following the respective protocol E. g., in Bitcoin, there is one reference implementation and several independent libraries that can participate in the Bitcoin network written in Go, Java, JavaScript, C, C++, Python, or Objective-C	A private blockchain is controlled by (a) a single organization that manages the permission or (b) a consortium with known members The access is controllable and permissioned. Any open source blockchain could be used as a private blockchain with small modifications, however, there exist specialized blockchains for running a private blockchain

render those consensus mechanisms useless. Thus, consensus mechanisms for blockchain need to by Sybil-proof. For public blockchains this is typically a PoW or PoS approach, for private or consortium blockchains it is PoS or a Trusted Entity (TE) acting as a gatekeeper and may be used in combination with the Byzantine Fault Tolerant protocol. Sidechains may leverage the consensus mechanism of its parent chain [19]. provides an overview on consensus protocols in blockchains. Table 19.3 summarizes the key three categories.

The third dimension distinguishes, whether the blockchain uses a ***crypto currency*** or not. This currency can be either mined or pre-created/burned (cf. Table 19.4). In the following existing blockchains are reviewed and categorized according to these dimensions. Many of those blockchains listed are a Proof-of-Concept (PoC) and it is yet to be seen how reliable they will work in the future. Since over 600 crypto currencies with a market capitalization exist [14], the focus here is laid on the most important, influential ones, while many specifically Bitcoin-based altcoins are omitted.

Bitcoin has the largest market capitalization and uses a PoW consensus mechanism. All blocks are created, as shown above, every 10 min and the reward is currently at 12.5 bitcoins, halving every 4 years. Bitcoin is a public blockchain with many clients and libraries available. Many variations of Bitcoin exist, the most popular with respect to market capitalization is *Litecoin*, which is based on the Bitcoin source code, but has a different PoW mechanism that makes it hard to use dedicated hardware for mining. Litecoin shows a block creation time of 2.5 min.

Ethereum also uses PoW, however, Ethereum plans to switch from PoW to PoS soon, especially to relax from the strong power and energy dependency of crypto puzzle usage. As such it is planned to lower costs of mining and increase the scalability. While some

Table 19.3 Consensus Mechanisms

Proof-of-Work (PoW)	Proof-of-Stake (PoS)	Trusted Entity (TE)
PoW is the consensus mechanism used in Bitcoin and Ethereum. A difficult crypto puzzle ensures that possible double spending attempts are expensive The main drawback is the huge amount of energy used to solve these crypto puzzles PoW can run with dedicated hardware (ASIC) or with a memory and bandwidth-hard crypto puzzle (MEM-HARD)	PoS defines a consensus mechanism, where owners of a crypto currency have to prove ownership (proof for their stake). A user with 1% of the crypto currency can create 1% of the blocks The main concern with PoS is "nothing at stake", with several mechanisms proposed to solve it [19] A mix between PoS and PoW is termed Proof-of-Activity (PoA) PoS is considered resource-friendly Several schemes exist with voting delegates (DELEG) or prepaying crypto currency (PRE)	Trusting entities defines another form of consensus, where multiple trusted entities can vote (and/or apply a Byzantine Fault Tolerant protocol) or a single trusted entity can decide for or against adding a block to become part of the blockchain Similar to PoS, TE is resource-friendly Many private blockchains use TE, however, there are also public blockchains, where trusted entities can vote or trusted entities can be chosen

Table 19.4 Crypto Currencies

Mining Crypto Currency (CRY-M)	Pre-creating Crypto Currency with Distribution (CRY-P)	No Use of Crypto Currency (NCRY)
The result of mining is a block with a reward in the form of crypto currency. Bitcoin and Ethereum reward with bitcoins and ethers, respectively. Some blockchains allow to define various other crypto currencies or assets besides its native crypto currency	Instead of mining crypto currency, the currency can be pre-created and distributed in an Initial Coin Offering (ICO). The incentive to mine a block is to collect transaction fees. Other variations include "Proof-of-Burn" (PoB) or "Proof-of-Possession" (PoP) using another crypto currency	Some blockchains do not need any kind of native crypto currency, but allow for overlay assets. Especially private blockchains do not use a native currency

elements may require PoW initially, it is planned to switch entirely to PoS. The status is a PoC that was released in March 2016 [20]. Ethereum can also be used as a private blockchain, as the source code is open and accessible.

