Information Systems Frontiers (2020) 22:29–35
https://doi.org/10.1007/s10796-019-09946-6

Blockchain in Context

Andrew J. Ehrenberg [1] **· John Leslie King** [1]

Published online: 22 July 2019

Abstract
Blockchain has been used primarily in cryptocurrency applications like Bitcoin and Ethereum. These use cases show the staying power of blockchain technology and suggest additional uses such as smart contracting. We suggest these use cases, while producing knowledge, do not forecast the future of blockchain. Learning-by-doing reveals the evolution of blockchain as a sociotechnical system, suggesting that there is more to learn. Predicting how sociotechnical systems will evolve is difficult, but historical and lexical analyses suggest two areas for blockchain growth. One is provenance, authentication through recording of ownership or other control state, applicable to jewels, real property, art works, food stuffs, designer items, and anything else where genuineness is valued. The other is chain-of-custody, proving that duty of care has been faithfully executed regarding living beings (children, people in legal custody, research subjects, research animals, pets), or that inanimate things (evidence, data, representations such as photographs) have not been tampered with.

Keywords Blockchain · Cryptocurrency · Bitcoin, Ethereum · Provenance · Chain of custody · Sociotechnical system

1 Introduction

Blockchain is not a *deus ex machina,* descending from heaven to resolve society's foundational issues. Blockchain involves fascinating new technology but it is also an aspiration. Blockchain has been treated like a brand to signal optimism about the new. This is misleading. The early internet (Dot Com) ventures put .com in their names to signal optimism and attract investors. Speculative value in the new technology became real to some, but naming did not make up for weak business models when Dot Com went bust. Companies that grew with the emerging commercial Internet market sometimes proved unsustainable. A few that succeeded (Amazon.com) were accompanied by many that did not (e.g., Pets.com, Freeshop.com). We see something similar in mass market visions of blockchain associated with cryptocurrency. Blockchain's true value can be seen only through better understanding of blockchain evolution as a sociotechnical system. That is gained through learning-by-doing, historical analysis, and lexical analysis. These lead us to provenance and chain of custody. We explore that evolution after a brief blockchain primer.

✉ John Leslie King
jlking@umich.edu

1 University of Michigan, Ann Arbor, MI, USA

2 A Blockchain Primer

Blockchain depends on information technology.[1] A set of information blocks on computers (transaction information, time stamp, block-specific information such as nonce value) is chained together in a digital ledger. Blockchains are typically peer-to-peer networks. New blocks are only admitted after "proof," like "proof of work" that requires solving a complex computational math problem through "mining." Successful miners are rewarded and their new blocks added to the end of the chain. Each block has a unique "hash" – a code that tells it apart from other blocks – and the hash of the block before. These hash codes link the blocks within the chain. A sender signs a transmission with a private key and a receiver decodes the encoded transmission with a public key. This secures transactions. Verified transactions are those that are proven within the system to have occurred as claimed. Only verified transactions can be stored in blocks before the chain is updated. Altering anything causes a block's hash to change that ultimately makes the entire chain invalid. If one wants to manipulate the blockchain successfully, it is necessary to convince a majority of nodes. Changing enough blocks almost simultaneously is prohibitively costly. The information in blocks can be made public as read-only, but not edited. This increases transparency. This combination of authoritative

[1] This paper does not explain the details of blockchain. See the following: (Beck 2018; Beck et al. 2017, 2018, Cao 2018; Marr 2017; XBT Network 2018))

blocks, transaction security, difficulty with manipulation and transparency makes blockchain special.

In principle, blockchains are "trustless," decentralized, hard to hack, and the information on them secure. In reality, blockchains are not "trustless." The trust previously placed in third parties is shifted to the blockchain system. Blockchains are not necessarily decentralized, but decentralizable. Nothing prevents a central authority from offering blockchain services.[2] Hackers have altered information on a blockchain by compromising enough nodes to "outvote" the other nodes (sometimes called a 51% attack). In cryptocurrency blockchains single coins have been spent twice in transactions too fast for the network to keep up (sometimes called a race attack, similar to decades-old "float" exploits). Cryptocurrency blockchains have seen substantial theft (over $1.2 billion in Q1 of 2019 according to Takahashi 2019). Blockchain problems have been anticipated in some cases. Some are said to be no worse than competitor systems. On the other hand, hyperbolic blockchain virtues are sometimes countered by facts. Technical improvements might fix some or all of these problems. Nothing is inevitable; little can be predicted precisely.

