2019

Is Blockchain the Next Step in the Evolution Chain of [Market] Intermediaries?

Marcela Gomez
University of Pittsburgh - School of Information Sciences, mmg62@pitt.edu

Pedro Bustamante
University of Pittsburgh - School of Information Sciences, Students, pjb63@pitt.edu

Martin B. H. Weiss
University of Pittsburgh - School of Computing and Information, mbw@pitt.edu

Ilia Murtazashvili
University of Pittsburgh - Graduate School of Public and International Affairs, ilia.murtazashvili@gmail.com

Michael J. Madison
University of Pittsburgh - School of Law, madison@pitt.edu

See next page for additional authors

Recommended Citation
Marcela Gomez, Pedro Bustamante, Martin B. Weiss, Ilia Murtazashvili, Michael J. Madison, Wilson Law, Tymofiy Mylovanov, Herminio Bodon & Prashabnt Krishnamurthy, *Is Blockchain the Next Step in the Evolution Chain of [Market] Intermediaries?*, TPRC47: The 47th Research Conference on Communication, Information and Internet Policy (2019).
Available at: https://scholarship.law.pitt.edu/fac_articles/403

Is blockchain the next step in the evolution chain of [market] intermediaries?

Marcela M. Gomez[1] mmg62@pitt.edu
Pedro J. Bustamante[1] pjb63@pitt.edu
Martin M. Weiss[1] mbw@pitt.edu
Ilia Murtazashvili[2] ilia.murtazashvili@pitt.edu
Michael Madison[3] madison@pitt.edu

Wilson Law[4] wilson_law@baylor.edu
Tymofiy Mylovanov[5] tym10@pitt.edu
Herminio Bodon[1] hdb15@pitt.edu
Prashant Krishnamurthy[1] prashk@pitt.edu

[1] Department of Informatics and Networked Systems, School of Information Sciences, University of Pittsburgh, Pittsburgh, PA 15260
[2] Graduate School of Public and International Affairs, University of Pittsburgh, Pittsburgh, PA 15260
[3] School of Law, University of Pittsburgh, Pittsburgh, PA 15260
[4] Department of Economics, Baylor University, Waco, TX 76798
[5] Department of Economics, University of Pittsburgh, Pittsburgh, PA 15260 – Honorary President of the Kyiv School of Economics, Kyiv, Ukraine – Deputy Chairman of the Council of the National Bank of Ukraine, Kyiv, Ukraine

Introduction

The blockchain is a decentralized solution for handling transactions where we are concerned (among other aspects) with the accuracy and verification of transactions. One of its main promises is to eliminate the need for centralized entities or intermediaries and legal enforcement. Rather than trusting self-interested human intermediaries, the blockchain provides an alternative that relies on transparent computational protocols (Werbach 2018).

In this paper, we delve into this *broker-less* claim and analyze whether the blockchain needs an intermediary to allow for widespread access to its functionality and whether the blockchain itself is an intermediary. The latter would turn the blockchain into a new type of middleperson that constitutes a shift in trust from humans or traditional agents to computer code. In other words, the next step in the evolution chain of intermediaries from humans to machines.

The overall goal of this paper is to get the discussion started on the relationship between the blockchain and intermediaries so that we can think of plausible policy, governance, and regulatory measures to address the shortcomings and increase the opportunities for the widespread adoption of the blockchain technology in its different areas of impact. We begin by providing an overview of the workings of the blockchain before shifting our focus to an economic analysis of blockchain, where we argue that the economics literature has yet to explicitly consider blockchain as a transformative intermediary. We then explore situations in which the blockchain acts as a middleperson, as well as those where it requires an intermediary. We conclude by reflecting on the different issues that the blockchain-intermediary link entails in the policy domain.

Background

An Overview of Blockchain

Architecture

Most blockchain-based platforms implement a replicated, shared, and distributed (i.e., decentralized) ledger.[1] The decentralized nature of the ledger allows the transfer of digital tokens associated with assets (e.g., cryptocurrencies) at a distance without a trusted third party.[2] To accomplish this, every user in the system has a full copy of the ledger and the network makes sure that every user's copy reflects the current *state of the world* (i.e., the up-to-date state of the system) (Brown 2015).

The best analogy of this implemented ledger is a secure form of a database of records (i.e., transactions) that is decentralized (transactions conducted in a peer-to-peer manner), persistent (each transaction is broadcasted to the whole network), immutable (no transaction can be modified and/or deleted), and secure (all data is cryptographically secure). This form of database is constructed as a log of records batched into time-stamped blocks, which are recognized by a unique identifier.[3] Each block points to the identifier of the previous block (i.e., the parent block), constructing in this manner a chain of blocks, and hence receives the name of blockchain (see Fig. 1). The first block in the chain is known as the *genesis* block, it has no parent block and it is common to the whole network (Nakamoto 2008).

---

[1] A ledger is a file recording and totaling transactions, with debits and credits in separate columns and a beginning and ending balance (Garrison 2010).
[2] As we explore in this paper, the technology behind blockchain can in itself be a trusted third party. Hence, we can reasonably assume that blockchain is acting as the replacement of the trusted third-party.
[3] The result of a cryptographic hash or digesting function.