BlockApps is such a provider for a private Ethereum blockchain. Eris Industries with their *eris:db*, which also uses Ethereum as a basis, is already using PoS, however, not in a public blockchain. Eris:db is a business-focused blockchain, where the Tendermint Consensus protocol is used for PoS. Although this protocol follows an interesting concept, if many validators sign each block, storage and network limitations may become an important issue for scalability. *Chain Core* is another company offering a blockchain for business. They provide a private blockchain with a controlled access. Further scalability improvements are planned for Ethereum with the Casper/Serenity release, such as sharding [20], which is the concept of horizontal partitioning of a database. In the case of Ethereum it is to split the space of possible accounts. Each shard gets its own validators with the idea that those validators only validate transactions within a shard and a special handling for inter-shard communication, where transactions from different accounts in different shards need to be consistently validated.

Monero is an anonymous crypto currency. It achieves this goal by using ring signatures with one real signature and several decoy signatures. Furthermore, a mixing of inputs is enforced in the network. Stealth addresses are used, making it difficult to trace the sender and recipient. Monero uses its own network, based on CryptoNote, and it uses a memory-hard PoW. Future plans consist of including the I2P protocol, an anonymization protocol to hide the real Internet Protocol (IP) address in use. Monero recently gained traction due to media coverage and the integration by darknet marketplaces, where privacy is a big concern.

Lisk is a public blockchain written from scratch. Lisk enables the development of "Dapps" (Distributed Applications), which are decentralized applications in an autonomous operation in terms of a peer-to-peer management. It uses a PoS mechanism using delegates and voting. However, a node can become a delegate only, if it owns many Lisk coins. Lisk uses smart contracts to determine procedures and constraints, which formulate rule-based, automatically operated processes.

Another blockchain written from Scratch is *IOTA*. The goal of IOTA is to become the backbone of IoT by supporting real-time transactions without fees. As it does not store the complete history, nodes going offline may take offline important history data. IOTA does not support mining; tokens will be distributed in an Initial Coin Offering (ICO) phase. Tokens are accessed using passwords rather than public/private key pairs.

Hyper Ledger an Open Source Linux Foundation project since January 2016, is a blockchain project creating a modular blockchain, specifically as an open standard for the basis blockchain technology of the Distributed Ledger Technology. The aim is to bring the blockchain technology a step forward to mainstream commercial adoption. They offer a modular architecture so that they can use any kind of consensus mechanism, such as PoW, PoS, or TE.

Nxt uses PoS as well and similar to IOTA is uses passwords to access crypto assets rather than public/private key pairs. Another business-oriented blockchain is *R3 Corda*. R3 Corda is a distributed ledger for recording and managing financial agreements. Unlike other blockchains, R3 Corda does not share transactions with other nodes. Only those parties involved in that transaction can access the data. Also validation is done by those parties involved and not by a random node. *Openchain* is a private blockchain for organizations that can be configured as a Bitcoin side chain. It supports smart contracts. It uses a trust-based consensus mechanism and uses a client/server architecture.

Stratis is built on top of the Bitcoin blockchain and allows to create private sidechains. Another business-oriented blockchain is *Multichain*, where private blockchains can be built. It is compatible to the Bitcoin API, however, allows many configuration options, such as block size, types of transactions, who can access it, and its assets. Any type of assets can be used and created on Multichain, allowing to trade shares, bonds, or commodities. In terms of scalability, *BigchainDB* claims to allow 1 million writes per second and petabytes of capacity. It is a private blockchain connecting to a RethinkDB cluster to achieve that speed. *Rootstock* (RSK) is a Bitcoin sidechain, which offers smart contracts with a Turing-complete language. RSK is compatible with the Ethereum VM and can run its smart contracts. Its currency Rootcoins can be exchanged to Bitcoins and vice versa. Similar to Rootstock is *Counterparty* that allows Ethereum smart contract to run on the Bitcoin platform. Counterparty uses a native currency, but allows to create any kind of assets. Another company working on sidechains is Blockstream, also providing an im-

