What's Next in Blockchain Research? – An Identification of Key Topics Using a Multidisciplinary Perspective

Horst Treiblmaier, Melanie Swan, Primavera de Filippi, Mary Lacity, Thomas Hardjono, Henry Kim

The Data Base for Advances in Information Systems

What's Next in Blockchain Research? – An Identification of Key Topics Using a Multidisciplinary Perspective

Horst Treiblmaier
horst.treiblmaier@modul.ac.at
Melanie Swan
melanie@blockchainstudies.org
Primavera de Filippi
pdefilippi@cyber.harvard.edu
Mary Lacity
MLacity@walton.uark.edu
Thomas Hardjono
hardjono@mit.edu
Henry Kim
hkim@schulich.yorku.ca

Date of Acceptance: 6/23/2020

Please cite this article as follows:
Treiblmaier, H., Swan, M., Filippi, P., Lacity, M., Hardjono, T., Kim, H. (Forthcoming). What's Next in Blockchain Research? – An Identification of Key Topics Using a Multidisciplinary Perspective. *The Data Base for Advances in Information Systems*, In Press.

What's Next in Blockchain Research? – An Identification of Key Topics Using a Multidisciplinary Perspective

Horst Treiblmaier
Modul University Vienna

Melanie Swan
Purdue University

Primavera de Filippi
National Center of Scientific Research (CNRS)
Berkman-Klein Center | Harvard University

Mary Lacity
University of Arkansas

Thomas Hardjono
Massachusetts Institute of Technology, MIT

Henry Kim
York University

Abstract

Distributed ledger technology, frequently designated as "blockchain," is evolving from its hype phase toward greater maturity and long-term value creation. Although many academic communities were initially slow to grasp the technology's numerous potential implications, meanwhile a substantial amount of research is dedicated to investigating the development and impact of blockchain and related technologies. As undertaken, most research projects take a specific homogenous perspective, such as a technical or business viewpoint. To date, blockchain research studies are largely missing a bridge between and across academic disciplines. Given the manifold implications of blockchain technology, a fruitful cross-disciplinary exchange is therefore needed. In this paper, we bring together researchers with varying expertise to provide a vision into what may be next in terms of concepts, applications, and research agendas. We consider business, economic, societal, legal, technical, and philosophical viewpoints and propose multiple research questions as well as hypotheses arising from these diverse viewpoints. Simultaneously, we challenge various academic communities to tackle some of the most crucial issues of current blockchain research and to develop a solid foundation for future exploration.

Keywords: Blockchain; Distributed Ledger Technology; Technological Impact, Technological Change; Multidisciplinary Research.

Introduction

Modern technology can have surprising and unintended side-effects that a multidisciplinary approach might help to identify and investigate. The Internet, for example, initially conceived as a communication means for the military and academia, turned out to be a major game changer for business relationships (Bunduchi, 2005), governmental and social structures (Bavec, 2006), and human lifestyle in general (Närvänen et al., 2013). The World Wide Web (WWW) led to the emergence of new transaction and communication patterns as well as novel social relationships. Many of the Internet-induced changes have had a substantial positive effect on human lives by increasing economic welfare and personal well-being (Castellacci & Tveito, 2018; Lapatinas, 2019), but simultaneously resulted in unintended side effects, such as loss of privacy, increased cybercrime, and addictive behavior (Broadhead, 2018; McNicol & Thorsteinsson, 2017; Meeks, 1997). Early research on the Internet mainly focused (narrowly!) on technical issues needed to establish a reliable and scalable transfer of data in the form of bits and bytes. As soon as the major technical problems were solved and the technology was embraced by public institutions, industry and the general public, transaction and communication patterns changed drastically. Concurrent with the permeation of the Internet through our professional and private lives, numerous academic communities started investigating its impact from different viewpoints, which included almost every business-related community, such as information systems, marketing, management, logistics or finance, but also economics, sociology, psychology, legal sciences and philosophy. While each researcher investigated the novel technology and its implications from his/her respective viewpoint, over time a substantial amount of research has accumulated that fosters an understanding of the Internet from these specialized perspectives.

In recent years, blockchain evolution has mimicked the history of the Internet. The seminal technological developments that constitute the technological foundation of blockchain, such as linked timestamping, verifiable logs, proof-of-work, fault tolerance, asymmetric cryptography and smart contracts, all took place in the decades preceding the emergence of the first online blockchain (Narayanan & Clark, 2017). The initial description of Bitcoin as a fully functioning blockchain on the Internet was published in 2008 (Nakamoto, 2008), followed by the implementation of the first client in 2009. From that point, several years passed before the technology gained widespread public recognition (Iansiti & Lakhani, 2017; Swan, 2015; Tapscott & Tapscott, 2016). The debate around Bitcoin and blockchain was soon dominated by discussions of applications which could deliver a wide variety of use cases with desirable goals such as food safety, better labor conditions, financial inclusion, better healthcare and direct democracy (Larios-Hernández, 2017; McDonald, 2017; Susskind, 2017; Treiblmaier 2019; Stafford and Treiblmaier, 2020), but also included the possibility of nefarious uses such as money laundering and drug trafficking (Engle, 2018; van Wegberg et al., 2018). Unintended side effects of blockchain technology included both positive

developments – such as the development of more efficient yet highly specialized hardware (i.e., ASICS), and advances in cryptography – and negative consequences – such the huge amount of energy needed for the proof-of-work algorithms applied in public and permissionless blockchains (Kugler, 2018) and threats to privacy (Feng et al., 2019).

Given the complexity of blockchain technology, which is still under development, our goal is to create awareness for the multiple implications of blockchain technologies, as well as to point the academic community toward exciting and novel research avenues. Multidisciplinary research builds bridges between otherwise disparate academic disciplines to avoid the tunnel vision which can result from solely relying on a narrow set of theories, methods or epistemological approaches (Treiblmaier, 2018a). Blockchain is neither an exclusively technological phenomenon nor solely an economic, philosophical, social, legal or business one. Rather, it is of relevance to all of these areas simultaneously, and probably to many more. For example, introducing a new technical feature on blockchain might at the same time open up a plethora of economic, social or legal opportunities and threats, such that well-coordinated multidisciplinary research projects are necessary to properly explain, explore and predict the wide-ranging ramifications of said technological change.

The technical underpinning of blockchain as well as its history has been outlined in numerous academic publications and shall not be discussed in detail here. Several definitions of the concept exist. Treiblmaier (2018b, S. 547), for example, defines *blockchain* as “a digital, decentralized and distributed ledger in which transactions are logged and added in chronological order with the goal of creating permanent and tamper-proof records”. According to Lacity (2018a, S. 41) a *blockchain application* is a “distributed, peer-to-peer system for validating, time-stamping, and permanently storing transactions on a distributed ledger that uses cryptography to authenticate digital asset ownership and asset authenticity, and consensus algorithms to add validated transactions to the ledger and to ensure the ongoing integrity of the ledger’s complete history”. Finally, the umbrella term *distributed ledger* denotes “a type of database that is spread across multiple sites, countries or institutions, and is typically public. Records are stored one after the other in a continuous ledger, rather than sorted into blocks, but they can only be added when the participants reach a quorum” (Government Office for Science, 2016, S. 17). Three types of blockchain exist, which differ according to the ability of the participants to read, write and verify transactions. *Permissionless public blockchains* allow all users to read, write and verify transactions; Bitcoin (launched in 2009) and Ethereum (launched in 2015) are two examples. In *permissioned private blockchains* only authorized users can do so; the IBM Food Trust, TradeLens, and WeTrade (all launched since 2018) are examples. In between the two lie *permissioned public blockchains*, in which all participants can view the stored data, but only authorized nodes are able to validate transactions (Pedersen et al., 2019); Ripple, launched in 2012, is an example. It is worth mentioning that the underlying structure of distributed ledgers does not necessarily need to be chain-like. Alternative approaches propose directed acyclic graphs (DAG) which entangle a stream of individual transactions. The main advantage of avoiding a linear blockchain lies mainly in the faster processing of transactions (Kauflin, 2018). Frequently, the term blockchain is used when in fact distributed ledger would be more appropriate. In this paper we follow this practice and mainly refer to blockchains independent of the underlying data structure.

An ancient Indian metaphor tells about the perceptions of a number of blind men, who each touch an elephant in order to gain an understanding of what it is like. Depending on the respective body parts they touch, they obviously come up with different conclusions. This metaphor has been applied to academic research to highlight the dependency of an outcome on the underlying mindset, knowledge and theory repository, as well as researchers’ personal interests. The hexagon in Figure 1 figuratively transforms the elephant into blockchain and the blind men into six disciplines – business, economics, sociology, law, technology (e.g., computer science and cryptography) and philosophy – all of which are equipped with idiosyncratic research interests and their respective methodological and epistemological knowledge. The economic perspective, as we discuss it in this paper, mainly pertains to macroeconomic issues, namely the behavior of market systems on a large scale.

Insert Figure 1 About Here

We posit that the full range of blockchain implications and also its unintended side effects can only be captured by adopting a multidisciplinary perspective. For example, smart contracts for business transactions not only pose a *technical* problem, but also involve the consideration of complex *legal* frameworks which need to be adapted to deal with the storage of immutable information. Moreover, smart contracts also touch on the *philosophy* of libertarianism and free markets (Cornelius, 2018). Decentralized systems can trigger substantial *economic* change which in turn might impact *societal* structures by allowing for new ways of governance (Voshmgir, 2017) or creating new forms of work (Treiblmaier & Umlauff, 2019). As another example, a philosophy of blockchain as a conceptual resource can help to better understand the progression caused by this technology (Swan & Filippi, 2017). In the following sections, we thus elaborate on the capabilities of blockchain technologies from various perspectives. Without any claim to completeness, via this analysis (which our readers can liken to the summary of a multi-disciplinary discussion panel) we raise potential research questions (RQs) – numbered 1 through 35 – and derive hypotheses (Hs) – numbered 1 through 7 – we deem to be important, simultaneously striving to highlight interdependencies between research areas.

The Business Perspective: Disrupting Organizational Structures, Processes and Information Flows

Viewing blockchain from a business perspective reveals numerous research opportunities, two of which we examine here, within the business perspective. First, we suggest investigating organizational transformation through an innovation lens. Second, we elaborate on information asymmetry and the coupling of a company's operational and financing system via blockchain to mitigate adverse selection and moral hazard.

The Transformative Power of Innovation

Although business scholars already have a broad blockchain research agenda which cannot be fully covered here, the reexamination of the very nature and boundaries of the firm is perhaps the most fundamental. "Why do firms exist?" is a question dating back to the 1930s (Coase, 1937). Transaction Cost Economics (TCE), one of the most widely appropriated theories in business, has two underlying assumptions: opportunism (one firm cannot trust other firms in the market) and bounded rationality (a firm cannot know everything nor exhaustively explore every option) (Williamson, 1975, 1991b). Where possible, counter-party risks are mediated with trusted third parties, which adds transaction costs. According to TCE, firms exist because market trust cannot always be efficiently established with contracts, such as under conditions of high uncertainty and high asset specificity (Williamson, 1975, 1991a, 1991b). *Blockchains have the potential to dramatically alter the boundaries of the firm.* Bitcoin's raison d'être was to replace the truth attestations performed by financial institutions with computer algorithms and cryptography (Nakamoto, 2008). Blockchains can prove asset ownership with digital signatures and prevent the double-spend problem (i.e., the spending of a digital token more than once) by maintaining a full history of sequenced transactions. Consequently, enterprises in the financial services sector have been among the first businesses to recognize the threats and opportunities afforded by Bitcoin because their revenues models are under threat (Lacity, 2020). According to McKinsey, the world sends more than $135 trillion across borders each year (McKinsey, 2016). Third-party intermediaries collect about $2.2 trillion in revenue to facilitate these transactions. Consequently, incumbent enterprises, including banks like Barclays, State Street, and Wells Fargo that have been in continuous operation for hundreds of years, are among the early firm explorers of blockchain technologies.

Will incumbent enterprises like these financial institutions succeed? Blockchains – which financial institutions might view as disruptive innovation – provide a rich context to test some of business's most revered theories, such as the Theory of Disruptive Innovation (Christensen, 1997; Christensen et al., 2015). According to this theory, incumbent firms will likely pursue *sustaining* innovations rather than *disruptive* innovations. Sustaining innovations improve today's products and services for an incumbent's most demanding and most profitable customers. It is unlikely that

incumbent firms will cannibalize their revenues to embrace a disruptive innovation, described by Christensen et al. (2015) as a process by which a new innovation takes root at the bottom of the market for the least sophisticated customers, but then rapidly improves to eventually overtake incumbents. The Theory of Disruptive Innovation suggests that many blockchain innovations will likely come from nimble startups because they have no legacy barriers. Over 250 FinTechs such as Axoni, BitPesa, and Digital Asset Holdings, have already entered the blockchain space (CBInsights, 2019) and more than 4,800 blockchain startups exist as of July 2020 (Angel.co, 2020). According to market experience, the majority of startups will likely fail due to the inherent risks (Griffith, 2017). Because there are so many failures, incumbents have a hard time monitoring the promising innovations, until it is too late to respond.