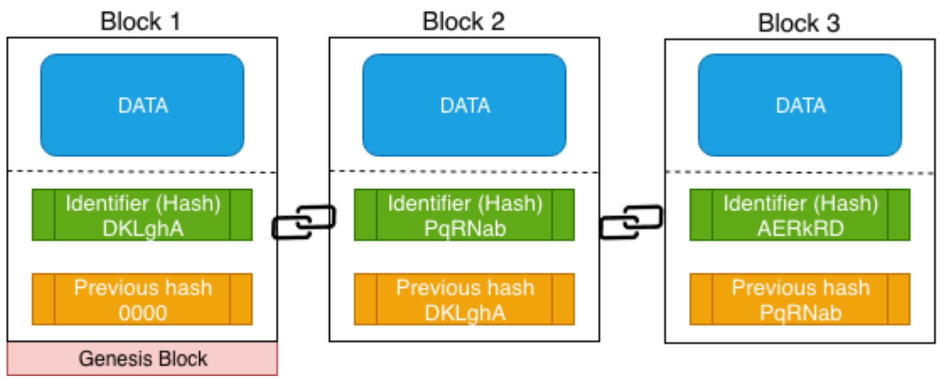

Figure 1: Blockchain Architecture

Taxonomy of Blockchain Platforms

In the literature there are multiple ways to categorize a blockchain-based platform: by the type of digital asset (e.g., cryptocurrency), by their support of smart contracts, etc. Nonetheless, the most common way to categorize a blockchain platform is by the access rights to the network (see Table 1), so that platforms are classified into private, consortium, and public blockchains (Crosby 2016). In a public or permissionless blockchain, such as Bitcoin or Ethereum, there are no access restrictions to the network. In other words, anyone can join the system. On the other hand, in a private or permissioned blockchain, only a limited number of users can access the network, where older users exercise access control of new participants. Finally, in a hybrid or consortium[4] blockchain, instead of allowing anyone to access the system or to have a single user/company to have full access control, a few selected nodes perform the most important functions in the platform, including network access control (Buterin 2015).

	Private	**Consortium**	**Public**
Access rights	Restricted	Restricted but more flexible	Open (no restrictions)
Read privileges	Restricted	Usually restricted	Open (no restrictions)
Centralization	Yes	Partial	No
User's identity	Known	Known/ Pseudonyms	Anonymous/Pseudonyms
Asset	Any	Any	Platform-native
Examples	Hyperledger	Riple & Multichain	Bitcoin & Ethereum

Table 1: Blockchain Taxonomy by access rights

[4] A hybrid/consortium blockchain takes characteristics from both public and private platforms.

Applications of Blockchain

The most common example of blockchain is, without a doubt, Bitcoin. The platform was the first to implement a blockchain based on the ideas of Satoshi Nakamoto in 2009 (Nakamoto 2008). Further, Bitcoin is considered the first cryptocurrency platform to enjoy commercial success, with a maximum market capitalization of over $300 billion dollars in December of 2018 (Coinmarket 2018). Nonetheless, it is not, by any means, the only available blockchain-based cryptocurrency. In fact, nowadays there exist over 2,000 different cryptocurrencies in circulation using different types of platforms (Coinmarket 2019). However, with the emergence of new platforms, such as Ethereum, Hyperledger Fabric, Ripple, etc., and the development of smart contracts,[5] a considerable number of new applications are being developed, deployed, and used on top of the blockchain (Brown 2015) (See Table 2[6]).

	Application	Description	Examples
Financial Applications	Private Securities	Issue stock exchange shares via the Blockchain to be purchased and sold in a secondary market sitting on top of the blockchain.	NASDAQ Private Equity and Chain (Chain 2019)
			Medici (Kelleher 2014)
			Blockstream (Churchbase 2019)
	Real Estate	The blockchain could ensure that the buyer gets the title and a seller gets the cash (e.g., cryptocurrency). In addition, the blockchain also records the title and all required documentation, while giving financing options to the buyer.	B11G group (B11G 2019)
	Insurance	Property, digital or physical, could be registered on the blockchain. Further, ownership and transaction history could be validated by any user, particularly insurance companies	Everledger - Diamond certification (Roberts 2017)
	Public Notary	Verifying document authenticity: Proof of Ownership, Proof of Existence, Proof of	Stampery (Dillet 2015)

[5] Smart contracts are registered code (i.e., scripts) in the blockchain in the form of agreements (i.e., contractual clauses), which are executed when certain conditions are met in an automatic, self-enforced, and self-adjudicated manner (Christidis 2016).
[6] These are merely a few examples of usage of blockchain and smart contracts.

Non-financial Applications		Integrity, and transfer of ownership.	Ascribe (Gautham 2015)
			Block Notary (Blocknotary 2019)
	Storage	Peer-to-peer (P2P) distributed cloud storage that allows users to transfer and share data without relying on a third-party provider (e.g., Dropbox)	Storj (Vaughan-Nichols 2017)
			FileCoin (Bitcoin 2018)
			SiaCoin (Evans 2018)
	Anti-counterfeit	Brands, merchants, and marketplaces could be part of a blockchain network to store and validate data about the authenticity of the products	Block verify (Hulseapple 2018)
			SimplyBrand (Simplybrand 2018)
Internet Applications	Domain Name Service (DNS)	A decentralized version of the traditional Domain Name Services (DNS)	Namecoin (Holman 2019)
	Crowdsourcing	Crowdsourcing applications can be built using the blockchain and smart contracts.	CrowdPrecisions (Crowdprecision 2018)
Government	Elections	Encrypted votes where private individuals can confirm that their votes were counted and who they voted for	Block Party (Jones 2018)
	Record management	Using blockchain to keep records (e.g., birth and death dates, marital status, property transfers, etc.)	Illinois Blockchain Initiative (Illinois 2017)
Other Applications	Energy Markets	Trading energy (e.g., solar) locally in a peer-to-peer manner.	Brooklyn Microgrids (Cardwell 2017)
	Internet of Things (IoT)	Provide access to data that is generated by IoT devices. Customers could decide who can purchase their IoT generated data[7].	Tilepay Coin (Ftreporter 2017)
	Healthcare	Secure medical records. Better sharing mechanisms for medical records, clinical trials, and health data.	Estonian eHealth Foundation (Einaste 2018)

Common Challenges to Blockchain

As is the case with the benefits from blockchain-based platforms, the challenges are also highly dependent on the characteristics of the platform: different types of

[7] Additional projects are being developed for the Internet of Things using blockchain and smart contracts. Additional examples can be found in the work by Christidis (2016).

blockchain (e.g., public vs. private), using different consensus algorithms (e.g., Proof of Work), with different network configurations (e.g., free vs. open access), etc., face different types of problems. Nonetheless, the literature has identified at least six general risks that can are highly associated with most blockchain platforms (Chalker 2018).