Table 19.5 Classification

Approach	Accessibility	Consensus	Crypto Currency
Bitcoin	Public	PoW/ASIC	CRY-M/Bitcoins
Ethereum	Public	PoW/MEM-HARD	CRY-M/Ethers
Ethereum Casper/Serenity	Public	PoS/PoA	CRY-M/Ethers
Litecoin	Public	PoW/MEM-HARD	CRY-M/Litecoin
Monera	Public	PoW/MEM-HARD	CRY-M/XMR
Lisk	Public	PoS/Del	CRY-M/Lisk
R3 Corda	Private	TE	NRCY
Openchain	Private/sidechain	TE	NRCY/various
IOTA	Public	PoW	CRY-P/IOTA tokens
Eris:DB	Private	PoS	CRY-M/Ethers
Chain Core	Private	TE	NRCY/various
Hyper Ledger	Private	TE/PoW/PoS	NRCY
Nxt	Public	PoS	CRY-P/various
Stratis	Private/sidechain	PoW (PoS in future)	CRY-M/STRAT token
Multichain	Private	PoW	NRCY/various
BigchainDB	Private	TE	NRCY/various
Rootstock	Public/sidechain	PoW (Bitcoin)	CRY-M/Bitcoin-Root-coin
Counterparty	Public	PoW (embedded Bitcoin consensus)/PoB	CRY-P/various
Ripple	Public	TE	CRY-P/Ripple/various
Stellar	Public	TE/PoP	CRY-P/Lumen/various

plementation of the *Lightning* network, which allows micro transaction on the Bitcoin blockchain.

Ripple is different since it uses trust to find consensus and nodes not behaving well are blacklisted. Ripple can send any currency and can automatically exchange currencies, while each transaction is verified in seconds. *Stellar* is based on Ripple, but uses its own consensus mechanism. Table 19.5 classifies these blockchains.

19.5 New Applications

Blockchains allow for new distributed applications. The main interest in the financial sector is to digitalize processes with other stakeholders and to eventually save money. In this chapter new types of distributed applications besides those financial ones, such as remittance, crowdfunding, or money transfer, are discussed. An example of such an application is *CargoChain*, which is a Proof-of-Concept (PoC) created at a hackathon to show how to

reduce paperwork, such as purchase orders, invoices, bills of lading, customs documentation, and certificates of authenticity.

Other popular non-financial areas with active blockchain projects are (a) fraud detection with *Everledger, Blockverify*, *Verisart, Ascribe, Provenance,* and *Chronicled*, (b) global rights databases with *Mediachain, Monegraph,* and *Ujo Music,* (c) identity management with *Blockstack*, *UniquID, ShoCard,* and *SolidX*, (d) ridesharing with *LaZooz* and *Arcade City,* and (e) document verification with *Tierion* and *Factom*. Many other types and applications in smaller application areas for the blockchain exist, such as *Augur* aiming at the prediction of markets with crowd intelligence. *Swarm* is a distributed storage platform and content distribution service. Dispute resolution systems based on blockchains or *Enigma*, a decentralized cloud platform with guaranteed privacy. *ChromaWay* has a first pilot carried out with a private blockchain for land registry. The *Blockchain Voting Machine* is a digital voting solution using its own VoteUnit blockchain. Temperature monitoring is performed by *modum.io* to enable cost savings in the pharmaceutical cold chain by combining sensor devices with blockchain technology.