3 Mass-Market Visions

Evolution of complicated sociotechnical systems contradicts mass-market visions of new technologies. Niches like open source development communities can support fast technical evolution. The "socio" can evolve more slowly, with technology running ahead. Users who cannot understand interfaces might fall to the back half of the adoption curve. Primacy and recency effects are reinforced when the first experience is also the most recent. Cryptocurrency was the first and still is the most socially and economically relevant implementation of blockchain. Almost everyone knows about Bitcoin. Focusing on cryptocurrency can occlude the blockchain ecology.

Cryptocurrency seems like ordinary money until one looks at the details. Cryptocurrency is from a system, not an authoritative third party like a bank. Cyptocurrency unit values can fluctuate greatly, less like a currency and more like a tradeable high-risk/high-reward asset (Popper 2019). Outside of FX arbitrage traders (whose margins are thin to begin with) fiat money is generally exchanged at at a rate, not sold. With cryptocurrency secondary markets appear (e.g., initial coin offerings, crypto trading). Get-rich-quick schemes pop up. Blockchain infrastructure becomes conflated with cryptocurrency. A stigma of shady activity still lingers for blockchain due to early uses of cryptocurrency for things like sex and drug trafficking, ransom payments, and money laundering until improved forensics reduced this. Such social implications of cryptocurrency are confusing: privacy might attract criminals but transparency might repel criminals. Prosocial applications can be overlooked in the confusion.

It is not clear that blockchain cryptocurrency can replace traditional fiat money. Take cash, an ancient form of fiat money, as an example. Blockchain does not forget, but cash usually forgets. A person with a U.S. $100 bill might call it "My Benjamin" (it has Benjamin Franklin's picture on it). That person does not care whose Benjamin it was before, nor whose Benjamin it will be next. It says on the bill that the Benjamin is worth 100 U.S. dollars. Some fiat currencies have been volatile but not so the U.S. dollar and similar "hard" currencies. Nor does the person holding the Benjamin care whether it is *this* Benjamin. Any and all Benjamins are *fungible*. On the whole, cash works. Yet it makes up less than 10% of the world's $33 trillion money supply (Desjardins 2017). The rest is digital information in bank and investment accounts, or in third-party payment platforms (e.g., PayPal, Venmo, Alipay). Nor is cryptocurrency-like virtual security common. Only 1% of non-cash spendable assets are virtually secured.

Balancing lawfulness and personal privacy is a challenge, yet the fiat money world of financial institutions, governments, cybersecurity/cyber-risk startups, and other stakeholders have used specialized tools to trace unlawful transactions while honoring privacy and other regulations (Bragina 2018). Blockchain might or might not help with detecting fraud, mitigating theft, or tracking down criminals; it is early and blockchain forensics are still developing. However, unless blockchain is very like fiat money, it will be necessary to adjust the tumultuous regulatory environment and assign interim risk to deal with cryptocurrency. To date, cryptocurrency's lure has more to do with capital gains than with currency. Traders now capitalize on inefficiencies in the nascent cryptocurrency markets to generate larger profits than bonds, equities, and derivatives offer. That might change in time, but it is now the reality. Online conversation can make prices of any money hypersensitive to public opinion, and cryptocurrency is no exception (e.g., cointelegraph.com). If the objective is to make cryptocurrency comparable with fiat money, why not just use fiat money?

Cryptocurrency using blockchain has gathered attention and made blockchain real. It has produced learning-by-doing. What has been learned?

[2] This is a fraught point: some equate distributed with decentralized, although they are not the same. It is an old issue. For interesting discussions of this see (King 1983; Buterin 2017).