Insert Table 1 About Here

The Theory of Disruptive Innovation may or may not hold up in the context of blockchain technologies, because blockchains are shared applications across firms, with no one firm controlling the application, as opposed to applications adopted within the boundaries of a single firm. We may even need a whole new theory of ecosystem innovations, where innovations happen at the ecosystem level rather than firm level by involving partners, customers, suppliers and competitors (Jacobides et al., 2018). In Table 1 we juxtapose sustaining innovations, disruptive innovations and ecosystem innovations, according to their strategic intent and locus of control. To give an example of an ecosystem innovation, industry consortia like R3, founded in 2014, were started to help incumbent enterprises create standards, write code bases, and bring blockchain financial services applications to life. These enterprises have developed numerous proof-of-concepts (POCs) for many financial services including but not limited to Anti Money Laundering (AML), betting & prediction markets, bond issuance, collateral management, compliance reporting, commodities pricing and cross-border payments. Despite the promised business value, enterprise adoptions have been slower than initially anticipated and most of these POCs will never be developed into production systems (Gupta, 2018). While hundreds of press announcements on enterprise proof-of-concepts and pilots have been announced, few enterprise blockchains have deployed—let alone scaled—as of mid-2020. We thus suggest our first hypothesis:

> Hypothesis 1 (H1)*:* When it comes to blockchain innovation, incumbent firms will likely pursue sustaining innovations rather than disruptive innovations.

As an ecosystem, any blockchain application that is launched into production faces an imposing challenge of attracting additional users. Metcalfe's law states that the value of a network is proportional to the square of the number of connected users in the system (Metcalfe, 2013). The question arises of how the founders of an innovation might attract additional adopters. In this regard, the Theory of Institutional Isomorphism might provide fresh insights. It models the process of homogenization among organizations facing similar environmental conditions (Mizruchi & Fein, 1999). Essentially, the theory seeks to answer the question: Why do organizations within an industry eventually change to become more alike? DiMaggio and Powell (1991) posited that organizations eventually adopt similar structures, processes, philosophies, practices, and technologies through three mechanisms of influence - coercive, normative and mimetic - ultimately leading to institutional conformity within an industry.

Coercive influences come from political pressures exerted on an organization by other organizations upon which they are dependent. Government regulations, legal requirements, and powerful trading partners' mandates are examples of coercive influences. Within the context of blockchains, for example, Walmart required that its loose-leaf lettuce providers adopt the IBM Food Trust blockchain by September 2019.

Normative influences arise from duties, obligations, and norms of professionalism, including formal education as well as professional and trade associations that seek to legitimize their existence (DiMaggio & Powell, 1991). In the context of blockchains, we see that powerful advisory firms—those companies that have built considerable blockchain services—influence their client's blockchain adoptions. While advisory firms seek to be technology

neutral, they will have insights as to which applications are the most enterprise-ready and the most context-suitable, thereby moving a sector toward adopting a winning application.

Mimetic influences arise from the perception that peer organizations are more successful; by mimicking peer behavior, the organization aims to achieve similar results. Mimetic influences are particularly strong when environmental uncertainty is high, goals are ambiguous, and when technologies are poorly understood (Mizruchi & Fein, 1999). IBM's strategy to attract "anchor tenants" like Maersk and Walmart for its major blockchain applications can be considered a mimetic influence (Wieck, 2017).

From the business innovation perspective, blockchains are prompting research inquiries for all business disciplines, including strategic management, accounting, supply chain, information systems, finance and marketing. In Table 2 we list the respective disciplines and related research questions (RQs).

Insert Table 2 About Here

Information Asymmetry Perspective on Blockchain

The core premise of blockchain is straightforward: rather than relying upon a trusted intermediary to proprietarily maintain one ledger of transactions between members of a network, all members maintain their own copies of the same ledger and ensure that the copies are all synchronized. This maintained synchronization of multiple ledgers obviates the need for the intermediary, who often exploits its information asymmetry advantage to act in self-interested and extractive, inefficient, or corrupt ways. Information asymmetry refers to a situation in which one party to a transaction or contractual obligation has more information than the other party or knows more about the other on a relative basis (Akerlof, 1970). Two phenomena may result because of this asymmetry (Eisenhardt, 1989). The first is adverse selection: one party makes a poor selection when it decides to engage in a transaction because it has limited awareness of the other party's shortcomings. The second is moral hazard: one party engages in risky behavior because the rewards of such behavior far outweigh the penalties. The other party is obligated to indemnify and moderate the penalties on the risk-taking party. To allay concerns about information asymmetry, trusted intermediaries and institutions arose to govern and use information about two parties in a trustworthy way, so that neither party would be able to take advantage of the other (North, 1991). The rationale for blockchain is that in many situations intermediaries exploit their information asymmetry advantages against both parties they were supposed to serve.

However, if these third-party intermediaries are disintermediated using blockchain technologies, then two parties to a transaction are left to deal with information asymmetry on their own, while the transparency provided by using blockchain promises to provide symmetric information. Business examples illustrating this situation include back-end processes in finance and provenance tracking along a value chain – two of the most popular and frequently implemented blockchain use cases. It also works elegantly in the operation of the Bitcoin and Ethereum networks.

In another very popular use case, however, the Initial Coin Offering (ICO) of a new cryptocurrency, blockchain does NOT mitigate information asymmetry. An asymmetry exists about what the investor knows about the issuer of the cryptocurrency and, more importantly, what the issuer will do with the proceeds of the ICO rather than what they claim that they would do. This inability or unwillingness to provide transparency to the operations of the issuer has *been problematic: many investors have bought cryptocurrencies whose issuers blatantly took the proceeds and* disappeared, leading to the emergence of a more strongly regulated environment as is the case with STOs (Security Token Offering) and IEOs (Initial Exchange Offering). Here we identify a significant research opportunity for design science research:

Research Question 13 (RQ13): How can a blockchain for financing and a blockchain for operations (e.g., provenance tracking) be designed and tightly coupled in order to simultaneously mitigate adverse selection and moral hazard?

Investors worry less if a smart contract on a blockchain can be attached to their investment in a company such that undesirable behavior or failure to meet milestones can be compensated for in their investment (e.g., a rebate) in a timely manner. If the company knows that its actions can be tracked on a blockchain and are subject to timely automated penalties, then it is not incentivized to engage in risky behavior because rewards for its behavior do not outweigh potential penalties. The precept for the proposed research program then is this:

Hypothesis 2 (H2)*:* By coupling a blockchain for operations that recognizes and penalizes moral hazard behavior with a blockchain for financing that offers contingent actions to lessen the effect of adverse selection, heightened productivity and effective allocation of resources are possible.

There is some thought that security tokens could serve the purpose suggested by H2. Blockchain-based investment instruments exist that possess some characteristics of securities like enforcement of KYC/AML (Know Your Customer/Anti-Money Laundering), requirement for investor identification, as well as benefiting from price appreciation and ability to receive dividends. However, security tokens do not generally enable token holders to own a share of the company. That is why regulators in Ontario Canada, for example, have publicly stated their willingness to develop a regulatory framework for security tokens (Boring & Kim, 2018), Canada along with most countries do not allow ICOs that do not offer similar regulatory oversight or investor protection. We posit that there may be an opportunity to marry the research, industry, and entrepreneurial opportunities in security tokens. Specifically, different blockchain and smart contracts technologies will need to be designed and analyzed such that tightly coupling blockchain-based operations and blockchain-based financing will reduce information asymmetry, and will lead to improved operations and more efficient allocation of capital. A promising example is a Canadian startup (Grain Discovery, 2020), which uses blockchain to couple an online marketplace for wholesalers to purchase grains from individual farms with a traceability system to assure provenance of the grains. Figure 2 shows how different initiatives can fit in with the proposed program's precepts. It illustrates the interplay between the operational and the financing systems before (upper part) and after (lower part) the introduction of blockchain. More specifically, the following areas of interest are identified: (a) semantic and data interoperability between operations-focused and financing-focused blockchains, (b) consensus mechanisms for blockchain interoperability, (c) agent-based modeling of integrated operations and financing blockchains, (d) refinement of a domain-independent traceability ontology for provenance checking across a value, and (e) smart contracts for investment instruments that are consistent with the research precept. Table 3 lists specific research questions and the corresponding methods following projects related to (a) - (e) annotated in Figure 2.

Insert Figure 2 About Here

Insert Table 3 About Here

The Economic Perspective: Transforming Markets, Trade and Money

Nakamoto's (2008) seminal blockchain paper was predominately a technical one, but he left a message in the genesis block of the Bitcoin chain that might indicate a more broader reaching motivation for blockchains.

Specifically, the message “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks” can be interpreted as the desire to enable peer-to-peer transactions and bypass financial intermediaries. Blockchains thus were conceived to also have a transformative impact on the conceptualization and execution of economics and finance. Many problems faced by both capital markets and goods markets are forms of liquidity problems in the sense of getting supply and demand to meet and coordinating available resources to respond to demand:

- In capital markets, there are liquidity problems related to credit extension and retraction, and the ability to manage risk, particularly as heightened in volatile conditions. Tokenized asset registries and black swan selectable risk preference contracts are mechanisms that might serve to diminish systemic risk by providing a quickly aggregated picture of overall financial risk in real-time, an information metric which has not been available previously and could reduce the fear of the unknown with information (Swan, 2019a).
- In goods markets (global value networks), three liquidity problems exist: first, the findability and fungibility of goods (a human-machine collaboration problem), second, the cost of attribute discovery (an information theoretic search problem), and third, the ease of contracting between buyers and sellers (a digital asset contracting and recourse financing problem), all of which might be ameliorated with blockchain-based models (Swan, 2019b).

The possible result of a widespread implementation of blockchain economic models is that higher levels of privacy-protected transparency and greater network connectivity might significantly increase liquidity and diminish the friction and cost of interaction and demand fulfillment. Liquidity could improve as a side benefit due to the reduced friction of financial transfer as organizations migrate toward blockchain-based shared business processes (all parties using the same business processes and ledger system with privacy-protected views) (Swan, 2017) and integrated blockchain supply chain ledgers (Swan, 2018). We therefore suggest the following hypotheses:

> Hypothesis 3 (H3)*:* Blockchains will increase liquidity in capital markets due to the quicker and more transparent availability of information concerning aggregate market conditions
>
> Hypothesis 4 (H4)*:* Blockchains will increase liquidity in goods markets and global value networks due to the ability for supply and demand to meet more effectively through shared business process infrastructure

The transformation of capital markets will inevitably impact its main stakeholders, most notably banks, who, amongst other roles, serve as intermediaries between investors and borrowers, help to smooth risks and create money by granting loans. It is especially the latter function of banks that has raised questions pertaining to the sustainability of our financial system and the role that cryptocurrencies can play to stabilize it (Leonard & Treiblmaier, 2019). When it comes to its impact on the banking sector, blockchain can either be seen as a technology or a governance mechanism. In the former view some banks will adapt and benefit while others will lag behind and fail. The latter perspective predicts fundamental shifts of organizational boundaries that renders many of the current functions executed by hierarchical banking institutions as unnecessary (MacDonald et al., 2016). This perspective can be easily illustrated by the example of Bitcoin, which allows for transactions between peers and skips powerful intermediaries. This leads us to a central research question which combines financial power and novel governance structures:

> Research Question 20 (RQ20): What is the future role of the financial sector in a decentralized economy?

The previously discussed TCE, Theory of Disruptive Innovation, and Theory of Institutional Isomorphism are just three examples of theories at the intersection of business and economics which can explain blockchain’s potential impact on the economy as a whole and may or may not be corroborated with empirical findings. Additionally, blockchains provide an academic treasure trove for putting our most reified theories residing at the intersection of business and economics to test. A comprehensive new institutional economics perspective can be applied to answer questions pertaining to the structure and management of a blockchain-based system. More specifically, TCE and Principal-Agent Theory can be used to investigate the structure of a system, while Network Theory (NT) and the resource-based view (RBV) of the firm can help to generate some insight into how to manage a specific structure (Halldorssón et al., 2007). Berg, Davidson & Potts (2019) take the next step and introduce a new type of corporate

structure, the outsourced vertically integrated firm (V-form organization) which is built around a supply chain that is managed by distributed ledgers. The core characteristic of this kind of organization is its vertical integration which is outsourced to a blockchain. This premise extends the idea of virtual organizations as temporary networks of independent companies without any hierarchy or vertical integration. When applying these theories to blockchain-based transformations, two specific research questions can be asked (Treiblmaier, 2018b):

Research Question 21 (RQ21): How to structure a value network that incorporates blockchain?

Research Question 22 (RQ22): How to manage a value network that incorporates blockchain?