[6] argues that many public, governmental applications can be implemented in form of a permissioned ledger, in which the party of the transaction needs to proof access via a dedicated credential. Transaction parties may be authorized governmental or public offices, for which each beneficiary may access his rights from a centralized authority, controlling the distributed ledger system's access. Obviously, only to trusted parties and beneficiaries such credentials will be granted. Upon such an approach, participants may – driven by the system-inherent proof of a transaction – interact reliably and trustworthy without any third party.

Finally, any application, which requires a trusted third party as a mediator between at least two stakeholders being involved in the process to conclude a contractual relationship, potentially can benefit from a blockchain. Besides the roles of banks and their mediation role for financial transactions, notaries as mediators for, e. g., property sellers and buyers – including respective enforcement options on the basis of related smart contracts – and escrow agents with a fulfillment mandate serve as an excellent application domain, largely unexploited as of today.

19.6 Legal and Economic Challenges

Blockchains are termed the "Blockchain revolution" [21] and adoption in domains requiring a very clear, stable, and secured state for all transactions is increasing as outlined above. Although the example of Bitcoins shows that crypto currencies on the basis of blockchains have reached a much wider adoption than any other electronic and fully digital payment system of the past, Bitcoin payments have been made possible by complementing other payment channels, such as restaurant payments [22], governmental transaction fee payments [23], and person-to-person payments [24]. Bitcoin has been regulated by national banking authorities, such as the Swiss Financial Market Supervisory Authority

(FINMA) [25], and different exchanges for bitcoins are possible into any regularly tradable fiat currency. Thus, a legally acceptable, however not uniform situation has been reached besides from a technical perspective of trading bitcoins and paying with bitcoins.

Therefore, it could be concluded that blockchains – the key underlying distributed technology – have been blooded, since they have been applied in the financial market sector. However, that needs to be considered as a short-handed argument, since other examples of a blockchain use in the financial markets have shown errors as in The DAO [4], malfunction as with Mt Gox [26], or get-quick-rich schemes [27]. Thus, in general it is too early to determine principle legal problems with blockchains, however, as [28] states, "how self-regulation has failed" and "how Bitcoin has not matched the expectations of some proponents. Various crashes and wave after wave of scandals and allegations of fraud have decidedly dented the perception that Bitcoin is the currency of the future." Nevertheless, legal frameworks and governmental regulation (for a very recent per-country regulation on Bitcoin see [29]) may need to adapt to take blockchain developments into account, while assuring at the same time data privacy, security, and other key facets of data handling, maintenance, and storage, many of which are determined and regulated already for other ICT-related applications and technologies. Thus, the perception of blockchains in society, with governments, and their possibly new reach in respective law and jurisdictions cannot be foreseen, however, the technical potential to offer trusted communications and persisted storage without any central element of control or operations offers opportunities, where especially human-based counseling of contact negotiations may not be required anymore.

Besides these views, it has to be stated that the economic perspective of blockchains is often broken down to an optimized performance and operation view, especially in comparison to today's technology in operation. Still, this has to be proven in a larger scale, since those approaches, which need to solve crypto puzzles do need a significant amount of electrical energy to perform the computations, determining a very clear factor for operational costs (OPEX). Thus, the PoW approach shows drawbacks compared to the PoS approach and others. It is estimated that mining actions require approximately 370 MW of energy for 2015 [30], the capacity of a smaller nuclear power plant.

As this determines a large amount of energy, optimizations in that dimension are essential. However, a future prediction of the energy consumption of Bitcoin miners in 2020 is difficult as relevant factors for a viable prediction will include at least: (a) the value of 1 Bitcoin in 2020, (b) the development of new hardware to solve crypto puzzles, (c) the reaction of miners to the halving of mining rewards, (d) the costs of energy applicable to which parts of the world, (e) the role will the Bitcoin blockchain may have in 2020, (f) the possibility to reach a practically infeasible blockchain length by or before 2020, (g) the effects of "side-chains" being developed these days, and (h) if Bitcoin is still using PoW and not, e. g., PoS.

