



Aalto University
School of Business

Viability of Public Blockchains in the Financial Services Sector

Bachelor's Thesis
Jurgis Pocius
23.05.2019
ISM Program

Approved in the Department of Information and Service Management 23.05.2019 and
awarded the grade



Author Jurgis Pocius

Title of thesis Viability of Public Blockchains in the Financial Services Sector

Degree Bachelor

Degree programme Information and Service Management

Thesis advisor(s) Johanna Bragge

Year of approval 2019

Number of pages 28

Language English

Abstract

Blockchain technology has significant potential in developing the financial services sector. Although blockchains are often undifferentiated in contemporary discussion, they are, in fact, divided into three types: public, private and consortium. Thus far, the financial services sector has focused on developing private and consortium blockchains while eschewing the innovative aspects of blockchain present in the public blockchain. Through a literature review this thesis will examine the validity of the issues leading to such a decision, suggest ways that the public blockchain could potentially innovate the financial services sector and discuss the future of public blockchains in the financial services sector.

This thesis found that while the current reservations regarding public blockchain implementation are valid, new public blockchain research and solutions are increasingly rendering these reservations obsolete. In addition, public blockchains contain inherent advantages such as incorruptibility, transparency, reduction of intermediaries and increasing financial market participation over their more private counterparts. Although public blockchains represent a threat to the financial services sector's existing revenue model, the improvements in public blockchain technology will present unique opportunities that will at least have to be considered by companies in the sector. In the meantime it seems that symbiotic private-public and consortium-public blockchain solutions will be adopted in the near future.

Keywords public blockchain, blockchain, Bitcoin, Ethereum, Zcash, Zilliqa, financial services innovation

Table of Contents

Abstract

1	Introduction	2
1.1	Research objectives and research questions	2
1.2	Scope of research	3
1.3	Methodology	3
1.4	Structure of the research	4
2	Theoretical background	4
2.1	What is a blockchain	5
2.2	Smart contracts	6
2.3	Differences between public, private and consortium blockchains	7
3	Review of the literature on public blockchain use in the financial services sector ..	8
3.1	The Blockchain Consensus Dilemma	8
3.2	Scalability issues	10
3.3	Privacy, Security, and Practical Concerns	13
3.4	The advantages of public blockchain implementation	14
3.5	The future of public blockchains in the financial services sector	16
4	Discussion and conclusions	18
4.1	Implications to practice	20
4.2	Suggestions for future research	20
	References	22

List of figures

Figure 1.	How blockchain transactions work (Wild et al. 2015)	5
Figure 2.	The structure of blocks in a blockchain (Prashanth Joshi et al. 2018)	6
Figure 3.	The different layers of a blockchain (Demirors 2017)	6
Figure 4.	Representation of private, consortium and public blockchains) (Evans 2015) ..	8
Figure 5.	Blockchain network congestion (Auer 2019)	11
Figure 6.	Current validation structure versus sharding (Imbrex 2017)	12
Figure 7.	Possible private-public blockchain symbiosis (Ali et al. 2018)	18

1 Introduction

Blockchain technology is an important innovation that has the potential to revolutionize several industries, including the financial services sector (Deloitte 2018). Blockchain could help modernize the global banking system and lead to faster payment types, such as more efficient B2B transactions, lower cross-border currency exchange friction (Hewlett-Packard 2016), improvements in the securities trading and settlement process, automated clearing, enhanced security, cost reduction and direct ownership of holdings (Avgouleas & Kiayias 2019). In addition, blockchain could open up banking to the unbanked and improve financial options of retail investors (Aggarwal 2017). According to Santander's InnoVentures, blockchain could save \$15 to \$20 billion per year in banks' infrastructure costs alone (Belinky et al. 2015). The financial services sector is one of the first industries to be innovated by blockchain technology and many industry experts agree that blockchain represents a significant innovation in the field (Deloitte 2018).

However, while we are often introduced to a blockchain that is transparent, decentralized, secure and immutable (Puthal et al. 2018), the financial services sector entities mostly focus on implementing private, or permissioned, blockchains which do not implement these features as extensively as public blockchains (Deloitte 2018, Gencer et al. 2017). The downside of private blockchains is that they often remind more of traditional databases (Kuo Chuen 2017, Wharton 2018) and consequently forgo "the open architecture, the flexible trust model and the strong security guarantees" of the public blockchain technology (Gencer et al. 2017). Public blockchain networks are currently not significantly pursued in the financial services sector and they are generally not considered as viable tools for the financial services sector (Kruglova & Dolbezhkin 2018). In justification for these claims, much of public blockchain coverage has relied on Bitcoin, and ignored the nuances of public blockchain technology as well as alternative blockchains. We will analyze the rationale of these concerns and eventually the viability of not only Bitcoin, but also other forms of public blockchains in the financial services sector.