4 Cryptocurrency and Blockchain: Learning-by-Doing

The concept of learning-by-doing or learning from experience is often credited to the American pragmatic philosopher John Dewey (1897, 1938). The basic idea is to gain experience by doing something, reflecting on the experience to form abstract concepts about it, test what has been learned, and apply that to gain more experience. The value of learning-by-doing has been established (Arrow 1962). It has been discussed as a key learning modality in information systems (Ryu et al. 2005). Experimenting with innovations generates insights about timing and growth, alternative applications, and the complementary assets required to release value, etc. By learning, we uncover the sociotechnical significance of blockchain. Some early learning misleads. We think it unlikely that replacing existing fiat money with cryptocurrency helps us understand the future of blockchain, but learning can be had from other aspects of cryptocurrency. One is “smart contracting.” Parties enter contracts in sight of the entire blockchain, which makes terms and provisions transparent. In some cases terms and provisions are automatically enforceable (e.g., via escrow). Trust and control issues arise. When trust is shifted to the system, system stability and security through control become paramount to the contract. Control might be programmatically governed by the system (no human supervision), or might work best as a hybrid of system and human control. “Trustless” environments have *hidden costs* to compensate for everyone cheating the system and trying to avoid being cheated by others (Werbach 2019). Participants know cheating is possible (e.g., participant private keys to individual accounts are compromised) and theft losses can be in the billions (ICODATA.IO 2019). Consolidated stores of private keys can be breached. Blockchains *can* have single points of failure. All new technologies have such problems. An entrepreneurial maxim, fail fast and keep iterating, comes to mind here. The more you do, the more you might learn.

The DAO (Decentralized Autonomous Organization) built on the cryptocurrency platform Ethereum (Ethereum.org) in early 2016 also taught control lessons. The DAO allowed project curators to raise funds from pseudonymous investors. Investor voting rights (e.g., involving proposals submitted by curators) were determined by investor virtual share allocations. Voting rights, equity, and settlement were managed transparently by automated smart contracts. There were no directors or centralized control. The DAO attracted much investment until a security problem arose. Token holders could use the *split DAO* function to move their investment elsewhere. A hacker used a trick (recursive call without condition reset) to move money (worth about $50 million at the time or one-third of all DAO investment) to the hacker’s wallet.[3] The entire Ethereum blockchain had to be forked (started anew) to salvage the losses. This became Ethereum Classic. The fork also served as an inflection point for the culture of smart contracts and the emphasis on immutability (though such immutability is what incentivizes hackers to exploit bugs in the first place). Some donors attacked the DAO to return money to the right people before the hacker drained everything, reinforcing the belief in the DAO project and creating new communities in both classic and current Ethereum.

Learning-by-doing suggests that blockchain is moving towards information infrastructure, the realm of entrepreneurs and enterprises interested in applying blockchain to routine social and commercial information needs. It takes time to ascertain the value of underlying infrastructure. Though it has now been decades only a portion of the Internet’s infrastructure value is known. In retrospect it is easy to see that enterprises unthinkable 40 years ago could emerge (e.g., Amazon.com in e-commerce and Salesforce.com in enterprise software). It took time: 10–15 years for some companies to surpass their Dot Com bubble highs; the NASDAQ took years to recover from the Dot Com bubble burst (Rushe 2015).

Mark Twain reportedly said history does not repeat itself, but often rhymes. Using history, blockchain appears to in the midst of a bubble. Post-bubble disruption might come, but no one knows how long that will take. Amazon.com and its investors made fortunes; no one really remembers those who failed. In retrospect we know that the internet transformed enterprise, but it was not clear from the onset that this would happen. Successful entrepreneurs of the Dot Com era leveraged the Internet infrastructure to solve real-world problems, irrespective of the .com in their name. Intentions to leverage blockchain infrastructure must be accompanied by willingness to experiment and learn by doing. This is to avoid failure from bad business and financial management, poor user experience, and many other factors. These factors might be centuries old: cost-cutting, sustainably lower prices, execution, modification of existing routines when necessary, and so on. Success is also contingent upon good fortune. The right timing, opportunities, influential clients/investors, etc. Learning by doing is essential for turning great organizational plans into great organizations, and a necessary condition of long-term blockchain evolution.

[3] Some prefer “exploit” to “hack.” This paper uses the terms synonymously to mean a person doing something with a computer that is not allowed by laws or rules.