The Social Perspective: New Forms of Governance and Order

Nakomoto's previously referenced message in the Bitcoin genesis block addressing the financial bailout is commonly seen as a political statement opposing government paternalism. Being a distributed system by nature, blockchain evokes ideas of disintermediation that go far beyond technical systems. Consequently, blockchain not only has the potential to change governance and societal structures in existing nation states, but also to create voluntary associations such as Bitnation, a decentralized borderless voluntary nation based on blockchain (Sullivan & Burger, 2017). Voshmgir (2017) critically investigates the gap between the initial conceptualizations of blockchains and their first implementations and concludes that "future research must turn its attention to a series of important questions around governance [including] information dissemination, communication and transparency, and new forms of principal-agent problems and power concentration" (p. 508). The topic of governance in the context of blockchain technologies is explored in some detail by Beck, Müller-Bloch & King (2018) who present an extended IT governance framework that juxtaposes the blockchain economy and the digital economy along the governance areas of decision rights, accountability and incentives. They derive several research questions that address these areas and suggest, amongst others, that future research undertakings investigate how decision rights are allocated in the blockchain economy, how accountability is determined in this context, and what role is played by technical and institutional accountability, as well as exploring the role of incentives in the blockchain economy. Summarizing, the interplay of blockchain and governance deserves further attention:

Research Question 23 (RQ23): How does blockchain impact existing governance structures?

A recurring theme in social and economic research is the so-called tragedy of the commons, which denotes the depletion of shared resources (Hardin, 1968). Elinor Ostrom, the 2009 winner of the Nobel memorial prize in economic sciences, spent several decades studying how such a situation can be avoided by the consideration of eight principles: 1) the drawing of clear boundaries, 2) the adaptation of rules to local needs and conditions, 3) the involvement of those affected by the rules, 4) the acknowledgement of the rules by outside authorities, 5) monitoring systems, 6) graduated sanctions, 7) mechanisms for dispute resolution, and 8) responsibility in nested tiers (Ostrom, 1990). Based on her work, Rozas, Tenorio-Fornés, Díaz-Molina, & Hassan (2018) developed a framework that matches affordances of blockchain technologies (i.e., tokenization, self-enforcement and formalization, autonomous automatization, decentralization of power over infrastructure, transparentization, codification of trust) with Ostrom's principles. Their research shows that blockchain technologies exhibit properties that are useful for tackling challenging problems that would be impossible or hard to solve without distributed ledgers. Tokens, for example, can be used to clearly delimit community boundaries (which do not necessarily need to be restricted to a certain geographical location), and the self-enforcement and automatization of smart contracts can help to create congruence between rules and local conditions. Such an approach seems to comply with the conservative libertarian vision that views large centralized institutional systems as inherently flawed, and somewhat ironically, also seems in line with a communitarian anarchist viewpoint that advocates non-hierarchical and solidarity-based systems for people to achieve emancipation (Scott, 2016). Empirical research is therefore needed to investigate the relationship of blockchain and the transformation of governance structures:

Research Question 24 (RQ24): How can blockchain help to govern the commons?

At a national level, Dahrendorf (1996) explores the dilemma of what he calls “squaring the circle” of wealth creation, social cohesion and political freedom in OECD countries. He developed proposals to remedy this situation, several of which might benefit from a blockchain solution. These proposals include the changing nature of work, the provision of generalized social service, and decentralized power structures. More specifically, he elaborated that “it is possible to counteract the simultaneous pressures towards individualization and centralization by a new emphasis on local power” (p. 247). Blockchain technologies might provide the means to establish these local power structures. We therefore suggest investigating the following inquiry:

Research Question 25 (RQ25): Can blockchain be applied on a national level to ensure local power?

In concert, these examples illustrate how social structure and order can be substantially altered by blockchain technologies. New boundaries and hierarchical orders might emerge that transcend existing political borders and yield a shift in economic power, perhaps even at the level of the commons. Supporters of conflicting political philosophies can find blockchain technologies appealing for very different reasons. Libertarians might be attracted by the opportunity to bypass central authority and ensure anonymity, while socialists might find them equally well-suited to enhancing socialist forms of governance by allowing for decentralized transparency and auditability (Huckle & White, 2016).

The Legal Perspective: From Lex Mercatoria Via Lex Informatica Toward Lex Cryptographica

During medieval times, domestic trade was regulated by customary laws that were specific to a kingdom. Advances in transportation infrastructures expanded the reach of trade beyond a single kingdom. Domestic rules could no longer apply, and a new set of principles was therefore established to regulate trade within and amongst kingdoms. These new principles were achieved by means of private ordering, as merchants themselves established the rules that would regulate different types of transactions. Over time, some of these customs and best practices became recognized as a customary body of law for international (and/or interregional) commerce. This evolution marked the advent of the so-called Lex Mercatoria (the law of merchants) (Connerty, 2014), best characterized in heuristic terms: Lex Mercatoria emerged organically from the interactions of merchants seeking to extend the reach and reduce the uncertainty of trade. It was not enforced by any sovereign authority or kingdom, as royal courts generally avoided cases involving international trade or simply refused to acknowledge the validity of foreign contractual deals. Hence, merchants developed their own courts to enforce their own legal frameworks rooted in the practical needs of structuring increasingly complex contractual deals. Merchant courts progressively emerged along the main trading routes, recognizing Lex Mercatoria as a universal set of rules that is applicable to everyone regardless of one’s geographical location. By definition, Lex Mercatoria was solely concerned with commercial dealings and related disputes. Thus, broader public considerations of justice and equity did not form part of the legal system. Lex Mercatoria is not just a historical relic. Today, merchants and ordinary consumers use modern lex mercatoria and/or customary law more so than at any time before (Toth, 2017).

With the advent of the Internet and digital technology, an alternative normative system emerged, as a particular set of rules spontaneously and independently elaborated by an international community of Internet operators. The information technology regime, in the form of technological capabilities and system design choices, effectively serves to draw boundaries and impose a normative set of rules on participant action-taking (for example, certain file formats are a de facto standard in collaboration applications). This system—sometimes referred to as *Lex Informatica* (Reidenberg, 1998), by analogy to Lex Mercatoria—is an ideal toolkit for the regulation of online transactions, since its normative power arises directly from the technical design of the network infrastructure, which is used as a complement (or a supplement) to contractual rules. Just like Lex Mercatoria, Lex Informatica ultimately relies on self-regulation: It is a system of customary rules and technical standards, elaborated by those who interact on the global Internet network. A long-standing example is the Improvement Protocol decision-making structure in open-source cryptographic software communities in which anyone can propose a change, the proposals are seen

and discussed by all in an open forum, and eventually there is a vote. A specific example is Bitcoin Improvement Protocols (BIP).

The Lex Informatica system operates transnationally, across borders, independent of national boundaries and domestic laws. However, as opposed to Lex Mercatoria, which was elaborated by and for an international community of merchants, in order to respond to their own needs, Lex Informatica is unilaterally imposed by online service providers onto their users. Indeed, by restricting the type of actions that can be performed on a digital platform, Lex Informatica introduces a system of technical norms which are not a direct expression of the will of the people, but rather of those in charge of maintaining the platform. While there is always a possibility for people to opt-out (vote with their feet), for many practical purposes, users are increasingly driven to 'consent' to specific terms and conditions, upon which they have no negotiation power.

Blockchain technology is enabling the emergence of yet another normative system, a new mechanism of coordination which also relies on technical means (blockchain protocols and technologies like so-called "smart contracts") in order to coordinate behavior. The benefit of this new normative system—sometimes referred to as *Lex Cryptographica* (De Filippi & Wright, 2018) —is the potential ability to operate independently of any third party authority or intermediary operator. However, the flipside is that blockchain-based rules do not have the flexibility required to manage a large majority of social interactions and commercial transactions. Hence, if such a system is to reach mainstream adoption, it is crucial to identify new mechanisms of conflict resolution capable of satisfying the basic requirements of transparency, accountability, accessibility, fairness and due process. For instance, TheDAO hack, in which an anonymous hacker exploited a vulnerability in the code of a smart contract to withdraw Ether, is an interesting example of how the Ethereum community had to come to a solution as to how to resolve an issue related to contractual liability by relying, only and exclusively, on internal mechanisms of coordination and community governance. Not only was TheDAO hack difficult to frame within an existing legal framework (was it a breach of contract? was it a theft? who had recourse against whom?), even if the dispute were to be brought to traditional judicial system, there would be no power of enforcement for the court order. Hence, the resolution of the dispute, and the enforcement thereof, had to be carried on via alternative mechanisms of deliberation (e.g., community discussion on online forums and a voting to assess the public opinion) and different ways of adjudication (e.g., soft-forks versus hard-forks) - which brought into light the governance challenges that the Ethereum community had to face, for lack of a formal mechanism of dispute resolution. This issue highlighted the need for the establishment of more formal mechanisms of private arbitration such as alternative dispute resolution (ADR) systems specifically designed for governing disputes between smart contracts and legal entities, or disputes between legal entities administered via a blockchain-based system (Allen et al., 2019). This brings forth our first legal research question:

> Research Question 26 (RQ26): How can alternative dispute resolution (ADR) systems be designed to govern disputes on blockchain?

In today's online space, a growing number of e-commerce transactions are not dealt managed by national courts, but rather via private arbitration mechanisms. This approach is not only more efficient and less costly than the traditional judicial system, but it also enables parties to choose the specific procedure and normative system for every potential dispute arising from an online interaction (e.g., eBay and Amazon both provide their own system of private arbitration, based on their own policy rules). Yet, private arbitration mechanisms are only possible because people rely on these trusted intermediaries (eBay or Amazon) who will be able to enforce the decision taken by the relevant agents. With smart contracts, the same becomes possible also in the context of a fully decentralized system, where there is no trusted authority mediating the transaction. Indeed, as opposed to traditional legal contracts, smart contracts are necessarily deterministic: all possible outcomes of the contract (including penalties for breach of contract) must be explicitly stipulated in advance —something akin to what liquidated damages clauses and letters of credit do in the paper world. Lessig's claim that "Code is Law" (1999) is thus brought to a new extreme with the advent of smart contracts, which can now directly incorporate legal or contractual provisions into a technological infrastructure that will automatically enforce these provisions, regardless of the will of the parties. Moreover, as more and more private or public actors start adopting blockchain as part of their information system,

we are witnessing a shift from “Code is Law”, namely code having the effect of law, toward “Law is Code”, meaning that law is defined as code (De Filippi & Hassan, 2018).

Smart contracts were first described by Nick Szabo in the late 1990s. He envisioned placing contracts into code that could be both “trustless” and self-enforcing, enhancing efficiency and removing ambiguity from contractual relationships (Szabo, 1996). In fact, in light of their technical properties of “guaranteed execution” (i.e., the fact that no single actor can intervene in order to interface or even stop the execution of the smart contract code), smart contracts eliminate the need for trust amongst the parties, who can be sure that the contract will be performed exactly as agreed (Savelyev, 2017). In this sense, a smart contract can be regarded as an enforcement mechanism for online dispute resolution, bypassing the need for intermediary operators (Koulu, 2016). Yet, blockchain actors who directly benefit from continued differentiation and fragmentation of Lex Cryptographica from legacy legal systems, need to acknowledge that, at the same time, state actors may also have legitimate regulatory aims for greater legislative/regulatory intervention into the blockchain space (Wright & De Filippi, 2015). For example, state actors moved quickly to regulate cryptocurrency exchanges and initial coin offerings to the public. Hence, the various stakeholders of a blockchain-based system need to understand current laws and regulations, both at the national and international level, in order to construct a new and separate techno-legal framework that operates according to its own rules and principles, and yet is properly recognized by governments and other state actors as a legitimate body of customary laws (Barnett & Treleaven, 2018). We therefore suggest a close investigation of stakeholders’ conflicting interests:

> Research Question 27 (RQ27): How can the conflicting legal interests of blockchain actors and state actors be balanced?

For this techno-legal framework to retain its autonomy (and independence) from existing laws and regulations, it is critical to implement at least two separate but interlinked strategies. The first one is the legal recognition of blockchain-based private arbitration as a binding decision. There are few instances of private arbitration or ADR systems run by international organizations which have acquired a certain degree of sovereignty in an international or transnational context. For example, FIFA has established an international Court of Arbitration for Sport (CAS), acting as a tribunal of last instance that has jurisdiction to settle football-related legal disputes, if attempts to solve the dispute internally at FIFA or the confederations prove unsuccessful. When FIFA rules have been properly proscribed and invoked within a court of law, these courts have declared that the sovereign law does not apply and that courts have no competence to hear the cases, referring the matter instead to CAS to apply FIFA rules. Based on these insights, some blockchain-based initiatives have emerged, providing new “virtual jurisdictions” (e.g., Kleros, Aragon). These initiatives could eventually acquire legal standing (Goldenfein & Leiter, 2018) and, if the procedure is done in compliance with the legal framework, the decisions made within these jurisdictions could potentially be recognized as legally binding according to the rules enshrined in the NY Convention. The second strategy is customary law for blockchain systems. Customary laws operate alongside existing regulatory frameworks. For instance, in Sharia law, the Muslim Arbitration Tribunal is a form of ADR which is recognized under the UK Arbitration Act of 1996. This enables Muslims to resolve disputes according to the rules enshrined in Sharia law, without recourse to the UK courts system (Bowen, 2011). UK arbitration law stipulates that parties can choose to settle their disputes under a non-state mandated law (e.g., Sharia law) under the condition that such law is sufficiently outlined (rising to the level of “black letter law”) and widely adopted by the community (Lando, 1995). In light of these examples, it is worth asking whether the rules by which relationships and disputes between decentralized autonomous organizations (DAOs) or other blockchain-based organizations are managed, could eventually be applied to blockchain-based systems (De Filippi & Wright, 2018) - creating a real “Lex Cryptographica” for the future recognition of non-state rules by state actors:

> Research Question 28 (RQ28): Can community rules emerge as a new form of customary law for blockchain based systems?