19.7 Summary and Conclusions

A blockchain is a distributed database maintaining securely a continuously growing list of transactional data, which are hardened against tampering and forgery. The discussion of main characteristics as well technical features of blockchains or distributed ledgers above reveals that such technology is in the wings to simplify administrative and transactional procedures and many applications in the future. While the simplification mainly relates to the decentralization and distribution of the data (at the same time assuring a lossless storage), the security and access control of those data is maintained efficiently, though, performance-wise not fully optimized yet. A unique proof of a transaction – including payments, access right grants, contracts operations, or data entry updates for commercial parties, citizens, companies, and governmental organizations – can be reached today. However, the cost-benefit ratio of blockchains cannot easily be quantified. Although, costs for, e. g., hardware, virtual machines, the network, and setups, are known, the benefits of less centralized infrastructure including soft factors, such as less trust and more transparency, are difficult to assess.

Specifically in the context of formal procedures, say for (a) commercial orders between a customer and a supplier or for (b) administrative acts between a citizen and a governmental organization, all participating parties will have the chance to check the status of such a procedure, since all parties do have access to all related data in a distributed manner, independent of their current location. Cross-organizational procedures, such as approvals, clearances, and permits, can relate to the same blockchain maintained for them to ensure an optimized handling. Note that only key information may become part of the blockchain itself, such that related electronic documents can be related via dedicated cryptographic hash values in time to the respective party. Signed time stamps can potentially speed up processes, maximizing the customer-supplier or citizen-governmental organization relationships. A public and legal acceptance of such procedures needs to be seen.

Blockchains are considered the "blueprint for a new economy" [31], which suggests that new technology can improve efficiently the existing status-quo of many application fields for distributed and reliable storage of secured transactions between customers and suppliers as well as citizens and governments. As discussed above, besides these new application domains digital market transactions, the financial industry, and governmental or private smart contracts in a decentralized form can be embedded into today's IT landscape. And due to the multitude of applications discussed many start-ups follow the blockchain path today, since an emerging potential and economic benefit is commonly considered to be in place. The survival rate of those start-ups and the success rate of the blockchain technology in the private and public application domain will tell, if all or only parts of those technically available characteristics and advantages can be practically exploited.

Acknowledgements
This work was partially funded by the FLAMINGO Network-of-Excellence (NoE) within the EU FP7 Program under Contract No. FP7-2012-ICT-318488.