5 Blockchain Evolution as a Sociotechnical System

Blockchain as a sociotechnical system is evolving in part because of innovative technology, especially the Internet that brought global information access, communication, and powerful cloud support. Ambitious entrepreneurs can use the Internet infrastructure to create network effects, data-driven marketing strategies, and connect people and organizations around the world. These accomplishments took decades with many ups and downs. The dot com world nearly collapsed while a startling change emerged. Responses evolved to meet emergent problems. The same thing is happening now: cryptocurrency's volatility has seen the response of "stablecoins" (e.g., J.P. Morgan's JPM Coin). Evolution is difficult to predict, but not impossible. Blockchain might evolve into a transport layer of Internet infrastructure. Already Ripple/XRP tokens provide currency-agnostic global money transfer that threatens SWIFT, the largest incumbent provider of currency transfer services for banks (Riseshine 2019).

Facebook's recent foray into cryptocurrency is a test of the nascent technology. It is worth paying attention any time a tech giant like Facebook invests in an emerging technology. Facebook introduced Libra in June of 2019. It is a fiat-backed cryptocurrency token similar to JPM coin. Some speculate it will be a serious alternative to traditional fiat currencies. After the announcement of Libra prominent cryptocurrencies experienced high volatility, with cryptocurrency proponents emphatically optimistic and skeptics distrustful of Facebook and Libra. Centralized institutions like banks and regulators are attempting delay until they understand Libra's implications. The conversation is dominated by proponents and skeptics, while centralized institutions still have power, and most cryptocurrencies remain volatile. As of this writing, Libra was not yet deployed. It could take months or years before its effects are clear. What makes Libra so interesting is scale. Facebook has nearly two and a half *billion* worldwide users, and despite its struggles with privacy (an issue in the 'trustless' blockchain environment), the *network effects* could be substantial. JPMorgan Chase and Bank of America have 200 million customers *combined*. Billions of people on the same transaction network could represent trillions in assets. That said, many Facebook users cannot take advantage of Libra right away because not all countries support contactless payments, connectivity, methods to purchase digital tokens, etc. Libra is said to help the 'unbanked', but many of the unbanked don't have the resources to use Facebook. It will interesting to see how Libra evolves compared to its predecessors.

Innovations compete with preceding ecosystems. Cryptocurrency competes with existing fiat money that has been around for a long time, works well, and is a standard almost everywhere. Blockchain might make the money system more secure, trackable, and difficult to counterfeit, but no one can yet say that it will rival traditional fiat money. Established ways of doing things can be hard to displace due to path dependencies. Checking and bank draft systems took decades to rival cash, as did credit cards and debit cards, but all are firmly established now. Technical innovation might punctuate evolution, as did magnetic ink character recognition (MICR) for automated check processing. Still, most innovation builds on what users already understand. Blockchain will be a game-changer only if the evolving ecosystem sees advantage in changing the game.

Complementary assets are required to deliver value. Motor transport requires motor vehicles (automobiles and trucks) but also drivers, roads, fuel, maintenance and repair, risk mitigation (e.g., insurance), regulation, enforcement, etc. Some of these complementary assets are inter-connected in the sociotechnical system. Fuel taxes help pay for roads, and vehicle registrations help with safety recalls. Motor transport depends on complementary assets, some of which co-evolved in public-private partnerships (e.g., good roads and vehicle safety). Blockchain depends on the complementary assets of for digital data networking, especially the Internet. Complementary assets must be designed in from the start or co-evolve. Design requires understanding the blockchain ecosystem, and understanding of that ecosystem is necessary to predict the course of co-evolution.

Ecosystems are context, from the Latin *contextus*, or connection. Full understanding of an event, statement, or idea requires context. Text requires context. Words with multiple meanings are disambiguated by context. People complain if their words are "taken out of context." Judicial courts routinely inquire about context when trying to interpret and render opinions about statutes and previous cases, or to establish "materiality" (something's meaning to the case). Contemporary archaeological excavation requires recording of exactly where and how items are found in three dimensional space to provide meaning later. Anything that fulfills a functional need in functionalist interpretations requires context. Contemporary scholarly research requires the context of re-executable methods and reusable data for reproducibility and economies.