Smart contracts challenge the maxim, “code is not law”: One solution is to create a system that translates legal contract templates into smart contract code. Barclays Bank, for example, developed a user interface where people

fill in variables on a legal contract template and the underlying smart contract code is automatically generated (Rizzo, 2016). Barclays Bank envisioned that standard-making bodies ultimately would be in charge of the legal/smart contract "templates" to ensure compliance and to facilitate standard agreements (Braine, 2016). Beyond a single firm's attempt at turning code into law, The Accord project, led by lawyers, is building an open source software toolkit for legally enforceable contracts. The project supports Corda, Hyperledger Fabric, and Ethereum blockchain platforms, illustrating the current efforts to reconcile an existing legal framework with new technical possibilities or vice versa.

The Technological Perspective: The Rise of Complex Distributed Systems and Cryptography

Blockchain systems are frequently seen as a promising technology for the future infrastructure of a global value-exchange network – or what some refer to as the "Internet of Value". The original hash-chained timestamp proposed by Haber and Stornetta (Bayer et al., 1993; Haber & Stornetta, 1991) is now a fundamental component within most blockchain systems, starting with the Bitcoin system which first adopted it for a digital currency use case. If blockchain technology is to become a fundamental part of the future global distributed network of commerce and value, then its architecture must also satisfy the fundamental goals of the Internet architecture. That is, it must possess the three main design goals of the Internet architecture. These goals were (i) the support for a variety of service types that span across multiple kinds of applications, (ii) the survivability of the system in face of various kinds of attacks (Hardjono et al., 2019), and (iii) the support for a variety of blockchain systems based on the minimal assumption of a standardized transaction format and syntax, and a standardized set of operations (opcodes). We will elaborate on all three in the sections below.

Given the history of the development of the Internet and of computer networks in general (e.g., LANs, WANs), it is unlikely that the world will settle on one global blockchain system operating universally. The emerging picture will most likely consist of "islands" of blockchain systems, which – like autonomous systems that make up the Internet – must be "stitched" together in some fashion to make a coherent unity end-to-end. Therefore, interoperability is core to the entire value proposition of blockchain technology. Interoperability across blockchain systems must be a requirement both at the mechanical level and the value level. At the value level, interoperability leads to the prevention of lock-in of value within a given blockchain system. Users must be able at any time to transfer value (tokenized or otherwise) from one blockchain system to another, with speed, trust and accountability. Interoperability at the mechanical level is necessary for interoperability at the value level but does not guarantee it. The mechanical level plays a crucial role in providing technological solutions that can help humans in quantifying risk through the use of a more measurable notion of technical trust. Human agreements (i.e., legal contracts) can be used at the value level to achieve semantically compatible meanings to the constructs (e.g., coins, tokens) that circulate in the blockchain system. Given the nascent state of blockchain technology today, we suggest the following:

> Research Question 29 (RQ29): What are the implications of interoperability of blockchain systems at the mechanical level?

At the mechanical level there needs to be interoperability at the "packet" level, meaning that a bare minimum transaction semantics need to be standardized. This is akin to the bare minimum IP packet instance that was proposed by Vint Cerf and Bob Kahn in their milestone 1974 paper (Cerf & Kahn, 1974). For example, standardized blockchain transactions could include a sender public-key (origin address), a recipient public-key (destination address), an operation code (op-code), timestamp and transaction-data that are contextual to the blockchain system and possibly the end users.

Survivability of blockchain systems presupposes interoperability of transactions across domains (cross-chain). In fact, A key lesson from the three decades of the development of the Internet is that *interoperability* is key to survivability. For inter-domain transactions, there are number of challenges that remain to be addressed relating to the atomicity of transactions. The notion of atomicity as understood in the classic ACID properties (atomicity, consistency, isolation and durability) of database systems (Gray, 1981) does not necessarily map cleanly to cross-

chain transactions (Herlihy, 2019). Thus, a new paradigm for contemplating "atomicity" for inter-domain transactions is needed.

> Research Question 30 (RQ30):: What are the implications of interoperability of blockchain systems at the value level?

Related to cross-chain transactions is the challenge of providing stability of the underlying value of assets being transferred cross-chain. This is particularly relevant for asset swap scenarios (e.g. bid/ask transactions) that require value stability during the transfer. Both sides in a swap need assurance that the value of their respective virtual assets remain stable until the swap settles on both blockchain systems. Since the blockchain systems on either side may employ differing consensus protocols and thus differing settlement (confirmation) times, this means that an (implicitly) agreed foundational value regime is needed. Thus, one implication may be that of the necessity for stable-coins (Lipton et al., 2020) – either centralized or decentralized – to be a pre-requirement for interoperable cross-chain transactions involving value-bearing virtual assets.

One key proposition of blockchain technology as exemplified by the Bitcoin system is the independence of nodes to compute the proof-of-work in order to obtain remuneration and contribute to the settlement of the next block of transactions. Consequently, the robustness of a blockchain system consisting of a peer-to-peer network of nodes is largely affected by the security of the nodes and other components that make up the network. If nodes are easily compromised directly (e.g., hacks) or via indirect means (e.g., dormant viruses), the utility of the blockchain system degrades considerably. The possible types of attacks to a blockchain system consist of a broad spectrum. These range from classic network-level attacks (e.g., network partitions, denial of services, distributed denial of service) to more sophisticated attacks targeting the particular constructs (e.g., consensus implementation (Eyal & Sirer, 2018; Gervais et al., 2014; Schneier, 2019)), to targeting specific implementations of mining nodes (e.g., code vulnerabilities, viruses). Thus, more research must be dedicated into understanding new trusted computing capabilities needed for the components that participate in the various types of blockchain autonomous systems. For example, trusted computing base (TCB) technologies may be able to provide a higher assurance to nodes participating in consensus protocols. Nodes that are TCB-capable may be able to not only operate in a provable trustworthy manner, but also allow them to convey this trust in some measurable way to external entities (e.g., to other peer nodes and to wallet systems at the end-users) (Hardjono & Smith, 2019). We thus suggest to closely investigate the design and impact of trust:

> Research Question 31 (RQ31): Can TCB technologies be used to create trust in blockchains?

Today there are a number of access models for blockchain systems being studied and developed. As we outlined above, these fall into (a) *access-permissionless* (public) blockchain systems, and (b) *access-permissioned* (or semi-permissioned) blockchain systems. The term "access" here is used to denote the situation in which any user/wallet and any node can participate in (have access to) the peer-to-peer network of nodes without authentication or authorization from another entity. One aspect that may determine the appropriateness of the access model for a given application is the ability of the participants (both users and nodes) to measure and quantify risks associated with their participation. Such quantification is core to the business risk assessment paradigm of many organizations. In traditional enterprises, technology-related risks can be mitigated in several ways, including developing a robust IT infrastructure, developing a comprehensive security and audit regime, strong user/device authentication and authorization mechanism. The situation is somewhat different with the nascent blockchain technology. New research efforts need to be devoted to understanding and addressing the new risk profiles associated with the use of the different kinds of blockchain systems. This includes understanding the risks in participating in access-permissionless and permissioned blockchains, in the use of custody wallet services, and in engaging with centralized/decentralized exchanges. The ability for a user or organization to quantify risks related to the use of blockchain technology may be a key factor in driving the adoption of blockchain technology globally. We thus suggest the following:

> Research Question 32 (RQ32): What types of risks are associated with different blockchain technologies and how can they be mitigated?

The Philosophy of Science Perspective: Conceptual Advance in Distributed Ledger Technology

Adopting a philosophy of science lens suggests that blockchains may be just one element in the larger overall digital transformation process of migrating to smart network technology platforms that include features of blockchains, machine learning, Internet of Things, and cloud computing technologies. *Smart networks* are autonomous self-operating computing networks that constitute a novel class of global computational infrastructure (Swan et al., 2020). A philosophical issue arises in that with smart networks, the conceptualization of the scope and definition of the Internet is greatly exceeding its initial form as a simple communications network for data transfer, to now being to a self-acting computational platform with increasing degrees of autonomous operation (Swan & Filippi, 2017). Smart network technologies with autonomous behavior examples include but are not limited to high-frequency trading networks, unmanned aerial vehicles, real-time bidding for advertising markets, and automated supply chains. Over time, smart networks with standard feature-sets from blockchains and machine learning (such as audit-logging and image recognition) might be used to automatically coordinate hundreds of fleet-many items at scales ranging from the macro logistics of space settlement to the micro coordination of brain-computer interfaces and medical nanorobots (Martins et al., 2019).

Important advances in the physical sciences, computer science, and network mathematics underly blockchain technology and can be brought to bear on blockchain design. These advances motivate the research questions proposed in this section. Moreover, many of these same advances are recognized as having generalized principles applicable in a multidisciplinary fashion to a variety of fields. The first step toward a better understanding is the conceptual articulation of how advances in one field may apply to another, and hence, the philosophy of science approach. The conceptual result often precedes the analytical formalization, and the numerical, computational, or mechanical realization of a technology advance. Two specific advances (spin glass optimization models and information-theoretic computational complexity) are developed here towards the resolution some of the biggest challenges facing blockchain economic networks, namely the scalability of network throughput and the ability to achieve consensus more efficiently (given the substantial resource consumption required by proof-of-work mining). To address scalability, a spin glass optimization model of blockchains is proposed, writing blockchains in the matrix model of a directed acyclic graph (DAG) for further interpretation as an energy minimization problem. To target consensus, a blockchain computational complexity model of distributed ledger technologies (DLTs) is considered with high-dimensional network geometry. Further, the implications of quantum computing are discussed as one of the biggest potential disruptions to blockchains.

Scalability: Blockchain Spin Glass Optimization Model

Blockchains have a scalability problem in that network throughput, as of June 2020, is 5-7 TPS (transactions per second) in public ledgers. This compares with an average of 1,700 processed transactions per second for VISA (Sedgwick, 2018), although burst capacity is estimated to be much higher. For mainstream adoption, blockchain throughput would need to be much higher, and various scalability solutions are under consideration.

Smart routing could be one way to achieve greater scalability. This is the idea of applying optimization methods to produce more expedient transaction routing through the network. Distributed ledgers are organized according to principles of security and anonymity as opposed to optimization. Other technologies such as machine learning are developed with optimization as a central principle that could inform blockchain design. For example, deep learning neural networks generate algorithms to classify patterns in existing data sets such that similar patterns can be identified in new data sets. The system catalogs all possible features, equally weighting each feature. Then the system operates by making trial and error guesses to “learn” which features occur with greater regularity, and gradually upweights the most relevant features (for example, in facial recognition images, the jaw line as opposed to the clothing color). The network architecture and the mechanism of automatically adjusted weights provides the basis for running as an optimization algorithm. Deep learning systems minimize gradient descent (a loss function) to find the best algorithm with the fewest errors.

Spin glasses provide the conceptual inspiration for machine learning network design by analogy to energy minimization principles in physical materials (Hopfield, 1982). A spin glass is a disordered magnet, meaning a metastable system in which some of the spins of its constituent atoms point up and others down. Contrast to an ordered magnet (such as a ferromagnet), which is a stable system with all of the spins ordered or pointing in the same direction, thus comprising the lowest energy configuration. Spin glasses are attractive as a computational model because the variable system can be manipulated into a lower-energy state which corresponds to the optimal solution to a problem. In addition to deep learning, the spin glass model has other notable applications in protein-folding (Bryngelson et al., 1995).

Smart routing in blockchains could likewise frame network transaction routing as an energy minimization problem in the spin glass model. The blockchain network is a spin glass in that individual nodes exist in variety of spin-up and spin-down states in terms of being available or unavailable to transmit network traffic. The idea is to frame network routing as a least-energy problem with the optimization equations from spin glass formulations used in deep learning and protein folding. The Ripple network already operates on this kind of basis (although not using spin glass models) in the sense of being a live credit network in which each network node has to agree to the passing of actual monetary balances as opposed to simple transaction message passing. Hence, each node has a binary on-off status analogous to a spin-up or spin-down state, and could be incorporated into a spin glass model. Sphinx routing and rendez-vous routing are other examples of blockchain smart routing techniques. In sphinx (unknown parties) and rendez-vous (connecting at a randomly-specified network node) routing, end users select preferred routing principles for greater levels of privacy and anonymity. The same structures could be deployed for network efficiency by applying spin glass optimization principles. Smart-routing SLAs (service level agreements) can be envisioned with criteria including options related to expediency, security, privacy, and timing requirements.