References

1. N. Szabo, "Smart Contracts," 1994. [Online]. Available: http://szabo.best.vwh.net/smart.contracts.html. [Accessed 6 August 2016].
2. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
3. V. Buterin, "On Public and Private Blockchains," Ethereum.org, 7 August 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. [Accessed 6 August 2016].
4. "The DAO," [Online]. Available: https://daohub.org/. [Accessed 6 August 2016].
5. "Ethereum Average BlockTime Chart," Etherscan – The Ethereum Block Explorer, [Online]. Available: https://etherscan.io/charts/blocktime. [Accessed 6 August 2016].
6. "Distributed Ledger Technology: Beyond Block Chain," UK Government Chief Scientific Advisor, 19 January 2016. [Online]. Available: https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review. [Accessed 29 August 2016].
7. "Confirmation," bitcoin wiki, 14 June 2016. [Online]. Available: https://en.bitcoin.it/wiki/Confirmation. [Accessed 29 August 2016].
8. V. Buterin, "On Slow and Fast Block Times," 14 September 2015. [Online]. Available: https://blog.ethereum.org/2015/09/14/on-slow-and-fast-block-times/. [Accessed 29 Augest 2016].
9. J. Tuwiner, "Bitcoin Mining Centralization," bitcoinmining.com, [Online]. Available: https://www.bitcoinmining.com/bitcoin-mining-centralization/. [Accessed 8 August 2016].
10. "Bitstamp to Become the First Nationally Licensed Bitcoin Exchange and Launches BTC/EUR Trading," Bitstamp, [Online]. Available: https://www.bitstamp.net/article/bitstamp-first-nationally-licensed-btc-exchange/. [Accessed 8 Augusst 2016].
11. "Europen Union: Directive 2005/60/EC of the European Parliament and of the Council on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing," 25 October 2005. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005L0060.
12. G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger," 2015. [Online]. Available: http://gavwood.com/paper.pdf. [Accessed 29 August 2016].
13. "ethereum/wiki," September 2015. [Online]. Available: https://github.com/ethereum/wiki/blob/master/Dagger-Hashimoto.md. [Accessed 29 August 2016].
14. "Crypto-Currency Market Capitalizations," [Online]. Available: https://coinmarketcap.com/all/views/all/. [Accessed 29 Augest 2016].
15. "Segregated Witness Benefits," Bitcoin Core, 26 January 2016. [Online]. Available: https://bitcoincore.org/en/2016/01/26/segwit-benefits/. [Accessed 29 August 2016].
16. L. Lamport, "Generalized Consensus and Paxos," Microsoft, March 2005. [Online]. Available: https://www.microsoft.com/en-us/research/publication/generalized-consensus-and-paxos/. [Accessed 29 August 2016].
17. D. Ongaro and J. Ousterhout, "In Search of an Understandable Consensus Algorithm," in *2014 USENIX Annual Technical Conference (USENIX ATC 14)*, Philadelphia, PA, USA, 2014.
18. J. Douceur, "The Sybil Attack," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems (IPTPS 2001)*, London, UK, 2002.
19. M. Swan, "Blockchain Consensus Protocols," Bitcoin Meetup, 6 May 2015. [Online]. Available: http://www.slideshare.net/lablogga/blockchain-consensus-protocols. [Accessed 29 August 2016].
20. V. Buterin, "Serenity PoC2," 5 March 2016. [Online]. Available: https://blog.ethereum.org/2016/03/05/serenity-poc2/. [Accessed 29 August 2016].
21. D. Tapscott and A. Tapscott, How the Technology Behind Bitcoin is Changing Money, Business, and the World, New York, USA: Penguin Random House LLC, 2016.

22. "What Can You Buy with Bitcoin?," CoinDesk, 19 October 2015. [Online]. Available: http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/. [Accessed 29 August 2016].
23. E. Aschwanden, "Stadt Zug wird weltweit zum Bitcoin-Pionier," 10 May 2016. [Online]. Available: http://www.nzz.ch/schweiz/crypto-valley-zukunftsmodell-oder-marketing-gag-ld.22911. [Accessed 29 August 2016].
24. "Coinblesk," [Online]. Available: https://bitcoin.csg.uzh.ch/. [Accessed 29 August 2016].
25. "Swiss Financial Market Supervisory Authority FINMA," [Online]. Available: https://www.finma.ch/. [Accessed 29 August 2016].
26. Y. B. Perez, "Mt Gox CEO Mark Karpeles Charged With Embezzlement," CoinDesk, 11 September 2015. [Online]. Available: http://www.coindesk.com/mt-gox-ceo-mark-karpeles-embezzlement/. [Accessed 29 August 2016].
27. "Bitcoin Nachahmer: Riskante virtuelle Währungen," 8 August 2016. [Online]. Available: https://www.test.de/Bitcoin-Nachahmer-Riskante-virtuelle-Waehrungen-5057128-5057138/. [Accessed 29 August 2016].
28. A. Guadamuz and C. Marsden, "Blockchains and Bitcoin: Regulatory Responses to Cryptocurrencies," *First Monday,* vol. 20, no. 12, 7 December 2015.
29. "Legality of bitcoin by country," [Online]. Available: https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country. [Accessed 29 August 2016].
30. V. Tombez, "Le bitcoin a consommé en 2015 autant d'énergie que 620'000 ménages," RTS Info, 26 April 2016. [Online]. Available: http://www.rts.ch/info/sciences-tech/7674767-le-bitcoin-a-consomme-en-2015-autant-d-energie-que-620-000-menages.html. [Accessed 29 August 2016].
31. M. Swan, Blueprint for a New Economy, Sebastopol, California, USA: O'Reilly Media, 2015.