"Lexical analysis," using words from descriptions and definitions, helps set the context for blockchain. Words change meaning and can be subjectivly interpreted, so caution is necessary. Blockchain is often described as a "distributed ledger." Some argue the adjective "distributed" is key, but, as noted above, there is nothing inherently decentralized in blockchain. Distributed might be nothing more than an implementation choice. Of greater interest is the noun "ledger." The Oxford English Dictionary describes a ledger as a record, (e.g., a family lineage recorded in a bible). For blockchain perhaps the best definition of ledger is from bookkeeping: the most prominent among a set of books that record business transactions (see Lemieux et al. 2019). This takes us to archival theory and the concepts of provenance and chain of custody.

The French noun, *provenance,* refers to a historic line of ownership that can validate the authenticity and origin of an item. Everledger, a blockchain-enabled provenance application, ties serial numbers to diamonds, encrypting them in a manner difficult to change or replicate. This allows identification of so-called "blood diamonds" mined in war zones, often sold to finance conflict. *Provenance* can be applied to anything that suppliers and/or customers want to ensure for authenticity, such as the origin and quality of food (organic, sustainable, wild), luxury items (designer clothing and accessories) and land records (title, legal descriptions, restrictions). For items that are touched by a large number of intermediaries, the likelihood of forgery or error increases, making blockchain ledgers a compelling solution given the demand for authenticity of 'premium' goods.

An aspect of provenance is "chain of custody," from the Latin *custodia*, to hold possession of and exercise duty of care control over something. Chain of custody applies to people (e.g., children, individuals held by law enforcement) or items (e.g., property, physical evidence), and the "how, when, and why" of authorities that "hold" people or items. Of particular importance is the conditions of the hold, from wence someone or something was received, and to whom someone or something was released. The guarantee is that the thing in question was not tampered with along the way, even if changes are expected like inventory markings or similar added at each step. Blockchain might be useful as a "keep track" utility, noting chain of custody.

6 Cost

The costs of an ecosystem can be substantial and difficult to forecast. Requisite technical and social innovations must come together, be debugged, and routinized. "Inevitability arguments" are of limited value. They suggest a need to move fast, but if something is inevitable, what's the rush? Assuming something *is* inevitable (and many things said to be inevitable have not happened), the discussion merely changes from whether to when. Even modest change, much less paradigm shifts, can be hard to predict accurately. Some enthusiastically predict a paradigm shift from cryptocurrency, but if people must abandon systems they have relied on for years, or adopt unknown or costly alternatives, such change is unlikely. The cost of blockchain will have much to do with its success.

Direct costs of blockchains include the cost of making the blocks, the underlying infrastructure of computers and data networks, and the cost of building and maintaining the blockchain. Some of these infrastructure costs have already been paid. Blockchain will add little marginal cost to these sunk costs. The cost of creating the blocks themselves can be substantial. Proof of work schemes, like that employed by Bitcoin, can require computationally-intensive work. Some "miners" use supercomputers, where a rule-of-thumb is that 2/3 of the electricity consumed goes to computation, and 1/3 is used to cool the heat generated by computation. Computationally-intensive facilities are often located where electricity is comparatively inexpensive. Some argue that blockchain is environmentally unfriendly due to electricity consumption. In time, less costly ways of providing proof for new blocks might be found. Until then, setting up a large blockchain can be costly.

All keep-track schemes have substantial indirect or overhead costs. The cash fiat money system, for example, includes the production and distribution of currency, recovery from circulation, secure disposal, control institutions, accounting, suppression of counterfeit, etc. Blockchain overhead is incurred every time a blockchain is updated. If blockchain survives, existing blockchain systems must be "ported" to replacement infrastructure. No one has yet proved that cryptocurrency has costs lower than alternatives. The cost would have to be substantially lower (i.e., very attractive) to overcome the advantages of incumbency.