1.1 Research objectives and research questions

The purpose of this thesis is to research the viability of public blockchains in the financial services sector today and in the future. The thesis discusses the arguments backing the current unwillingness to adopt public blockchains in the financial sector,

the possible benefits of public blockchain adoption in the financial sector and the future of public blockchains in the financial sector.

This thesis will focus on the following research questions:

RQ1: How valid are the current concerns over public blockchain use in the financial services sector?

RQ2: What would be the advantages of public blockchain implementation in the financial services sector?

RQ3: What is the future of public blockchains in the financial services sector?

1.2 Scope of research

This thesis focuses on the general viability of public blockchains in the financial sector. The public blockchain technology is mainly discussed holistically, occasionally delving deeper into the specific parts of the technology.

Private and consortium blockchains will be discussed insofar as to offer context and a point of comparison for public blockchains. We will also assume the permissioned blockchains are analogous to private blockchains, although some may divide the blockchain into further subtypes.

The focus of this thesis is only on blockchain technology and will not discuss other distributed ledger technologies, such as the directed acyclic graph. The legal aspects of blockchain technology are also beyond the scope of this thesis.

1.3 Methodology

High quality published research papers and articles were used for the literature review of this thesis. A variety of scientific and reliable sources on public blockchains were chosen in an effort to cover the topics as objectively and as analytically as possible. Scientific databases such as Scopus, IEEE Xplore and Web of Science were primarily used. Some previous knowledge from past research work on blockchain technology was also utilized in the writing of this thesis.

1.4 Structure of the research

The rest of the thesis is structured as follows. Chapter 2 will set a framework for the research questions and discuss the important concepts that are needed in addressing the thesis' research questions. Chapter 3 will discuss the results within the framework of the three research questions and based on the literature gathered. Chapter 4 will conclude and summarize the main points of the thesis.

2 Theoretical background

A blockchain is a shared ledger of transactions that is stored across all the participants of the blockchain (OECD 2019). One of the revolutionary consequences of the technology is that no central party is in charge of owning or updating the information stored on the blockchain. Instead, identical copies of the blockchain, or the universal ledger, are distributed to all participants of the blockchain and the blockchain updates itself automatically through various mechanisms depending on the blockchain. As such, blockchain creates unique data capabilities that include “immutability, irreversibility, decentralization, persistence and anonymity” (Puthal et al. 2018). In Figure 1, we see how a basic currency transaction is conducted on the blockchain. It is to be noted that the currency represents not only money, but can also represent, for example, data, some sort of utility, security or ownership. However, the way these transaction are conducted is the same. As seen in Figure 1, after the transaction is initiated, it is broadcasted and verified by the blockchain network, or the nodes of the blockchain. When the transaction is verified, the transaction is added to the existing blockchain along with other transactions in a medium called a block. The time that it takes for the block to be verified is called the confirmation time. After the verification is complete, the currency is received by the counterparty.

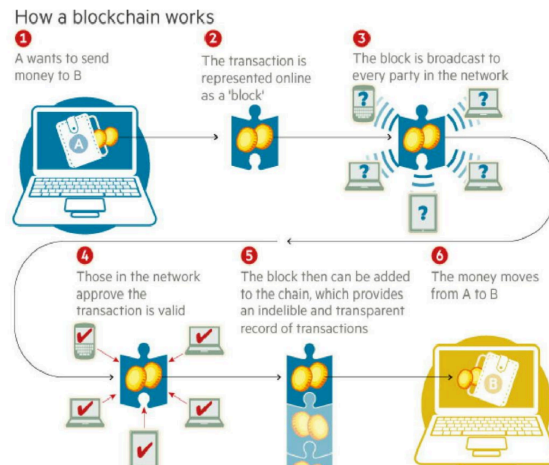


Figure 1. How blockchain transactions work (Wild et al. 2015)

2.1 What is a blockchain

More specifically, a blockchain is a linked chain of blocks. Blocks are data storage units that update and upkeep data or transactions in the ledger (Yang et al. 2019). Each block includes a set number of individual transactions made in the same period (OECD 2019). In addition to transaction data, each block also includes a timestamp, as well as a hash, or a unique identifier, and the previous block's hash, as visualized in Figure 2 (OECD 2019). As these blocks are linked together, they create a historical ledger with all conducted transactions (Hughes et al. 2019). The transactions are auditable by the public, but the transaction information itself stored in the blocks is encrypted and anonymized (Hughes et al. 2019).