- **Scalability**: In many blockchain-based systems, particularly public platforms, the biggest challenge is to overcome the scalability issues. The goal is to process as many transactions as possible as fast as possible. Nonetheless, in many platforms, there are limitations for the frequency with which new blocks are appended to the chain.[8] In addition, for many consensus mechanisms, the time required to reach a consensus is very high.
- **Data Privacy:** A key characteristic in blockchain is that all transactions are broadcasted to the whole network. In fact, most of the time, every user in the network has a full copy of the ledger containing all the details of the executed transactions in the system. Consequently, this transaction transparency can represent a significant issue for applications dealing with sensitive information.
- **Decentralized Nature:** Most blockchains can act as Decentralized Autonomous Organizations (DAOs). This organization brings legal questions that are not straightforwardly answered: Who is responsible if laws are broken? What, if any, is the liability of DAOs? How to deal with malicious nodes? Who or what is claimed against in the case of a legal dispute? How soft and hard forks are introduced into the system? etc.
- **Jurisdiction:** Most blockchain platforms do not rely on a centralized, trusted third-party. Moreover, the nodes responsible for the main functionalities of the system are usually spread around the world. This situation arises complex jurisdictional issues that require careful consideration when dealing with relevant contractual relationships.
- **Encryption:** Cryptographic tools provide a very powerful instrument to blockchain to convert it into a secure platform. Nonetheless, the usage of encryption in most blockchain processes has also some drawbacks. For instance, anyone with the encryption key is able to read the encrypted data, if the key is stolen or made public. In addition, for most platforms, if the encryption key is lost, the user can never get it back.
- **Service Level Agreements and Performance:** Most blockchain implementations are highly dependent on node and communication availability. Consequently, one can foresee some challenges for guarantees regarding availability and performance from vendors offering *blockchain-as-a-service* and the services based on these platforms.

[8] For instance, in Bitcoin the average time to mine a block (i.e., append it to the chain) is 10 minutes (DataBitcoin).

Beyond these risks, since the users are in control of crucial tasks such as validation and verification of blocks and transactions, many other situations could emerge and impact the normal operations of the blockchain network. The most common threats come from potential collusion situations. Thus, blockchain platforms could be susceptible to the 51% attack,[9] sybil attacks, mining centralization, etc. (Watanabe 2016). Beyond these organizational risks, blockchain depends on the security of its cryptography, which is itself vulnerable to paradigmatic shifts in computing, especially quantum computing (Fedorov 2018 et al 2018).

The Economics of Blockchain

Prior to 2008, all ledgers were centralized and controlled by governments and firms, including functions such as recording information about goods and services, standardization, maintaining a monetary system, collection of taxation, recording property ownership, and maintaining repositories of information about identities of individuals and groups in society. Many of these tasks are considered critical public goods necessary for the functioning of capitalist economies (Allen 2011, Hodgson 2015; Deakin *et al.* 2017). However, centralized recording creates challenges because the entity recording information may be more powerful than others in society (in the case of the state) and there are often incentives to hide, change, or manipulate information (in both the case of the state and firms).[10]

The blockchain promises to remove many of these functions from states or firms. This transformative function led Davidson, De Filippi, and Potts (2018) to claim that the blockchain is an institutional technology the stands alongside firms, markets, and relational contracting. Accordingly, the economic analysis of blockchain brings together insights from the theory of the firm (Coase 1937), the use of knowledge in society and spontaneous order (Hayek 1945, 1948), the study of the commons (Ostrom 1990), polycentric governance (Ostrom 1994), incomplete contracting (Williamson 1996), and collective choice, including analysis of the choice of rules, exit and voice (Hirschman 1970; Brennan and Buchanan 1985).

There are several domains where the blockchain is potentially transformative, including contracting among firms. Williamson (1975, 1985) analyzed the relationship of trust to

---

[9] Where users are able to collude to gain the majority (i.e., 51%) of the computing power or the total assets in the network. Consequently, they could control the validation of blocks in the case of most Proof-based consensus algorithms (Bano 2017).

[10] Orwell's "1984", though fictional, illustrates the social and political incentives for manipulating information.

contracting through the concept of "opportunism with guile." Trust facilitates contracting, but even with trusting relations, there is a possibility of exploitation of those trusting relations. Formal contract law can address opportunism with guile (La Porta *et al.*, 1999; La Porta, Lopez-de-Silanes and Shleifer, 2008), though as Macaulay (1963) recognized, most business people do not use formal contract law to settle disputes. Landa (1981) showed that under the assumptions of contract uncertainty and positive transaction costs, traders rank other traders according to their trustworthiness. Accordingly, blockchain, by reducing the need for trust, can reduce the necessity of formal contract law or relational (e.g., ethnic) networks, although contract law is required at some level to implement and adopt blockchain in the first place.