Expectation failures add costs. If a blockchain turns out to require a central authority, the cost associated with creating or involving that central authority must be added. Similar issues can arise regarding block size, now typically set at around 1 megabyte. Changing block size might require retroactively updating existing blockchains and building all new blockchains to correspond. Or the cost of preparing for a predicted need might be moot, as with Internet Protocol Version 6 (IPv6). IPv6 was created in part to deal with predicted shortage of IP addresses. Dynamic IP addressing delayed that problem and the high cost of moving to IPv6 caused most organizations to stay with the earlier protocol (IPv4). The Internet of Things might compel movement to IPv6 or something else. Even the best of plans and intentions can go awry, which leads to risk mitigation as in insurance. Most motor vehicle owners have insurance (many states require it). Most mortgage holders require homeowners to have fire insurance. Risk of failure in important blockchains might bring requirements for insurance or other risk mitigation. Who bears what liability is one of the many cost issues to be resolved. These are but some of the costs that might come from expectation failures.

7 A Research Agenda

Blockchain, like all technologies that affect humans, cannot be purely technical. If it is to have effect at all it is through a sociotechnical system. Most sociotechnical systems evolve over time. They cannot easily be designed and implemented. Cryptocurrency as a replacement for existing fiat money might not be a good predictor of the future of blockchain, but through learning-by-doing it does teach two lessons: that blockchain can be put to use in storing value, and that it might be used more significantly in smart contracting. It is important to see blockchain thus far as experimental. Much of our knowledge comes from learning-by-doing. While this is instructive, it is best to not mistake the domain of learning at the moment (e.g., cryptocurrency) for the long-run implications of the sociotechnical system that might evolve. Thus far blockchain is mostly in praxis. Technical research will continue, but information systems questions will focus on how sociotechnical systems involving blockchain evolve to address the needs of individuals, organizations, institutions and society. The general research model is shown in Fig. 1.

The question is what to look for. Learning-by-doing coming from experience fed by the sociotechnical systems concept provides a good start. It tells us whether the evolving sociotechnical system can be used for *something*. We also learn about analogies helpful in reasoning by analogy – learning about this thing indirectly by comparing it to something about which we know more (e.g., fiat money, contracting). These guide decisions to look further and about what to look for. Blockchain deserves a further look. Cryptocurrency is analogous to fiat money, but we do not think blockchain's future is as a replacement for fiat money. Smart contracting is emerging. Much is known about contracting. That is something to explore. Smart contracting suggests benefits from a relatively secure "keep-track" capability. We carry that insight forward.

Lexical analysis gathers what has been learned by people thinking through the evolving sociotechnical system. Learning-by-doing has taught about keep-track capability. Blockchain is described as a ledger that provides keep-track capability. Two areas of keep-track, provenance and chain-of-custody, seem promising. Historical analysis shows the importance of context in keeping track – even anthropology uses this. Blockchain experimentation with provenance and chain of custody has begun. Learning-by-doing knowledge should follow. Applications happen more quickly in well understood domains. Perhaps by using the legal world's understanding of contracting we can speed up learning-by-doing in smart contracting. Maybe blockchain can be used for smart contracts in insurance, financial instrument trading, and real estate transactions. But any area already automated might be hard to overcome because of path dependency or incumbent interests. Information-intensive transactions like loan syndication, or tasks tied to protocols, such as currency-agnostic cross-border payments with instant settlement, might be easier to penetrate. The most attractive domains for blockchain application are well-understood but heretofore unamenable to automation that are made more amenable by blockchain. Perhaps supply chain information management or project/startup funding – anything that requires keep-track.

Getting complementary assets identified and to scale requires learning-by-doing, which takes time. Timing is usually difficult to manage: some organizations (Pets.com and Freeshop.com) died before Amazon.com succeeded. Many failures might be required before a domain well enough understood for a victor to emerge. But some things are known. Central authority requirements can make experimentation less costly (standards) or more costly (legislation). If standards are not an issue, decentralized blockchain experimentation might be less costly. Some provenance and chain of custody applications do not require standards or other aspects of central authority. They might be ripe for learning by doing about the applicability of blockchain. Hold time and the number of transactions can affect cost. They interact: long hold-time can be offset by infrequent transactions (real property transactions without title searches – a notion that might be extended to artworks). Similarly, short hold-time might offset frequent transactions to warranty the genuineness of designer clothes and accessories, ensure the traits of