The concrete implementation of blockchain spin glass smart routing requires two steps. The first is writing the blockchain in a format conducive to being translated into an optimization problem. This need could be satisfied with an overlay to the existing blockchain software which would continue to operate as normal. The blockchain could be written as a DAG (directed acyclic graph), irrespective of whether the underlying blockchain itself is organized as a DAG (most are not). The DAG format is a communications network formalism that allows traffic management features such as directed path routing, time cycle routing, and other parameters to be implemented. The idea is to see blockchains as a network computing platform, and perform various computations with network theory principles. The scalability problem can be framed as a network science problem specified in terms of a directed graph, which means that all of the formalisms of graph theory become available to problem-solving in the blockchain domain. With matrix algebra, an equation for the blockchain as a DAG can be written. The blockchain scalability challenge is made explicit as a solvable formalism.

The second step is translating the blockchain DAG equation to an energy landscape problem using the spin glass model. The spin glass model is then used to calculate the lowest energy state of the system which corresponds to the optimal smart route. The spin glass blockchain model could be solved with classical or quantum computers.

> Research Question 33 (RQ33): How does smart routing based on spin glass optimization and DAG network mathematics impact network scalability?

More specifically, we hypothesize a positive effect of spin glass models on scalability:

> Hypothesis 5 (H5)*:* Spin glass models deliver improved blockchain scalability via optimized smart routing (see Figure 3)

Insert Figure 3 About Here

Consensus: Blockchain computational complexity facilitates efficient consensus

Part of the blockchain scalability problem constraining the number of transactions processed per second is the high cost of reaching consensus in public ledgers. Consensus is the automated process by which the nodes in the distributed worldwide computer network automatically arrive at agreement about updates to the ledger (i.e. what is to count as valid transactions between wallet balance holders). The traditional way to transfer funds is to use a bank, which is a centralized party that confirms account holder identity and the availability of funds for transfer. The blockchain method is a decentralized worldwide network that checks in real-time when transactions are presented, that funds are available and that the sending party and the receiving party wallet addresses exist. To have such a smart network, a worldwide always-on value transfer system, requires a way of providing cryptographic (network cryptography based) security measures such that the ledger records and transfers do not get hacked.

The Bitcoin blockchain is a triumph in providing cryptographic security for this kind of system of always-available consensus-driven digital value transfer (Bitcoin's first transactions were in January 2009, and the chain has logged over 636,000 blocks of transactions as of June 26, 2020 according to btc.com). The Bitcoin blockchain itself has not been hacked (hacking is typically at the on- and off-ramps of user wallets and exchange websites). It is known that not even one bit is different in the entirety of the Bitcoin ledger because every time a new block is added, the participating accountants (miners) confirm that nothing has changed. The ledger records can be confirmed quickly due to the Merkle tree structure of blockchains. The transaction block data is organized into a tree structure in the form of hash codes which aggregate arbitrarily-large bodies of digital data. The entire Bitcoin blockchain can be called with one 64-character top-level hash code, the Merkle root. Accounting (mining) software automatically checks each time a new block is presented that no change has occurred to any previous block.

In spite of blockchains' success in providing cryptographic security, the cost is high in terms of the amount of computing power (electricity) used by the hundreds of thousands of accountants (miners) worldwide who compete to record the next transaction block. Miners participate because rewards are lucrative, and the mining operation is designed to deter malicious participants by forcing bonafide participants to demonstrate their good intent by actually performing a proof-of-work, by competing to solve a cryptographic puzzle. The challenge is to find more efficient ways of delivering the same level of cryptographic security at lower cost.

Here, the research proposal is to employ complexity methods more formally to develop next-generation consensus algorithms. Blockchains are complex systems and as such warrant a greater application of known complexity methods for their study and execution. Complex systems are those that are non-linear, emergent, open, unknowable at the outset, interdependent, and self-organizing (Swan, 2020a). The risk of failing to consider the full range of effects in complex systems, as Cartwright (1983) points out, is that solutions are often not adequate to the complexity of the underlying problem domain. Complexity methods are starting to be used to study blockchains. For example, since proof-of-work consensus is known to be secure but inefficient, proof-of-stake (wallet owners effectively co-signing new blocks proposed by other wallet owners) and hybrid algorithms (a combination of proof-of-work and proof-of-stake) have been proposed. Dos Santos (2017, 2019) used statistical complexity to demonstrate that proof-of-work algorithms have low complexity (and therefore convey less financial system risk) as compared with proof-of-stake and hybrid algorithms. The result is that even if more efficiently executed, proof-of-stake consensus algorithms might be undesirable due to contributing to greater overall financial system risk.

The specific complexity methods to be used in a first-principles analysis of blockchains could include computational complexity (the computational resources in terms of time and space required to calculate a problem) and algorithmic efficiency (assessing query complexity (the number of queries the algorithm makes to the information source) and gate logic complexity (the number and type of operations in the process)). The success of information theory and complexity methods has been demonstrated as a physical science-based result that has application to many fields (Swan, 2020b). A landmark example is Harlow & Hayden proposing (2013) a resolution to a problem in the study of black holes, suggesting with an information theoretic analysis that although it would be possible to obtain information about a particle radiating out of a black hole, it would not be possible to do so within a practical time frame.

Central to complexity methods is the computational complexity analysis of the amount of time and memory (space) needed to solve a computing problem. Problems are classified into tiers of computational complexity labeled in categories such as P and NP, indicating problems that are solvable in polynomial time (i.e. a reasonable amount of time) or those that are not. The canonical Traveling Salesperson problem (an optimal route to as many cities as possible) is an NP-hard problem, meaning that it is difficult to find an answer but easy to check a solution that is presented. The Traveling Salesperson problem has the network structure of one-to-many connections. However, blockchains have a many-to-many connections network landscape that requires a new and higher-dimensional consideration in complexity analysis. This work therefore proposes *blockchain computational complexity* as a metric to capture the complexity of blockchains as they grow. The analysis parameter of interest is whether blockchains grow linearly or exponentially in complexity as they grow in transaction processing. Blockchain computational complexity can be represented and solved with random tensor matrix models (Gurau, 2016) which accommodate the higher-dimensional network geometries of blockchains with many-to-many connections.

In the practical domain, blockchain computational complexity could be used to analyze proposed next-generation consensus algorithms (e.g., from DFINITY, Hashgraph, IOTA, Nano, and ByteBall). These algorithms are able to deliver greater efficiency by harnessing the law of large numbers in that having more blockchain participants means being able to randomly select users to perform tasks rather than having an expensive alongside mining operation. Testing the complexity of such proposals could help determine which are most financially sound from a risk perspective. Blockchain computational complexity could likewise be directed to the analysis of other technical problems such as questions related to block size, setting transaction fees, sidechain offloading, payment channel ecologies (for example, the optimal smart contract configuration for a 30-year mortgage), and the capacity of system overlays such as the Lightning Network to deliver liquidity to the underlying chain. Another issue is trust creation in the context of resolving the problem that without being mined, enterprise blockchains do not deliver so-called “trustless trust”. We therefore propose the following research question and hypothesis:

> Research Question 34 (RQ34): How does blockchain computational complexity impact consensus?
>
> Hypothesis 6 (H6)*:* Computationally-efficient consensus algorithms might deliver low-complexity cost-effective consensus at the same or better levels of cryptographic security. (Figure 4)

Insert Figure 4 About Here

Quantum Computing: New Foundations

Quantum computing is in the early stages of development, but is farther along than may be realized as systems are commercially available from IBM, Rigetti, and D-Wave Systems (Swan et al., 2020). Quantum computing simultaneously poses the biggest threat and opportunity for blockchains as it is anticipated that quantum computing would eventually be able to break the existing cryptographic standards which are central to blockchain operation. On one hand, a US National Academies of Sciences report indicates that “it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade” (Grumbling & Horowitz, 2019, 157). On the other hand, methods are constantly improving, and the time frame could shrink (Gidney & Ekerå, 2019). Irrespective, ten years is well within the planning horizon for most large-scale organizations and many parties have strategic quantum readiness initiatives underway.

The implication of quantum computing for distributed ledger technology is that blockchains will have to upgrade to the current cryptographic standard, including those which may eventually involve quantum cryptography. Cryptographic standards are of tantamount concern for maintaining the security of blockchain ledgers. Beyond cryptographic security, more foundationally, there is the possibility of implementing blockchain protocols themselves

on quantum computation platforms. Transaction data might be encoded in qubits, which could store the history of all previous transactions, and per quantum entanglement, could not be hacked without destroying the qubits (Rajan & Visser, 2019). Even without instantiating blockchains in quantum networks, quantum computing as a platform is indicated as an upgrade for the Internet due to cost reduction in network transfer time and resource utilization.

In particular, blockchain-based consensus processes could benefit from quantum computing. Consensus relies on the concept of entropy, meaning that it is unknown which machine or set of machines (for example, which 250 signatures out of 300 machines selected at random) will be engaged to confirm the next block of transactions. Such unpredictability is needed to prevent malicious hackers from guessing which machines to attack in the distributed network. Hence, the key to consensus is efficient entropy creation. Proof-of-work mining is expensive, and instead, quantum interference patterns might provide an effective source of entropy. Following the work of Aaronson (2018), quantum computing models might be used to assign amplitudes to possible states of the world, and then these amplitudes exploited to obtain a speed advantage with orchestrated interference patterns. The amplitude results are converted into probabilities (as the squared absolute value of the amplitude), and are provably random since the statistical patterns could only have been generated by a quantum computer. Thus, a more efficient means of trustless trust is provided with quantum randomness. Boneh et al. (2018) propose related efforts to develop high-probability confidential transaction confirmation. We suggest the following research question and hypothesis:

> Research Question 35 (RQ35): How does provable quantum randomness impact distributed ledger technology (DLT) entropy-based consensus?
>
> Hypothesis 7 (H7)*:* Quantum interference patterns can be used to produce secure and efficient consensus processes.

Conclusions, Limitations & Future Research

In this paper we present blockchain technology as a multifaceted artifact that necessitates multidisciplinary research in order to explain, explore and predict its full range of potential implications. We neither claim nor believe that blockchain is a silver bullet for all problems mankind is currently facing, but we strongly believe that a rigorous and comprehensive research agenda will unveil a plethora of interesting use cases for this novel technology and will allow us to better understand its potential impact. By simultaneously considering business, economic, social, legal, technical, and philosophical implications, new insights can be gained that can help us to systematically advance blockchain research. More specifically, we believe that the careful investigation of the “side effects” on other domains and the emergence of research that spans boundaries will lead to new insights into the disruptive power of blockchain. Not every blockchain solution that is feasible from a technical perspective is legal; solutions that benefit individual businesses can have unprecedented macroeconomic implications and the societal change that can be triggered by blockchain applications is largely unexplored. Smart network theory, as presented in this paper, creates an inextricable bond of technology and philosophy. All research questions (RQs) and hypotheses (Hs) that we propose in this paper originate in a specific domain, but the difficulty lies in taking them up, developing them further and, finally, looking at them from a different perspective. We believe that each merits a profound investigation and so we challenge inquisitive scholars to use them as starting points for their own research.

The research program introduced here is possibly limited by a number of constraints. Many of these apply to blockchain adoption in general. As discussed in the business section, commercial adoption has been slow. There is a lack of “killer apps” in the sense of solid implementation cases that demonstrate the technology’s value proposition, a paucity of skilled distributed ledger technology software programmers that can implement solutions, and the fact that the complexity of the technology makes it recalcitrant to both organizational and consumer end user adoption. Still, we believe that this should not stop us from conducting cutting-edge research which can support the industry and policy to overcome the aforementioned issues and educate the general public about the ramifications of blockchain. Another potential limitation is blockchain’s rapid development which may lead to new application opportunities, but might also create new attack vectors. We therefore confined ourselves to selected topics which we believe will be relevant for the years to come and do not claim to have comprehensively covered

all potentially interesting areas in a structured way. Rather it was our intention to inspire other researchers by suggesting a few innovative research questions and hypotheses that we deem worthwhile for further investigation. A multidisciplinary perspective to research challenges is outlined here, whereas problems regularly tend to be taken up within the scope and methods of the field in which they arise. However, the point of an approach that transcends boundaries is that it allows to develop a wider range of tactical and conceptual resources for problem solving in the distributed ledger technology domain and fosters a deeper understanding of the phenomenon under investigation. The first step is for these varied disciplines to "get to know each other"; it has been our intention to encourage that familiarity. We thus hope that our paper will serve as a departure point for many promising research endeavors and strongly encourage researchers from different disciplines to work together and use our research suggestions as inspirations to take blockchain research to the next level.

References

Aaronson. (2018). PDQP/qpoly=ALL. *Quantum Information & Computation*, *18*(11 & 12), 901–909.

Adhami, S., Giudici, G., & Martinazzi, S. (2018). Why do businesses go crypto? An empirical analysis of initial coin offerings. *Journal of Economics & Business*, *100*(C), 64–75. Retrieved from https://doi.org/10.1016/j.jeconbus.2018.04.001

Akerlof, G. A. (1970). The market for „lemons": Quality uncertainty and the market mechanism. *Quarterly Journal of Economics*, *84*(3), 488–500. Retrieved from https://doi.org/10.2307/1879431

Allen, D. W. E., Lane, A., & Poblet, M. (2019). The governance of blockchain dispute resolution, *Social Science Research Network*. Retrieved from https://papers.ssrn.com/abstract=3334674

Angel.co. (2020). Blockchain Startups. *AngelList*. Retrieved from https://angel.co/blockchains

Barnett, J., & Treleaven, P. (2018). Algorithmic dispute resolution—The automation of professional dispute resolution using AI and blockchain technologies. *The Computer Journal*, *61*(3), 399–408. Retrieved from https://doi.org/10.1093/comjnl/bxx103

Bavec, C. (2006). On the current environments for e-Government development in the enlarged European Union. *Information Polity: The International Journal of Government & Democracy in the Information Age*, *11*(3/4), 197–206.