Blockchain can also transform the relationship between citizens and the state. According to Buchanan (1975), the government has a protective function (coercion) and productive function (providing public goods). The two fundamental dilemmas of government are that it may be unable to commit to limits on its authority, or what Weingast (1995, 1997) calls the "sovereign's dilemma," and it may not know what public goods citizens want, which Hayek (1945) called the "knowledge problem." One way that blockchain can limit the state is through DAOs, which provide a potentially radical ability to self-govern, including with crypto-democracy (Allen *et al.*, 2018).[11] Blockchain can strengthen the state's ability to complete its productive functions, including improving the transparency, accuracy, and efficiency government functions, with applications to tax collection, delivery of public services, digital citizen identity, land registry management, and public records, especially in developing contexts where the government lacks credibility (Reinsberg, 2018).

Third, blockchain affects the sharing/innovation/knowledge commons. Allen and Potts (2016) and Potts (2018, 2019) consider the "innovation commons," which refers to self-organizing groups developing rules under conditions of uncertainty. The innovation commons pools distributed information about uses, costs, problems, and opportunities to new technologies. In this case, the commons refer to the pool of resources about the application of technology. Blockchain, like any knowledge commons, may require governance to function effectively; it may also be the basis for scaling up the knowledge commons to truly global levels.

The Functions of Market Intermediaries

In contrast with Davidson, De Filippi, and Potts (2018), who focus on blockchain as an institutional technology, we consider whether it is the next step in the evolution of

[11] We emphasize on the "potentially" aspect of this claim, as The DAO has faced its own constraints, even when the underlying code has followed the rules it was supposed to. It has proven to be vulnerable to attacks, hence forcing modifications to a system that was conceived as immutable (Werbach, 2018).

intermediaries: a new, trustless intermediary. Economics has long had a role for middlepersons who bring together buyers and sellers. Yet there is a diversity of functions served by these intermediaries. Since we are also interested in whether the blockchain eliminates the need for intermediaries in the traditional sense, or whether it in fact needs intermediaries, it is necessary to consider these functions of intermediaries.

The need for intermediaries stems from transaction costs and asymmetric information (Allen and Santomero, 1999). These issues affect a large range of domains, which translate into different types of intermediaries that are in charge of fulfilling different functions.

According to Krakovsky (2015), according to its functions, a middleperson can be classified within six categories:

1. **Bridge**: An intermediary whose role is to reduce the “physical, social, or temporal distance” between buyers and sellers. In this way, a bridge is capable of finding transacting opportunities between two disconnected sets of agents.
2. **Certifier**: A certifier reduces the asymmetry of information between buyers and sellers by screening the available options, and scouting for the buyers’ requirements. Then, this intermediary uses its own reputation to endorse its findings. Both buyers and sellers rely on these valuations, which can potentially enable both parties to maintain their credibility.
3. **Enforcer**: This type of intermediary makes sure that “buyers and sellers put forth full effort, cooperate and stay honest”. In this way, enforcers are concerned with designing and applying rules that add value to the network, as well as using threats of punishment to ensure compliance.
4. **Risk Bearer**: A risk bearer’s role is to reduce uncertainty for both negotiating parties. Such intermediaries are better than their trading partners at bearing risks and actually earn a premium for doing so. These intermediaries should be able to manage internal and external risks, including by developing management skills.
5. **Concierge**: A concierge helps a consumer to perform certain tasks such as buying a house, booking travel, buy or sell cars, among others. These intermediaries provide value to consumers by understanding their needs and pricing their services “with consumers’ ever-changing alternatives in mind”.
6. **Insulator**: An insulator’s function is to limit the flow of information between two parties, when this communication may be detrimental for their partnership, relationship, etc.

In a broader sense, a middleperson is a *matchmaker* whose function is to match buyers to sellers (e.g., real estate agents, services like Uber). Other intermediaries perform a technical function leveraging skills or information that consumers don't usually possess, e.g., lawyers and accountants. The function of these intermediaries can also be understood as reducing intellectual barriers (i.e., transaction costs arising from lack of expertise) that consumers need to overcome in order to successfully participate in a given transaction. Other intermediaries are bookkeepers e.g., stock traders, bank tellers, etc. These functions resonate with the blockchain context, as these intermediaries are candidates for replacement by a blockchain.

Catalini and Gans (2016) argue that from a market perspective, trusted intermediaries help participants verify and audit transaction attributes. This is particularly useful when we are dealing with commodities that are not entirely fungible, as well as when the search space would require significant efforts to find appropriate commodities. In exchange for these services, a middleperson charges fees and may take advantage of the information they obtain from observing all the transactions that are carried out within a marketplace.

Negative consequences stem from the combination of informational advantage with network effects and economies of scale, which translates into market power,[12] and potential control over market participants that intermediaries can gain. Thus, the more indispensable intermediaries become, the higher their potential to manage information on participants, resources, prices, etc., which increases the impact they can have on resulting outcomes. Misaligned incentives can be another type of problems, e.g., real estate agents prefer to sell homes faster than for higher prices (Levitt and Syverson 2008).

Is Blockchain a Superior Intermediary?

As pointed out by Catalini and Gans (2016), blockchain networks are better suited for applications relying on digital (and online) information. When the information is not digital in nature, blockchain-based applications may not scale.

To better illustrate the relationship between intermediaries and the blockchain, we focus on two questions that frame this relationship: 1) (When) is the blockchain an intermediary? and 2) When does the blockchain require an intermediary?

(When) Is the Blockchain an intermediary?