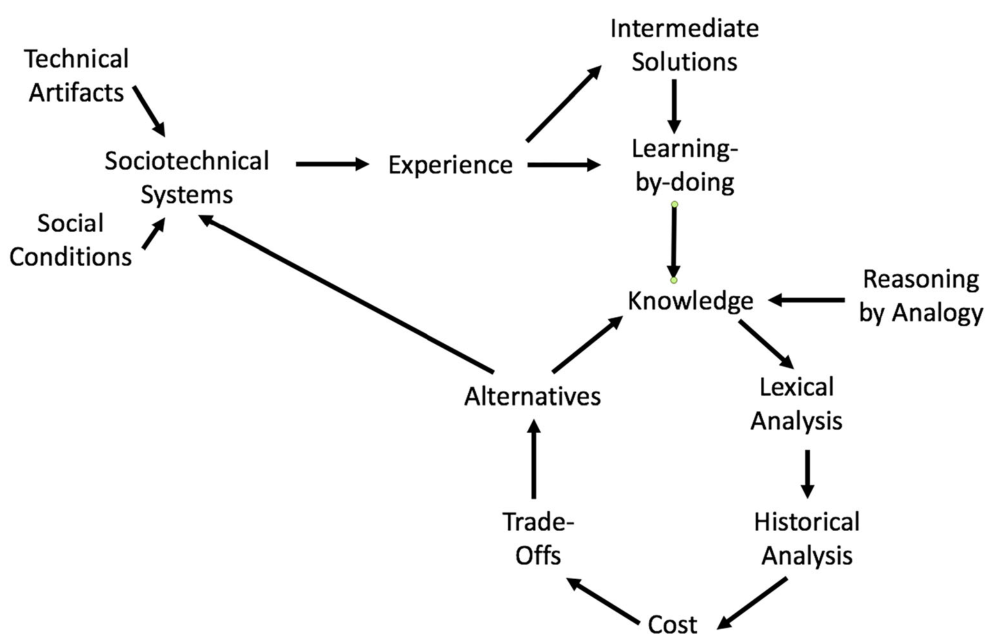

Fig. 1 General research model for blockchain

foodstuffs (organic, free range) and pharmaceuticals, or combat voting fraud.

Existing conditions might make blockchain implementation difficult. Anything with short hold-time and low transaction volume might already be automated. Motor vehicle records are a case in point given that each vehicle has a unique vehicle identification number that motor vehicle authority records systems use. Blockchain would have to undercut the costs of such systems before motor vehicle authorities would adopt it. Similarly, high transaction volume and long hold time might make even blockchain solutions prohibitively costly. The right mix of hold time and transaction volume can guide research on provenance and chain of custody blockchain applications. These trade-offs inform our sense of viable alternatives that affect our knowledge and the sociotechnical system. By implication, they affect experience and learning-by-doing, and provide intermediate solutions that might evolve into widely-used solutions.

8 Conclusion

Blockchain might be a breakthrough, but the evidence so far is more suggestive than convincing. "This changes everything" developments sometimes fail. Enthusiasm for blockchain requires looking *beyond* the mass-market vision of cryptocurrency. The excitement of cryptocurrency is akin to a dog walking on its hind legs. Samuel Johnson's observation comes to mind: the surprise is not that the dog does it well, but that it does it at all. Cryptocurrency shows that blockchain can be used, but predicting blockchain's value requires looking beyond the foreground.

Acknowledgements The authors thank Roman Beck, Roger Ehrenberg, David Kobrosky, and Victoria Lemieux for their help.

References

Arrow, K. J. (1962). The economic implications of learning by doing. *Review of Economic Studies, 29*(3), 155–173.

Beck, R. (2018). Beyond bitcoin: The rise of Blockchain world. *Computer, 51*(2), 54–58.

Beck, R., Avital, M., Rossi, M., & Thatcher, J. (2017). Blockchain technology in business and information systems research. *Business & Information Systems Engineering, 59*(6), 381–384.

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the Blockchain economy: A framework and research agenda. *Journal of the Association of Information Systems, 19*(10), 1020–1034.