Bayer, D., Haber, S., & Stornetta, W. S. (1993). Improving the efficiency and reliability of digital time-stamping, In R. Capocelli, A. DeSantis, & U. Vaccaro (Eds.), *Sequences II: Methods in Communication, Security and Computer Science*, New York: Springer, 329-334.

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, *19*(10), 1020–1034. Retrieved from https://doi.org/10.17705/1jais.00518

Berg, C., Davidson, S., & Potts, J. (2019). *Understanding the Blockchain Economy: An Introduction to Institutional Cryptoeconomics*. Cheltenham: Edward Elgar.

Boneh, D., Bünz, B., & Fisch, B. (2018). *Batching Techniques for Accumulators with Applications to IOPs and Stateless Blockchains* (Cryptology ePrint Archive Nr. 1188). Retrieved from https://eprint.iacr.org/2018/1188

Boring, P., & Kim, A. D. (2018). *Understanding Digital Tokens: Market Overviews and Proposed Guidelines for Policymakers and Practitioners*. Chamber of Digital Commerce. Retrieved from https://digitalchamber.org/token-alliance-paper/

Bowen, J. (2011). How could English courts recognize Shariah? *University of St. Thomas Law Journal*, *7*(3), 411–436.

Braine, L. (2016). *Barclay's Smart Contract Templates*. Barclays Accelerator London Demo Day. Retrieved from https://www.r3cev.com/projects/

Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review*, *34*(6), 1180–1196. Retrieved from https://doi.org/10.1016/j.clsr.2018.08.005

Bryngelson, J. D., Onuchic, J. N., Socci, N. D., & Wolynes, P. G. (1995). Funnels, pathways, and the energy landscape of protein folding: A synthesis. *Proteins: Structure, Function, and Bioinformatics*, *21*(3), 167–195.

Bunduchi, R. (2005). Business relationships in internet-based electronic markets: The role of goodwill trust and transaction costs. *Information Systems Journal*, *15*(4), 321–341. Retrieved from https://doi.org/10.1111/j.1365-2575.2005.00199.x

Cartwright, N. (1983). *How the Laws of Physics Lie*. Oxford: Oxford University Press.

Castellacci, F., & Tveito, V. (2018). Internet use and well-being: A survey and a theoretical framework. *Research Policy*, *47*(1), 308–325. Retrieved from https://doi.org/10.1016/j.respol.2017.11.007

CBInsights. (2019). *The Fintech 250*. Fintech 250. Retrieved from http://instapage.cbinsights.com/research-fintech250

Cerf, V. G., & Kahn, R. E. (1974). A protocol for packet network intercommunication, *IEEE Transactions on Communications*, COM-22(5), 637–648

Chod, J., Trichakis, N., Tsoukalas, G., Weber, M., & Aspegren, H. (2018). Blockchain and the value of operational transparency for supply chain finance. *SSRN Electronic Journal*.

Christensen, C. M. (1997). *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*. Boston: Harvard Business Review Press.

Christensen, C. M., Raynor, M., & McDonald, R. (2015). What is disruptive innovation? *Harvard Business Review*, *93*(12), 44–53.

Clohessy, T., Acton, T., & Rogers, N. (2019). Blockchain adoption: Technological, organisational and environmental considerations. In H. Treiblmaier & R. Beck (Eds.), *Business Transformation through Blockchain (Vol. 2)*, Cham: Palgrave Macmillan, 47-76.

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

Connerty, A. (2014). Lex mercatoria: Reflections from an English lawyer. *Arbitration International*, *30*(4), 701–719.

Cornelius, K. B. (2018). Smart Contracts and the Freedom of Contract Doctrine. *Journal of Internet Law*, *22*(5), 3–11.

Coyne, J. G., & McMickle, P. L. (2017). Can blockchains serve an accounting purpose? *Journal of Emerging Technologies in Accounting*, *14*(2), 101–111. Retrieved from https://doi.org/10.2308/jeta-51910

Dahrendorf, R. (1996). Economic opportunity, civil society and political liberty. *Development and Change*, *27*(2), 229–249. Retrieved from https://doi.org/10.1111/j.1467-7660.1996.tb00587.x

Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, *31*(3), 5–21. Retrieved from https://doi.org/10.2308/isys-51804

De Filippi, P., & Hassan, S. (2018). Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday*, 21(12). https://doi.org/10.5210/fm.v21i12.7113

De Filippi, P., & Wright, A. (2018). *Blockchain and the Law: The Rule of Code*. Cambridge: Harvard University Press.

DiMaggio, P. J., & Powell, W. W. (1991). The iron cage revisited: Industrial isomorphism and collective rationality in organizational fields. In W. W. Powell & P. J. DiMaggio (Eds.), *The New Institutionalism in Organizational Analysis*, Chicago: University of Chicago Press, 63-82.

Dos Santos, R. P. (2017). On the philosophy of Bitcoin/blockchain technology: Is it a chaotic, complex system? *Metaphilosophy*, *48*(5), 620–633. Retrieved from https://doi.org/10.1111/meta.12266

Dos Santos, R. P. (2019). Consensus algorithms: A matter of complexity? In M. Swan, J. Potts, T. Soichiro, F. Witte, & P. Tasca (Eds.), *Blockchain Economics: Implications of Distributed Ledgers: Markets, Communications Networks, and Algorithmic Reality*, Singapore: World Scientific Publishing Co. Pte. Ltd, 147-170.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *The Academy of Management Review*, *14*(1), 57-74. Retrieved from https://doi.org/10.2307/258191

Engle, P. (2018). Blockchains and Bitcoins. *ISE: Industrial & Systems Engineering at Work*, *50*(1), 20–20.

Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, *61*(7), 95–102. Retrieved from https://doi.org/10.1145/3212998

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. *Journal of Network & Computer Applications*, *126*, 45–58. Retrieved from https://doi.org/10.1016/j.jnca.2018.10.020

Gervais, A., Karame, G. O., Capkun, V., & Capkun, S. (2014). Is Bitcoin a decentralized currency? *IEEE Security Privacy*, *12*(3), 54–60. Retrieved from https://doi.org/10.1109/MSP.2014.49

Gidney, C., & Ekerå, M. (2019). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *arXiv:1905.09749 [quant-ph]*. Retrieved from http://arxiv.org/abs/1905.09749

Goldenfein, J., & Leiter, A. (2018). Legal engineering on the blockchain: 'Smart contracts' as legal conduct. *Law and Critique*, *29*(2), 141–149. Retrieved from https://doi.org/10.1007/s10978-018-9224-0

Government Office for Science. (2016). *Distributed ledger technology: Beyond block chain. A report by the UK government chief scientific advisor*. London: Government Office for Science.

Grain Discovery.com (2020). *Welcome to the Future of Agriculture*. Grain Discovery. Retrieved from https://graindiscovery.com

Gray , J. (1981). The transaction concept: Virtues and limitations, *Proceedings of the 7th Very Large Data Bases International Conference*, September 1981, 144-154.

Griffith, E. (2017). *Startups: Conventional Wisdom Says 90% Fail. Data Says Otherwise.* Fortune. Retrieved from https://fortune.com/2017/06/27/startup-advice-data-failure/

Grumbling, E., & Horowitz, M. (Eds.). (2019). *Quantum Computing: Progress and Prospects*. US National Academies of Sciences. Retrieved from https://doi.org/10.17226/25196

Gupta, S. (2018). *Demystifying the Real World of Blockchain*. HFS FORA Summit, December 11, New York.

Gurau, R.G. (2016). *Random Tensors*. Oxford: Oxford University Press.

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, *3*(2), 99–111. Retrieved from https://doi.org/10.1007/BF00196791

Halldorssón, A., Kotzab, H., Mikkola, J. H., & Skøjtt-Larsen, T. (2007). Complementary theories to supply chain management. *Supply Chain Management*, *12*(4), 284–296.

Hardin, G. (1968). The tragedy of the commons. *Science*, *162*(3859), 1243–1248.

Hardjono, T., Lipton, A., & Pentland, A. (2019). Toward an Interoperability architecture for blockchain autonomous systems. *IEEE Transactions on Engineering Management (Early Access)*, 1–12. Retrieved from https://doi.org/10.1109/TEM.2019.2920154

Hardjono, T., & Smith, N. (2019). Decentralized trusted computing base for blockchain infrastructure security. *Frontiers in Blockchain*, *2*(24). Retrieved from https://doi.org/10.3389/fbloc.2019.00024

Harlow, D., & Hayden, P. (2013). Quantum computation vs. firewalls. *Journal of High Energy Physics*, 85.
Retrieved from https://doi.org/10.1007/JHEP06(2013)085

Herlihy, M. and Liskov, B. & Shrira, L. (2019). Cross-chain deals and adversarial commerce, *Proceedings of VLDB*, *13*(2), 100-113.

Hopfield, J.J. (1982). Neural networks and physical systems with emergent collective computational abilities. *Proceedings of the National Academy of Sciences*, *79*(8), 2554–2558.

Huckle, S., & White, M. (2016). Socialism and the blockchain. *Future Internet*, *8*(4), 1-15. Retrieved from https://doi.org/10.3390/fi8040049

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, *95*(1), 118–127.

Jacobides, M. G., Cennamo, C., & Gawer, A. (2018). Towards a theory of ecosystems. *Strategic Management Journal*, *39*(8), 2255–2276. Retrieved from https://doi.org/10.1002/smj.2904

Kauflin, J. (2018). *Hedera Hashgraph Thinks It Can One-Up Bitcoin And Ethereum With Faster Transactions*. Forbes.com. Retrieved from https://www.forbes.com/sites/jeffkauflin/2018/03/13/hedera-hashgraph-thinks-it-can-one-up-bitcoin-and-ethereum-with-faster-transactions/#44dc6f09abcb

Kim, H., Laskowski, M., & Nan, N. (2018). A first step in the co-evolution of blockchain and ontologies: Towards engineering an ontology of governance at the blockchain protocol level. *ArXiv:1801:02027*. Retrieved from https://arxiv.org/abs/1801.02027

Kim, H. M., & Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. *Intelligent Systems in Accounting, Finance & Management*, *25*(1), 18–27. Retrieved from https://doi.org/10.1002/isaf.1424

Kim, H. M., Turesson, H., Laskowski, M., & Fard Bahreini, A. (2020a). Permissionless and permissioned, technology-focused and business needs-driven: Understanding the hybrid opportunity in blockchain through a case study of Insolar. *IEEE Transactions on Engineering Management*. 10.1109/TEM.2020.3003565

Kim, H. M., Laskowski, M., Zargham, M., Turesson, H., Barlin, M., & Kabanov, D. (2020b). *Token economics in real-life: Cryptocurrency and incentives design for Insolar's blockchain network*. IEEE Computer. (To be published).

Koulu, R. (2016). Blockchains and online dispute resolution: Smart contracts as an alternative to enforcement. *SCRIPTed*, *13*(1), 40–69. Retrieved from https://doi.org/10.2966/scrip.130116.40

Kugler, L. (2018). Why cryptocurrencies use so much energy—and what to do about it. *Communications of the ACM*, *61*(7), 15–17. Retrieved from https://doi.org/10.1145/3213762

Kumar, V. (2018). Transformative marketing: The next 20 years. *Journal of Marketing*, *82*(4), 1–12. Retrieved from https://doi.org/10.1509/jm.82.41

Lacity, M. C. (2018a). *A Manager's Guide to Blockchain for Business: From Knowing What to Knowing How*. Stratford-upon-Avon: SB Publishing.

Lacity, M. C. (2018b). Addressing Key Challenges to Making Enterprise Blockchain Applications a Reality. *MIS Quarterly Executive*, *17*(3), 201–222.

Lacity, M. C. (2020). *Blockchain Foundations for the Internet of Value*. Fayetteville: Epic Publishing and the University of Arkansas Press.

Lando, O. (1995). Assessing the role of the UNIDROIT principles in the harmonization of arbitration law. *Tulane Journal of International and Comparative Law*, *3*, 129–143.

Lapatinas, A. (2019). The effect of the Internet on economic sophistication: An empirical analysis. *Economics Letters*, *174*, 35–38. Retrieved from https://doi.org/10.1016/j.econlet.2018.10.013

Larios-Hernández, G. J. (2017). Blockchain entrepreneurship opportunity in the practices of the unbanked. *Business Horizons*, *60*(6), 865–874. Retrieved from https://doi.org/10.1016/j.bushor.2017.07.012

Laskowski, M., Kim, H. M., Zargham, M., Barlin, M., & Kabanov, D. (2019). *Token Economics in Real-Life: Cryptocurrency and Incentives Design for Insolar's Blockchain Network* (SSRN Scholarly Paper ID 3465085). Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=3465085

Leonard, D., & Treiblmaier, H. (2019). Can cryptocurrencies help to pave the way to a more sustainable economy? Questioning the economic growth paradigm. In H. Treiblmaier & R. Beck (Eds.), *Business Transformation through Blockchain – Volume II*. Cham: Palgrave Macmillan, 183-205.