To understand when the blockchain may act as an intermediary, it is useful to return to the functions of intermediaries as discussed above. Note that Krakovsky (2015) is

[12] Market power can be translated into higher prices, high switching costs, single points of failure, reduce privacy, user lock-in, censorship risks, among others (Catalini and Gans, 2016).

explicitly concerned with intermediaries who are human and, therefore, who have a tendency to respond to their own incentives. Because blockchains are code operating on computers,[13] the extent to which they can have agency is highly restricted, which narrows the kinds of intermediary functions they can perform.

Intermediary functions for which blockchains are suited

Blockchain as a Certifier: A certifier reduces the asymmetry of information between buyers and sellers. Transacting parties using a blockchain explicitly rely on this function; it is a central way in which blockchains may act as an intermediary.

Blockchain as a Risk Bearer: These intermediaries are better than their trading partners at bearing risks and may earn a premium for doing so. Risk management may be done in a variety of ways, including diversification and explicit risk management vehicles (e.g., financial options). In the case of cryptocurrencies, risk bearers can handle the volatility of these assets. As a distributed ledger, blockchains do not have this capability. However, applications written on the chain against smart contracts may be able to perform some risk management functions, so that this role of blockchains as an intermediary may be a possibility in some circumstances.

Intermediary functions for which blockchains are not suited

Blockchain as an Enforcer: This function seeks to ensure that “buyers and sellers put forth full effort, cooperate and stay honest”. In a trivial sense, the essence of smart contracts on blockchains is exactly to fulfill or enforce contractual terms based on the performance of the parties. This might seem a likely way in which blockchains can be an intermediary. However, it is not self-enforcing. In situations can be easily punished in a network, it can be an enforcer, but is it more accurate to say a noncompliant transaction will not proceed - but in either case, only within the blockchain. The legal significance of either step still must be determined by some other authority, possibly a court (the state) or by a private decision-maker (such as a contractually-agreed upon arbitrator).

Blockchain as a Bridge: The “bridging” function consists of finding transaction opportunities between two disconnected sets of agents. The act of *finding* suggests agency on the part of the blockchain, which it does not have. Thus, we cannot expect a blockchain to act as a bridge.

---

[13] In most cases, blockchain software projects are developed by the community under open source licenses. Consequently, their behavior could be considered predictable more transparent (Gaba 2018).

Blockchain as an Insulator: An insulator's function is to limit the flow of information between two parties, under blockchain, each user controls what information it wishes to place on the blockchain. Once it is recorded, it cannot be withdrawn. Thus, blockchains would not be able to limit information flow *ex post*.

Blockchain as a Concierge: A concierge helps a consumer to perform certain tasks such as buying a house, booking travel, buy or sell cars, among others. These intermediaries provide value to consumers by understanding their needs and pricing their services "with consumers' ever-changing alternatives in mind."

When does Blockchain require intermediaries?

Most private blockchains are implemented as regular databases based on blockchain concepts. Hence, it becomes more interesting to analyze the case of public blockchains. An important example is transactions using Bitcoin and Ether, where it is important to differentiate between users acting as full nodes[14], and users who are only interested in particular transactions. When users act as full nodes, they are taking advantage of their ability to self-custody and transact with their digital assets without the need for intermediaries, which is provided by the blockchain. Nevertheless, for this broker-less environment to fully operate, users' still need "greater privacy, higher portability between service providers, and increased competition" (Catalini and Gans, 2016). Due to these shortcomings, traditional, *centralized,* solutions remain a convenient option, even in the blockchain environment.

One of the most common centralized solutions takes the form of third-party *wallets*, or wallets provided by an exchange, which interact with the blockchain to enable transactions (Cointelegraph, 2018). The main function of the wallets is to store a user's private key. In this way, when using a wallet, a user is giving the exchange full control over their funds. Hence, wallet users essentially trust wallets with their funds as they would other central institutions such as banks[15].

Unless running a full node, wallet users do not need to download the full blockchain to operate. Instead, wallets rely on miners to obtain current and accurate information on

[14] Full nodes are the individual parts of the data structure in the blockchain. Nodes contribute computing, storage, and time resources to store and validate blocks and transactions and, in most cases, earn a reward for doing so (Morishima 2018).
[15] It is necessary to point out that wallets are essentially a software package, which is usually owned by a company. Consequently, users using these systems need to trust the software provider of the wallet as well.

the state of the blockchain network. There are multiple types of wallets, which adapt to the level of trust, convenience, and risk that best suits the users. For instance, users may choose online (hot) or offline (cold) wallets, depending on whether they want their private key to be available online or offline. With this choice, questions of availability, ease of access, and hacking risks arise.

To the best of our knowledge, wallets are designed for handling cryptocurrency transactions. Since these are digitally born assets, blockchain is an adequate method for handling them. In this case, the need for an intermediary stems from the difficulty to become a savvy and self-sufficient cryptocurrency user. The latter would require users to run full nodes, which is an onerous task, and perhaps not easily accessible by the general public. Along these lines, wallets are the intermediary that handles the inner workings of blockchain-based transactions, while making this transparent and convenient for the users. Still, in the blockchain context, the market power gains of intermediaries may be decreased due to the increased competition that wallets face, and due to the fact that they are not essential to running networks where cryptocurrency transactions take place (Catalinis and Gans, 2016).

Policy Implications

The relationship between blockchains and intermediaries is not entirely straightforward. We have been able to identify situations where the blockchain can act as an intermediary as well as cases where the blockchain needs an intermediary, especially if it wants to reach widespread adoption. The examples we have found suggest that the blockchain cannot entirely eliminate intermediaries.

When the blockchain requires intermediaries for end-users to access its functionalities, we expect intermediaries to be subject to the same regulatory guidelines that other intermediaries face, according to the domain in which they operate. Would (or should) this also apply when the blockchain acts as an intermediary?