Bragina, A. (2018) All-in-one e-commerce fraud guide: types, detection, prevention. *AmastyBlog*, Mar 15, https://amasty.com/blog/all-in-one-e-commerce-fraud-guide-types-detection-prevention-2018/ . Accessed 15 Jul 2019

Buterin, V. (2017) The meaning of decentralization. The Medium, February 6, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 . Accessed 15 Jul 2019

Cao, S. (2018) Ethereum Creator vitalik buterin explains what you really need to know about Blockchain. *The Observer*, December 14 https://observer.com/2018/12/ethereum-creator-vitalik-buterin-blockchain-uses-beyond-bitcoin/ . Accessed 15 Jul 2019

Desjardins, J. (2017) All of the World's money and markets in one visualization. The Money Project, October 26, http://money.visualcapitalist.com/worlds-money-markets-one-visualization-2017/ . Accessed 15 Jul 2019

Dewey, J. (1897). My pedagogic creed. *School Journal, 54*, 77–80.

Dewey, J. (1938). *Experience and education*. New York, Kappa Delta Pi.

ICODATA.IO (2019) ICO status, https://www.icodata.io/stats/ . Accessed 15 Jul 2019

King, J. L. (1983). Centralized vs. decentralized computing: Organizational considerations and management options. *ACM Computing Surveys, 15*(4), 319–345.

Lemieux, V., D. Hofman, D. Batista, and A. Joo, (2019) *Blockchain technology and recordkeeping*. ARMA, May 30, http://armaedfoundation.org/wp-content/uploads/2019/06/AIEF-Research-Paper-Blockchain-Technology-Recordkeeping.pdf . Accessed 15 Jul 2019

Marr, B. (2017) A complete beginner's guide to Blockchain. Forbes, January 24, https://www.forbes.com/sites/bernardmarr/2017/01/24/a-complete-beginners-guide-to-blockchain/#311432c16e60 . Accessed 15 Jul 2019

Popper, N. (2019). After the bust, are bitcoins more like tulip mania or the internet? *New York Times, 23*, 2019 https://www.nytimes.com/2019/04/23/technology/bitcoin-tulip-mania-internet.html . Accessed 15 Jul 2019

Riseshine, J. (2019). Ripple is the only token issuer to beat SWIFT to the emerging market. *Today's Gazette*, June 1, 2019. https://todaysgazette.com/ripple-is-the-only-token-issuer-to-beat-swift-to-the-emerging-market/ . Accessed 15 Jul 2019

Rushe, D. (2015) Nasdaq reaches new record high, 15 years after dotcom tech surge. *The Guardian*, April 23 https://www.theguardian.com/business/2015/apr/23/nasdaq-new-record-high-dotcom-bubble . Accessed 15 Jul 2019

Ryu, C., Kim, Y. J., Chaudhury, A., & Rao, H. R. (2005). Knowledge acquisition via three learning processes in Enterprise information portals: Learning-by-investment, learning-by-doing, and learning-from-others. *MIS Quarterly, 29*(2), 245–278.

Takahashi, E. (2019) Cryptocurrency thefts, scams, and fraud top $1.2 billion in Q1 2019. *Venturebeat*, April 30, 2019, https://venturebeat.com/2019/04/30/cryptocurrency-thefts-scams-and-fraud-top-1-2-billion-in-q1/ . Accessed 15 Jul 2019

Werbach, K. (2019). People don't trust blockchain systems – is regulation a way to help? *The Conversation*, February 5, http://theconversation.com/people-dont-trust-blockchain-systems-is-regulation-a-way-to-help-110007 . Accessed 15 Jul 2019

XBT Network (2018). What is bitcoin 2.0? *XBT Network*, Jul 17, https://xbt.net/blog/bitcoin-blog/what-is-bitcoin-2-0/ . Accessed 15 Jul 2019

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Andrew Ehrenberg is a recent graduate from the University of Michigan School of Information and Ross School of Business. He has worked in financial technology and related fields as an analyst and researcher in New York City and Boston and plans to return to Michigan to pursue a Masters in Applied Data Science.

John Leslie King is W.W. Bishop Collegiate Professor in the University of Michigan School of Information. He studies the relationship between technical and social change. He was 20 years on the faculties of information and computer science and management at U.C. Irvine before joining Michigan in 2000.