Lipton, A., Sardon, A., Schär, F., & Schüpbach, C. (2020). Stablecoins, digital currency, and the future of money. In A. Pentland, A. Lipton, and T. Hardjono (Eds.), *Building the New Economy*, Cambridge: MIT Press.

Lessig, L. (1999). *Code: And Other Laws Of Cyberspace*. New York: Basic Books.

MacDonald, T. J., Allen, D. W. E., & Potts, J. (2016). Blockchains and the boundaries of self-organized economies: Predictions for the future of banking. In P. Tasca, T. Aste, L. Pelizzon, & N. Perony (Eds.), *Banking Beyond Banks and Money: A Guide to Banking Services in the Twenty-First Century*, Cham: Springer International Publishing, 279-296.

Malinova, K., & Park, A. (2016). Market design for trading with blockchain technology. *SSRN Electronic Journal*. Retrieved from https://doi.org/10.2139/ssrn.2785626

Martins, N. R. B., Angelica, A., Chakravarthy, K., Svidinenko, Y., Boehm, F. J., Opris, I., Lebedev, M. A., Swan, M., Garan, S. A., Rosenfeld, J. V., Hogg, T., & Freitas, R. A. (2019). Human brain/cloud interface. *Frontiers in Neuroscience*, *13*, 112. https://doi.org/10.3389/fnins.2019.00112

McDonald, M. (2017). Blockchain technology and the food supply chain. *Food & Beverage Industry News*, 40–41. Retrieved from https://www.foodmag.com.au/blockchain-technology-and-the-food-supply-chain-2/

McKinsey. (2016). *Global Payments 2016: Strong Fundamentals Despite Uncertain Times*. Retrieved from https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/A%20mixed%202015%20for%20the%20global%20payments%20industry/Global-Payments-2016.ashx

McNicol, M. L., & Thorsteinsson, E. B. (2017). Internet addiction, psychological distress, and coping responses among adolescents and adults. *CyberPsychology, Behavior & Social Networking*, *20*(5), 296–304. Retrieved from https://doi.org/10.1089/cyber.2016.0669

Meeks, B. N. (1997). Privacy lost, anytime, anywhere. *Communications of the ACM*, *40*(8), 11–13. https://doi.org/10.1145/257874.257876

Metcalfe, B. (2013). Metcalfe's law after 40 years of Ethernet. *Computer*, *46*(12), 26–31. https://doi.org/10.1109/MC.2013.374

Mizruchi, M. S., & Fein, L. C. (1999). The social construction of organizational knowledge: A study of the uses of coercive, mimetic, and normative isomorphism. *Administrative Science Quarterly*, *44*(4), 653–683. https://doi.org/10.2307/2667051

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. 1–9. Retrieved from https://bitcoin.org/bitcoin.pdf

Narayanan, A., & Clark, J. (2017). Bitcoin's academic pedigree. *Communications of the ACM*, *60*(12), 36–45. https://doi.org/10.1145/3132259

Närvänen, E., Kartastenpää, E., & Kuusela, H. (2013). Online lifestyle consumption community dynamics: A practice-based analysis. *Journal of Consumer Behaviour*, *12*(5), 358–369. https://doi.org/10.1002/cb.1433

North, D. C. (1991). Institutions, institutional change and economic performance. *Journal of Economic Perspectives*, *5*(1), 97–112.

Ostrom, E. (1990). *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge: Cambridge University Press.

Pedersen, A., Risius, M., & Beck, R. (2019). Blockchain decision path: When to use blockchains? Which blockchains do you mean? *MIS Quarterly Executive*, *18*(2), 1–17.

Rajan, D., & Visser, M. (2019). Quantum blockchain using entanglement in time. *Quantum Reports*, *1*, 3–11.

Reidenberg, J. R. (1998). Lex informatica: The formulation of information policy rules through technology. *Texas Law Review*, *76*(3), 553-593.

Rizzo, P. (2016, April 26). How Barclays used R3's tech to build a smart contracts prototype. *CoinDesk*. Retrieved from https://www.coindesk.com/barclays-smart-contracts-templates-demo-r3-corda

Rozas, D., Tenorio-Fornés, A., Díaz-Molina, S., & Hassan, S. (2018). *When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance.* Social Science Research Network, Retrieved from https://papers.ssrn.com/abstract=3272329

Savelyev, A. (2017). Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, *26*(2), 116–134. Retrieved from https://doi.org/10.1080/13600834.2017.1301036

Schneier, B. (2019). There's no good reason to trust blockchain technology. *Wired*. Retrieved from https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/

Scott, B. (2016). *How can cryptocurrency and blockchain technology play a role in building social and solidarity finance?* Working Paper 2016-1; UNRISD Working Papers. United Nations Research Institute for Social Development. Retrieved from http://www.unrisd.org/unrisd/website/document.nsf/(httpPublications)/196AEF663B617144C1257F550057887C?OpenDocument

Sedgwick, K. (2018). *No, Visa Doesn't Handle 24,000 TPS and Neither Does Your Pet Blockchain*. Retrieved from https://news.bitcoin.com/no-visa-doesnt-handle-24000-tps-and-neither-does-your-pet-blockchain/

Stafford, T. and Treiblmaier, H. (2020). Characteristics of a distributed ledger ecosystem for secure and sharable electronic medical records. *IEEE Transactions on Engineering Management* (Early Access), 1-23, 10.1109/TEM.2020.2973095

Sullivan, C., & Burger, E. (2017). E-Residency and blockchain. *Computer Law & Security Review*, *33*(4), 470–481. https://doi.org/10.1016/j.clsr.2017.03.016

Susskind, J. (2017). Decrypting democracy: Incentivizing blockchain voting technology for an improved election system. *San Diego Law Review*, *54*(4), 785–827.

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

Swan, M. (2017). Anticipating the economic benefits of blockchain. *Technology Innovation Management Review*, *7*(10), 6–13. Retrieved from https://doi.org/10.22215/timreview/1109

Swan, M. (2018). Blockchain economics: "Ripple for ERP". *European Financial Review*, 24–27.

Swan, M. (2019a). Blockchain economic networks: Economic network theory—Systemic risk and blockchain technology. In H. Treiblmaier & R. Beck (Eds.), *Business Transformation through Blockchain I*. Cham: Palgrave Macmillan.

Swan, M. (2019b). Blockchain theory of programmable risk: Black swan smart contracts. In M. Swan, J. Potts, T. Soichiro, F. Witte, & P. Tasca (Eds.), *Blockchain Economics: Implications of Distributed Ledgers: Markets, Communications Networks, and Algorithmic Reality*, Singapore: World Scientific Publishing Co. Pte. Ltd, 171-194.

Swan, M. (2020a). *B/CI: Quantum computing, Holographic control theory, and blockchain IPLD for brain*. Preprint. CRC Press. Retrieved from https://www.researchgate.net/publication/342184271_BCI_Quantum_Computing_IPLD_for_Brain.

Swan, M. (2020b). Black hole zero-knowledge proofs. FQXi undecidability, uncomputability, and unpredictability essay contest entry. Retrieved from https://www.researchgate.net/publication/342184205_Black_Hole_Zero-Knowledge_Proofs.

Swan, M., & De Filippi, P. (2017). Toward a philosophy of blockchain: A symposium: Introduction. *Metaphilosophy*, *48*(5), 603–619. https://doi.org/10.1111/meta.12270

Swan, M., dos Santos, R. P., & Witte, F. (2020). *Quantum Computing: Physics, Blockchains, and Deep Learning Smart Networks*. Singapore: World Scientific.

Szabo, N. (1996). Smart contracts: Building blocks for digital free markets. *Extropy Journal of Transhuman Thought*, *16*, 1–10.

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

Toth, O. (2017). *The Lex Mercatoria in Theory and Practice*. Oxford: Oxford University Press.

Treiblmaier, H. (2018a). Paul Feyerabend and the art of epistemological anarchy—A discussion of the basic tenets of 'Against Method' and an assessment of their potential usefulness for the information systems field. *The DATA BASE for Advances in Information Systems*, *49*(1), 93–101. https://doi.org/10.1145/3229335.3229342

Treiblmaier, H. (2018b). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. *Supply Chain Management: An International Journal*, *23*(6), 545–559.

Treiblmaier, H. (2019) Toward more rigorous blockchain research: Recommendations for writing blockchain case studies, *Frontiers in Blockchain*, 2, Article 3, 1-15.

Treiblmaier, H., & Umlauff, U. (2019). Blockchain and the future of work: A self-determination theory approach. In M. Swan, J. Potts, S. Takagi, F. Witte, & P. Tasca (Eds.), *Blockchain Economics: Implications of Distributed Ledger Technology*, Singapore: World Scientific, 105-124.

Turesson, H., Laskowski, M., Roatis, A., & Kim, H. M. (2019). Privacy-preserving blockchain mining: Sybil-resistance by Proof-of-Useful-Work. *Journal of Database Management*, *under review* (arXiv:1907.08744 [cs.CR]).

van Hoek, R., Fugate, B., Davletshin, M., & Waller, M. A. (2019). *Integrating Blockchain into Supply Chain Management: A Toolkit for Practical Implementation*. London: Kogan Page.

van Wegberg, R., Oerlemans, J.-J., & van Deventer, O. (2018). Bitcoin money laundering: Mixed results? *Journal of Financial Crime*, *25*(2), 419–435. Retrieved from https://doi.org/10.1108/JFC-11-2016-0067

Voshmgir, S. (2017). Disrupting governance with blockchains and smart contracts. *Strategic Change*, *26*(5), 499–509. https://doi.org/10.1002/jsc.2150

Wieck, M. (2017). *Marie Wieck, GM of IBM Blockchain, speaking at Consensus 2017*. Retrieved from https://ibmgo.com/interconnect2017/search/?q=blockchain&tags=all&categoryType=video

Williamson, O. E. (1975). *Markets and Hierarchies, Analysis and Antitrust Implications*. New York: The Free Press.

Williamson, O. E. (1991a). Strategizing, Economizing, and Economic Organization. *Strategic Management Journal*, *12*(S2), 75–94. https://doi.org/10.1002/smj.4250121007

Williamson, O. E. (1991b). Comparative Economic Organization: The Analysis of Discrete Structural Alternatives. *Administrative Science Quarterly*, *36*(2), 269–296. https://doi.org/10.2307/2393356

Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia, *Social Science Research Network*, Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

About the Authors

Horst Treiblmaier is a Professor and Head of the Department of International Management at MODUL University Austria. He received a Ph.D. in Management Information Systems in 2001 from the Vienna University of Economics and Business in Austria and has worked as a Visiting Professor at Purdue University, University of California, Los Angeles (UCLA), University of British Columbia (UBC), University of Technology in Sydney (UTS) and the Kazakhstan Institute of Management, Economics and Strategic Research (KIMEP). He has more than fifteen years of experience as a researcher and consultant and has worked on projects with Microsoft, Google, and the United Nations Industrial Development Organization (UNIDO).

Melanie Swan is a Research Associate at the UCL Centre for Blockchain Technologies, a Technology Theorist in the Philosophy Department at Purdue University, and a Singularity University faculty member. She is the founder of several startups including the Institute for Blockchain Studies, DIYgenomics, GroupPurchase, and the MS Futures Group. Melanie's educational background includes an MBA in Finance from the Wharton School of the University of Pennsylvania, an MA in Philosophy from the New School for Social Research in New York NY, and a BA in French and Economics from Georgetown University. She is the author of the best-selling book *Blockchain: Blueprint for a New Economy*.

Primavera De Filippi is a permanent researcher at the National Center of Scientific Research (CNRS) in Paris, a faculty associate at the Berkman Klein Center for Internet & Society at Harvard University, and a Visiting Fellow at the Robert Schuman Centre for Advanced Studies at the European University Institute. She is a member of the Global Future Council on Blockchain Technologies at the World Economic Forum, and co-founder of the Internet Governance Forum's dynamic coalitions on Blockchain Technology (COALA). Her fields of interest focus on legal challenges raised by decentralized technologies, with a particular focus on blockchain technologies. She is investigating the new opportunities for these technologies to enable new governance models and participatory decision-making through the concept of governance-by-design.

Mary C. Lacity is a Walton Professor of Information Systems and Director of the Blockchain Center of Excellence in Sam M. Walton College of Business at The University of Arkansas. She was previously Curators' Distinguished Professor at the University of Missouri-St. Louis. She has held visiting positions at MIT, the London School of Economics, Washington University, and Oxford University. She is a Certified Outsourcing Professional®, Industry Advisor for Symphony Ventures, and Senior Editor for MIS Quarterly Executive. Her recent research focuses on improving business services using Robotic Process Automation (RPA), Cognitive Automation (CA), and Blockchain technologies.