As we have seen, intermediaries have the potential to gain market power as the information they control increases. Additionally, one of the main functions for the blockchain is to allow for verification of transactions, without requiring centralized entities. In this particular case, absence of regulation may allow for fraudulent transactions co-existing with legitimate ones, thus allowing for the presence and profits of ‘unsophisticated’ investors (Catalini and Gans, 2016; Werbach, 2018). This highlights the need for an efficient regulatory framework that helps reduce uncertainties for investors, network participants, as well as protect investors and early adopters. These requirements translate into creating and maintaining trust mechanisms in the blockchain. Indeed, if we consider the blockchain an intermediary, we need to think of the metrics that will allow end-users to trust and choose to rely on the blockchain. For instance, we could think of what makes us choose one middleperson over another for different transactions (e.g., why would we choose Amazon over Craigslist? and when?). As intermediaries evolve, there is an increasing number of metrics that reflect their trustworthiness, which can be understood and weighed by end-users (e.g., customer reviews on Amazon, Airbnb, Yelp; rating systems in Uber, Lyft, etc.). In turn, there are systems that verify the accuracy and validity of these metrics so that these can be actually trusted by the end-users.

Another policy challenge in regulating blockchain is in contradiction with its decentralization nature. How should one regulate a blockchain network if it doesn't have an owner? How much liability the software platform has for the activities performed on the network? Consider the debate on Uber drivers' employment status (See NPR News). Uber is a matching service, it doesn't "employ" the drivers. Both drivers and riders are customers. The same goes for Airbnb. Also, consider the calls for regulations on the operations of Facebook, Twitter, and YouTube regarding their users' contents. The situation is also more complex than this: in the legal literature, for example, these companies are considered "platforms" (along with Facebook and Amazon, for example), and the research question tends to focus on concentrated power (antitrust and competition law) rather than on their "intermediary" status.

Another important approach towards increasing trust in the blockchain system is the utilization of *smart contracts*. These are autonomous software agents (Werbach, 2018), whose function is to enforce different types of transactions that take place on top of the blockchain network[16]. There are multiple platforms that allow users to develop smart contracts (the most prominent being Ethereum), and code new types of applications on top of them. One example of these applications is *DApps* or decentralized applications, which mimic existing centralized applications such as cloud storage systems, open discussion platforms and ridesharing applications (Werbach, 2018). The issue with smart contracts is that there is no contract that can account for every possible alternative (i.e., contracts are incomplete). In this way, even if smart contracts are developed to increase trust in blockchain-based systems, these would still require a third-party to handle the cases that smart contracts cannot.

A regulatory framework consists of rules established to govern economic behavior and enforced by third parties. Such frameworks do not necessarily translate into the

---

[16] Note that the idea of smart contracts is not inherent to the blockchain. Smart contracts were introduced even before Bitcoin was developed (Werbach, 2018)

government overseeing or controlling blockchain functions. Instead, we could think of *'off-chain governance'*, whose function is to allow "communities of developers to reach agreement about fundamental changes to market design without destroying confidence in the network" (Catalini and Gans, 2016). As Werbach (2018) puts it, even when the math behind the blockchain is flawless, it is still a system that has been designed, implemented, and used by humans. Hence, for the blockchain to reach its transformative goals, it requires a regulatory framework.

Conclusion

Summarizing, to date, economic theory has viewed blockchain as an institutional technology. To an extent it is, but we focused on whether it is a new and potentially superior intermediary. We find that it performs some intermediary functions well, but for others, it does not. In some instances, blockchain also need intermediaries to function. For example, while there is the potential to revolutionize contracting, all contracts remain incomplete; its enforcement is trivial, once rules are agreed upon, but the existence of the blockchain depends to an extent on contract law, and disputes may arise that require external adjudication and enforcement.

From a policy perspective, our analysis suggests the need for regulation. It also suggests that regulation should continue to encourage the decentralized development of technology. This reflects the nature of blockchain: it is a partially transformative technology, and so is requires perhaps a moderate regulatory approach.

References

Allen, D. W. (2011) *The institutional revolution: Measurement and the economic emergence of the modern world*. University of Chicago Press.

Allen, D. W. *et al.* (2018) 'Cryptodemocracy and its institutional possibilities', *The Review of Austrian Economics*, pp. 1–12.

Allen, D. W. and Potts, J. (2016) 'How innovation commons contribute to discovering and developing new technologies', *International Journal of the Commons*, 10(2), pp. 1035–1054.

Allen, F., & Santomero, A. M. (1999). *What do financial intermediaries do? Wharton School University of Pennsylvania*. Working paper.

B11G. (2019). Project B11G: A European Real Estate Project Powered by Blockchain. Retrieved on 06-06-2019 from https://b11g.eu

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2017). Consensus in the age of blockchains. *arXiv preprint arXiv:1711.03936*.

Braithwaite, V. and Levi, M. (2003) *Trust and governance*. Russell Sage Foundation.
Bitcoin Exchange Guide News Team. (2018). Filecoin Blockchain Data Storage Network. Retrieved on 06-06-2019 from https://bitcoinexchangeguide.com/filecoin-blockchain-data-storage-network-sets-sights-on-middle-of-2019-for-release/

Blocknotary. (2019). Blocknotary Timestamp. Retrieved on 06-15-2019 from https://www.blocknotary.com/timestamp

Brennan, G. and Buchanan, J. M. (1985) *The reason of rules: Constitutional political economy*. New York: Cambridge University Press.
Brown, R. G. (2015). A simple model for smart contracts. *Online in Internet: https://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/, Stand*, *4*, 2018.

Buchanan, J. M. (1975) *The limits of liberty: Between anarchy and Leviathan*. University of Chicago Press.

Buchanan, J. M. and Tullock, G. (1962) *The calculus of consent*. University of Michigan Press Ann Arbor.
Buterin, V. (2015). On public and private blockchains. *Ethereum blog*, *7*.

Cardwell, Diane. (2017). Solar Experiment Lets Neighbors Trade Energy Among Themselves. *The New York Times.* Retrieved on 06-06-2019 from https://www.nytimes.com/2017/03/13/business/energy-environment/brooklyn-solar-grid-energy-trading.html

Catalini, C., & Gans, J. S. (2016). *Some simple economics of the blockchain* (No. w22952). National Bureau of Economic Research.

Chain.com. (2019). "Chain | Enterprise Blockchain Infrastructure." Chain | Enterprise Blockchain Infrastructure. N.p., n.d. Web. 06-06-2019.

Chalker, Anthony. (2018). Prepare for the Blockchain Disruption. *The Institute of Internal Auditors International Conference.*

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *Ieee Access*, *4*, 2292-2303.

Churchbase. (2019). Blockstream. Retrieved on 06-06-2019 from https://www.crunchbase.com/organization/blockstream#section-overview

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

Coinmarket, (2018), "Top 100 cryptocurrencies by market capitalization"

Coinmarket, (2019). "All cryptocurrencies"

Cointelegraph (2018). Guide on Ethereum Wallets: Mobile, Web, Desktop, Hardware. Retrieved from https://cointelegraph.com/ethereum-for-beginners/ethereum-wallets#mobile-wallets

Cooter, R. and Landa, J. T. (1984) 'Personal versus impersonal trade: The size of trading groups and contract law', *International Review of Law and Economics*, 4(1), pp. 15–22.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.

Crowdprecision. (2018). Crowdprecision White-paper.

DataBitcoin. (2019). Average Time to Mine a Block in Bitcoin. Retrieved on 07-25-2019 from https://data.bitcoinity.org/bitcoin/block_time/all?f=m10&t=l

Davidson, S., De Filippi, P. and Potts, J. (2018) 'Blockchains and the economic institutions of capitalism', *Journal of Institutional Economics*, 14(4), pp. 639–658.

Deakin, S. *et al.* (2017) 'Legal institutionalism: Capitalism and the constitutive role of law', *Journal of Comparative Economics*, 45(1), pp. 188–200.

Dillet, Romain. (2015). Stampery Leverages the Blockchain to Certify All Your Documents. *TechCrunch.* Retrieved on 06-10-2019 from https://techcrunch.com/2015/09/22/stampery-leverages-the-blockchain-to-certify-all-your-documents/

Einaste, Taavi. (2018). Blockchain and Healthcare: The Estonian Experience. *e-Estonia.* Retrieved on 06-06-2019 from https://e-estonia.com/blockchain-healthcare-estonian-experience/

Evans, Brian. (2018). Blockchain Tech Company Sia (Siacoin) Could Disrupt Dropbox and Amazon. *Inc.com*. Retrieved on 06-07-2019 from https://www.inc.com/brian-d-evans/blockchain-tech-company-sia-siacoin-could-disrupt-dropbox-and-amazon.html

Fedorov, Aleksey K., Kiktenko, Evgeniy O., and Alexander I. Lvovsky, Quantum computers put blockchain security at risk, *Nature* **563**, 465-467 (2018)

Ftreporter. (2017). Your Data is in Your Hands with Tilepay Coin. *FTreporter.* Retrieved on 06-19-2019 from http://ftreporter.com/your-data-is-in-your-hands-with-tilepay/

Gaba, A. (2018). 'Open source money: Bitcoin, blockchain, and free software. Retrieved on 07-24-2019 from https://opensource.com/article/18/7/bitcoin-blockchain-and-open-source
Garrison, R. H., Noreen, E. W., Brewer, P. C., & McGowan, A. (2010). Managerial accounting. *Issues in Accounting Education*, *25*(4), 792-793.

Gautham, M. (2015). Ascribe Helps You Manage Your Copyright on Blockchain. *NewsBTC.* Retrieved on 06-15-2019 from https://www.newsbtc.com/2015/05/31/ascribe-helps-you-manage-your-copyright-on-blockchain/

Granovetter, M. S. (1977) 'The strength of weak ties', in *Social networks*. Elsevier, pp. 347–367.

Greif, A. (2005) 'Commitment, coercion and markets: The nature and dynamics of institutions supporting exchange', in *Handbook of new institutional economics*. Springer, pp. 727–786.

Greif, A. (2006) *Institutions and the path to the modern economy: Lessons from medieval trade*. New York: Cambridge University Press.

Hayek, F. A. (1945) 'The use of knowledge in society', *The American economic review*, pp. 519–530.

Hayek, F. A. (1948) *Individualism and economic order*. University of Chicago Press.

Hirschman, A. O. (1970) *Exit, voice, and loyalty: Responses to decline in firms, organizations, and states*. Harvard university press.

Hodgson, G. M. (2015) *Conceptualizing capitalism: Institutions, evolution, future*. University of Chicago Press.

Holman, Trevor. (2019). Introduction to Namecoin: A Blockchain Protocol that Functions as a Naming System. *CryptoNewsZ*

Hosmer, L. T. (1995) ‘Trust: The connecting link between organizational theory and philosophical ethics’, *Academy of management Review*, 20(2), pp. 379–403.