Thomas Hardjono is the CTO of Connection Science and Engineering. He leads technical projects and initiatives around identity, security and data privacy, and engages industry partners and sponsors on these fronts. He is also the technical director for the Internet Trust Consortium under MIT Connection Science that implements open source software based on cutting edge research at MIT. The consortium embodies the MIT philosophy of giving back to the community. As part of the MIT outreach to industry, Thomas is active in a number of industry associations and standardization bodies. These include IETF, IEEE, Kantara, OASIS, TCG and OIC. Throughout his 20 year career in the computer and network security industry Thomas has primarily been engaged in advancing new technologies, working in various CTO offices and advances engineering groups.

Henry Kim is an Associate Professor at the Schulich School of Business, York University in Toronto, and is the Director for blockchain.lab at Schulich. As one of the leading blockchain scholars in Canada, he has authored more than 30 publications on blockchain topics and over 70 overall. Prof. Kim is engaged in blockchain research projects with Toronto and Region Conservation Authority (on electricity micro-grid), the Swiss blockchain startup Insolar (on hybrid blockchains and token economics), Ontario Ministry of Agriculture and Rural Affairs (on food traceability), Don Tapscott's Blockchain Research Institute (on commercial insurance) and many others. He is the co-organizer

for the Fields Institute Seminar Series on Blockchain and the 2020 IEEE Conference on Blockchain and Cryptocurrencies, and speaks and consults broadly on Digital Transformation.

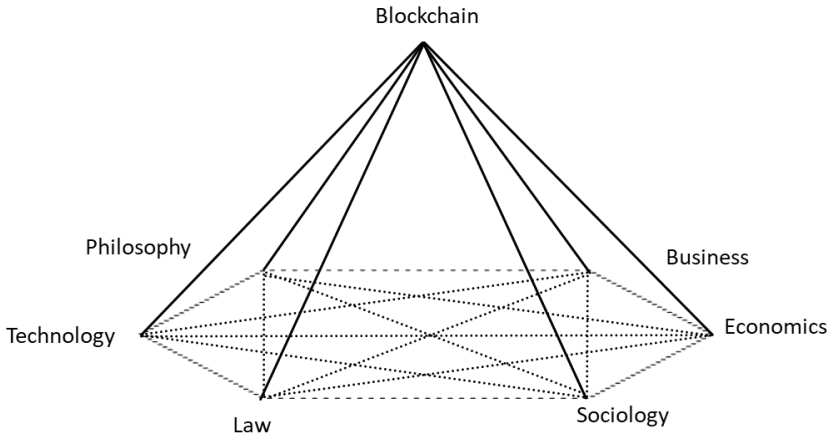

Figure 1. Views on Blockchain

Table 1. Strategic Intents of Blockchain Applications (cf., Lacity et al. (2018a))

	Sustaining Innovations	Disruptive Innovations	Ecosystem Innovations
Strategic Intent	Strengthen the current business model by improving the performance of existing products and services to better serve today's high-end customers	Build a new business model to sell to under-served customers or to create a new market where none exists	Coordinate transactions among trading partners to benefit all parties
Locus of Control	The enterprise	The enterprise	Shared among trading partners
Blockchain Examples	• Cross-division transactions within a global enterprise • Cross-border payments between current clients	• Solar energy sharing • Additive manufacturing • Electric car charge sharing	• Pharmaceutical tracking • Food provenance • Trade finance • Shipping container tracking

Table 2. Business Areas and Related Research Questions

	Description	(Exemplary) Research Questions	Exemplary sources
Strategic Management	Companies need to make strategic decisions which consider the external environment (including technological change) as well as their internal resources.	*RQ1:* What are the determinants of successful sustaining, disruptive and ecosystem innovations based on blockchain? *RQ2:* Will some of our most reified theories be corroborated, adapted or refuted in context of blockchains' distributed nature? *RQ3:* Does blockchain necessitate a new theory on ecosystems?	(Jacobides et al., 2018)
Accounting	Blockchain applications promise to eliminate the need for accounting reconciliations since trading partners share one version of the truth. It is a "confirm as you go" rather than "confirm after the fact" model.	*RQ4:* How will the audit function change? *RQ5:* Are blockchains more secure as compared to traditional ledgers? *RQ6:* How will blockchains impact the risk profiles required in accounting reports?	(Coyne & McMickle, 2017; Dai & Vasarhelyi, 2017)
Supply Chain Management	Blockchain applications promise to provide instant status, asset authenticity, and track & trace through an asset's entire life cycle.	*RQ7:* What new tools and theories are needed to explain and guide the design of blockchain-enabled supply chains?	(Treiblmaier, 2018b; van Hoek et al., 2019)
Information Systems	Blockchains are designed to be shared applications, prompting research questions about ideal use cases, firm and individual adoption.	*RQ8:* How can information system be designed that capitalize on the strengths of decentralized ledgers? *RQ9:* What factors foster and inhibit the adoption of blockchain-based information systems?	(Clohessy et al., 2019; Lacity, 2018b; Pedersen et al., 2019)
Finance	Digital assets represent a new asset class, unlocking new financing models such as Initial Coin Offerings (ICOs), Security Token Offerings (STOs), and Initial Exchange Offerings (IEOs).	*RQ10:* How will blockchains impact corporate finance? *RQ11:* What are emerging funding models and how do they affect investor risks?	(Adhami et al., 2018)
Marketing	Blockchains are creating new models for advertising where individuals, rather than companies, can grab the advertising revenues from the value of their own data.	*RQ12:* How will blockchains change marketing practices, particularly if individuals gain self-sovereignty over their data?	(Kumar, 2018)

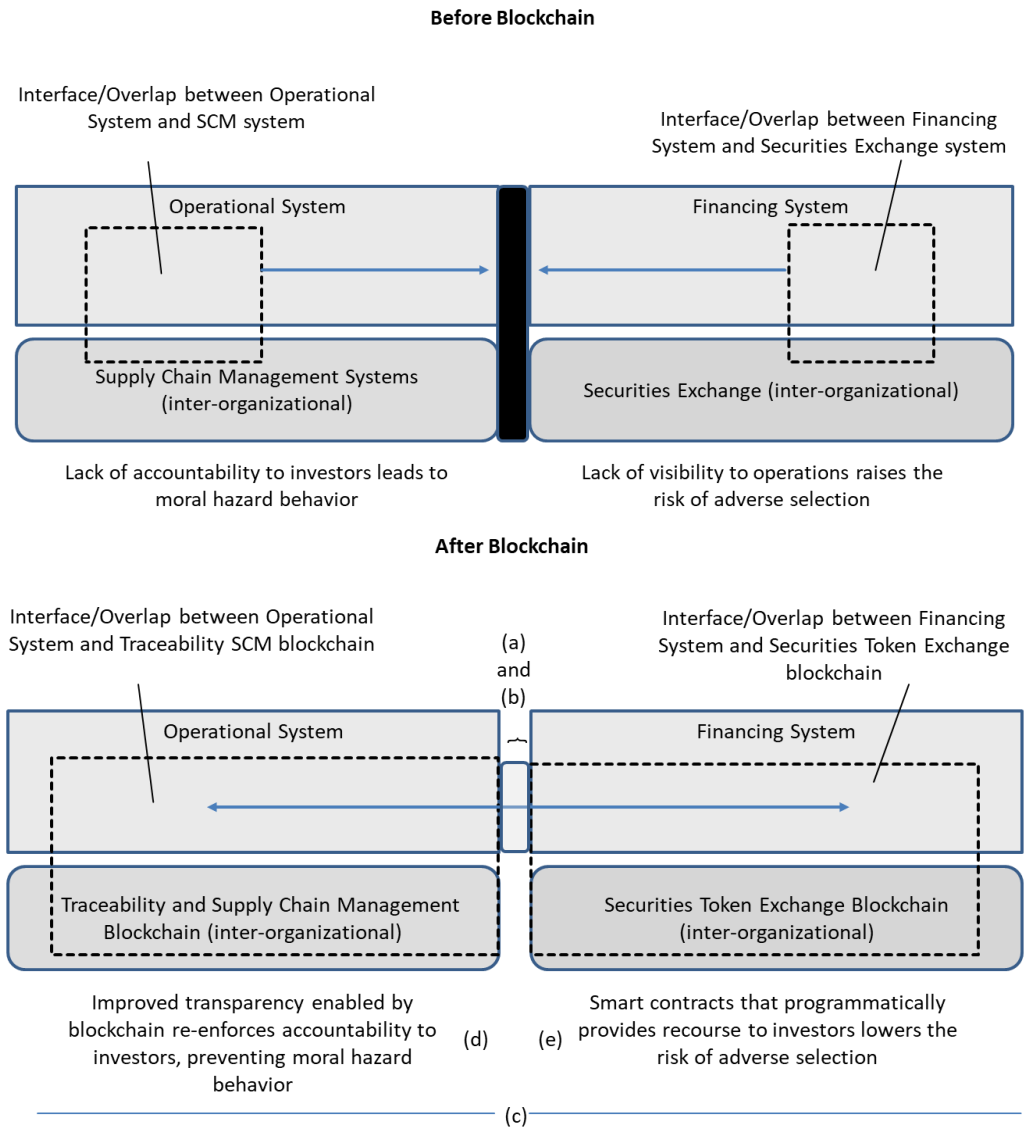

Figure 2: Operations and Financing Systems Before and After Blockchain

Table 3. Integrating Operations and Finance with Blockchain

	Research Question	Method
(a)	*RQ14:* How can data and the semantics defining and constraining that data be interoperated between operations and financing blockchains? (Kim et al., 2018)	Engineering ontologies
(b)	*RQ15:* When data and semantics are inter-operated from one blockchain to another, how can it be demonstrated that a fair consensus as to whether an inter-operation is valid was achieved? (Kim et al., 2020a) *RQ16:* Given that historically achieving consensus on blockchain required excessive use of CPU cycles across networks like Bitcoin and Ethereum, is there a mechanism where CPU cycles are not wasted but rather used to solve a meaningful problem? (Turesson et al., 2019)	Framework specification
(c)	RQ17: How can a testbed agent-based simulation environment be used to test out different configurations of integrating operations and financing blockchains? (Kim et al., 2020b; Laskowski et al., 2019)	Agent-based modeling
(d)	*RQ18:* How can a traceability ontology as well as other ontologies be refined so that they can be used as an implementation-independent specification of semantics that then can be semiautomatically converted into smart contracts that can be used to provide diagnostics for provenance tracking and surveillance for investor oversight? (Kim & Laskowski, 2018b; Kim et al., 2018)	Ontologies
(e)	*RQ19:* How can a prototype of some class of smart contracts that will serve as programmatic conditions on security tokens on the financing blockchain be developed? (Malinova & Park, 2016; Chod et al., 2018; Kim & Laskowski, 2018)	Feasibility analysis

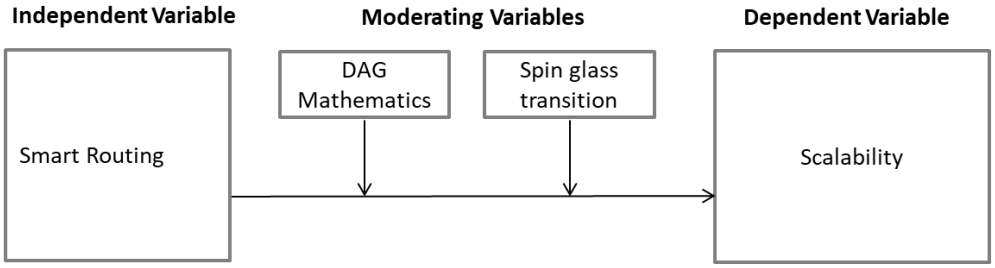

Figure 3. Theoretical Spin Glass Model for Blockchains (DAG written as an energy optimization)

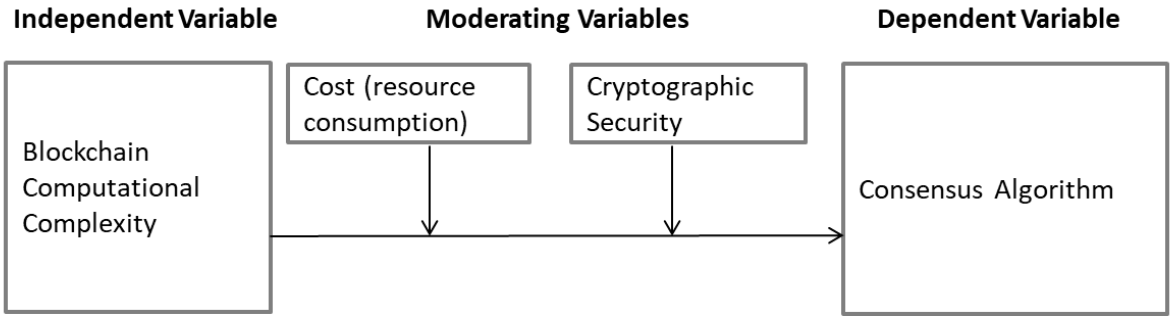

Figure 4. Consensus: Blockchain Computational Complexity facilitates Efficient Consensus