Hulseapple, Cheryl. (2018). Block Verify Uses Blockchains to End Counterfeiting and ‘Make World More Honest’. *CoinTelegraph.* Retrieved on 06-07-2019 from https://cointelegraph.com/news/block-verify-uses-blockchains-to-end-counterfeiting-and-make-world-more-honest

Illinois Blockchain Initiative. (2017). Illinois Partners with Evernym to Launch Birth Registration Pilot. *Medium.* Retrieved on 06-06-2019 from https://illinoisblockchain.tech/illinois-partners-with-evernym-to-launch-birth-registration-pilot-f2668664f67c

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

Jones, Brad (2018). Blockchain Could be Implemented in Elections. Retrieved on 06-06-2019 from https://www.digitaltrends.com/computing/blockchain-could-be-implemented-in-electoral-voting-by-2019/

Kelleher, John. (2014). Medici, The Blockchain Stock Exchange. *Investopedia*. Retrieved on 06-06-2019 from https://www.investopedia.com/articles/investing/121014/medici-blockchain-stock-exchange.asp

Krakovsky, M. (2015) *‘The Middleman Economy: How Brokers, Agents, Dealers, and Everyday Matchmakers Create Value and Profit’*, Palgrave McMillan US.

La Porta, R. *et al.* (1999) ‘The quality of government’, *The Journal of Law, Economics, and Organization*, 15(1), pp. 222–279.

La Porta, R., Lopez-de-Silanes, F. and Shleifer, A. (2008) ‘The Economic Consequences of Legal Origins’, *Journal of Economic Literature*, 46(2), pp. 285–332.

Landa, J. T. (1981) ‘A theory of the ethnically homogeneous middleman group: An institutional alternative to contract law’, *The Journal of Legal Studies*, pp. 349–362.

Landa, J. T. (1994) *Trust, ethnicity, and identity: beyond the new institutional economics of ethnic trading networks, contract law, and gift-exchange*. University of Michigan Press.

Levi, M. and Stoker, L. (2000) ‘Political trust and trustworthiness’, *Annual review of political science*, 3(1), pp. 475–507.

Levitt, S.n D., and Syverson, C. (2008) "Market distortions when agents are better informed: The value of information in real estate transactions." *The Review of Economics and Statistics* 90(4): 599-611.

Macaulay, S. (1963) ‘Non-contractual relations in business: A preliminary study’, *American sociological review*, pp. 55–67.

Mailath, G. J. and Samuelson, L. (2006) ‘Repeated games and reputations: long-run relationships’, *Oxford University Press*.

Morishima, S., & Matsutani, H. (2018, March). Accelerating blockchain search of full nodes using gpus. In *2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)* (pp. 244-248). IEEE.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

North, D. C. (2005) *Understanding the process of economic change*. Princeton, NJ: Princeton University Press.

Odyssey (2018). Blockchain Applications in Supply Chain. Retrieved on 06-11-2019 from https://www.odysseylogistics.com/blockchain-supply-chain/

Olson, M. (1965) *The logic of collective action: public goods and the theory of groups.* Harvard University Press.

Ostrom, E. (1990) *Governing the commons: The evolution of institutions for collective action*. New York: Cambridge University Press.

Ostrom, E. (2005) *Understanding institutional diversity*. Princeton, NJ: Princeton University Press.

Ostrom, E. and Ahn, T.-K. (2009) 'The meaning of social capital and its link to collective action', *Handbook of social capital: The troika of sociology, political science and economics*, pp. 17–35.

Ostrom, V. (1994) *The meaning of American federalism: Constituting a self-governing society*. San Francisco: Institute for Contemporary Studies.

Potts, J. (2018) 'Governing the innovation commons', *Journal of Institutional Economics*, 14(6), pp. 1025–1047.

Potts, J. (2019) *Innovation Commons*. Oxford University Press, USA.

Reinsberg, B. (2018) 'Blockchain technology and the governance of foreign aid', *Journal of Institutional Economics*, pp. 1–17.

Roberts, Jeff. (2017). The diamond industry is obsessed with the Blockchain. *Fortune*. Retrieved on 06-07-2019 from http://fortune.com/2017/09/12/diamond-blockchain-everledger/

SimplyBrand. (2018). SimplyBrand White-paper V 3.03.

Tiebout, C. M. (1956) 'A pure theory of local expenditures', *Journal of political economy*, 64(5), pp. 416–424.

Tyler, T. R. (2003) 'Procedural justice, legitimacy, and the effective rule of law', *Crime and justice*, 30, pp. 283–357.

Tyler, T. R. (2006) 'Psychological perspectives on legitimacy and legitimation', *Annual Review of Psychology*, 57, pp. 375–400.

Vaughan-Nichols, Steve J. (2017). Storj Introduces a Distributed Blockchain-protected Cloud Storage Service. *ZDnet*. Retrieved on 06-06-2019 from https://www.zdnet.com/article/storj-introduces-a-distributed-blockchain-protected-cloud-storage-service/

Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. (2016, January). Blockchain contract: Securing a blockchain applied to smart contracts. In *2016 IEEE international conference on consumer electronics (ICCE)* (pp. 467-468). IEEE.

Weingast, B. R. (1995) 'The economic role of political institutions: Market-preserving federalism and economic development', *Journal of Law, Economics, and Organization*, 11(1), pp. 1–31.

Werbach, K. (2018). Trust, but verify: Why the blockchain needs the law. *Berkeley Tech. LJ*, *33*, 487-550.

Williamson, O. E. (1979) 'Transaction-cost economics: the governance of contractual relations', *The journal of Law and Economics*, 22(2), pp. 233–261.

Williamson, O. E. (1996) *The Mechanisms of Governance*. New York: Oxford University Press.