The validity of the transactions and data in the blocks are verified through a pre-set mechanism called the consensus mechanism. The mechanism seeks to maintain integrity of the blockchain and prevent fraud (Yang et al. 2019). The consensus mechanism ensures that all the nodes agree on the state of the universal ledger and a new block can be added on the blockchain only if all agree on the same version of the ledger (OECD 2019). The consensus mechanisms, however, vary according to the blockchain protocol, or a set of predefined rules, and blockchain type (OECD 2019). Generally in public blockchains, the implementation of the consensus mechanism is called mining (Puthal et al. 2018).

A blockchain generally consists of three layers as seen in Figure 3: a protocol layer, a networking layer and an application layer (Demirors 2017). The protocol layer is programmable layer in which the rules of the blockchain are defined. The networking

layer is the realm in which these rules are implemented, and the application layer is the user-interface in which the applications are built based on the protocol and networking layers (Demirors 2017).

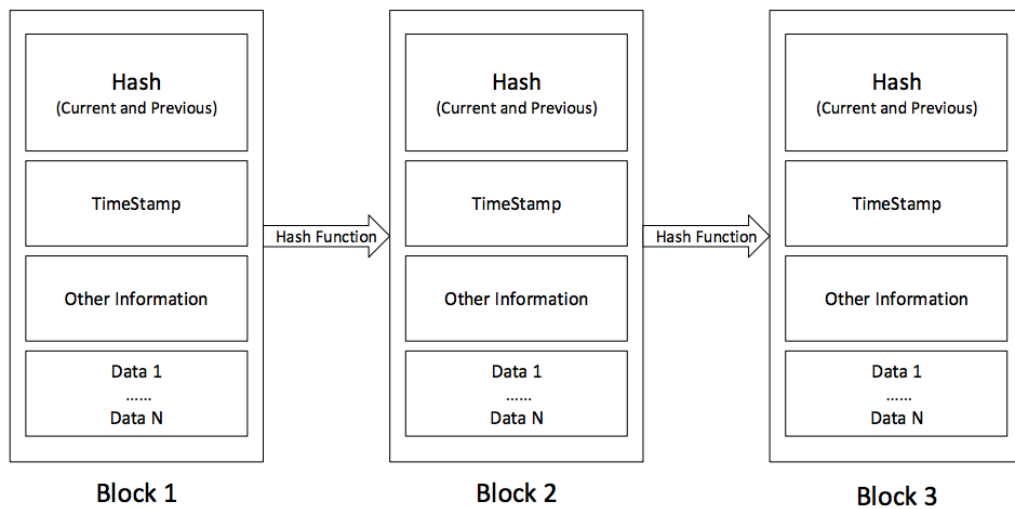


Figure 2. The structure of blocks in a blockchain (Prashanth Joshi et al. 2018)

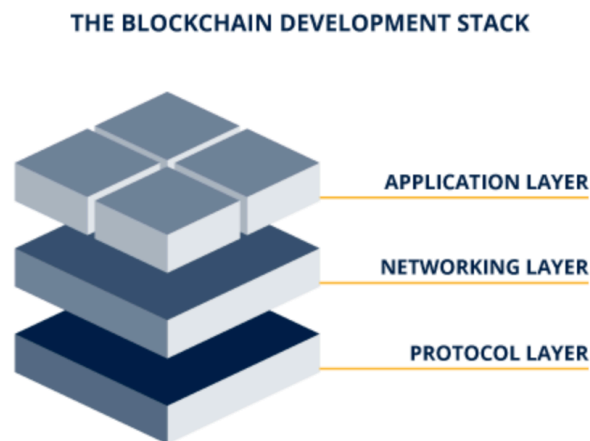


Figure 3. The different layers of a blockchain (Demirors 2017)

2.2 Smart contracts

The first application of blockchain technology, Bitcoin, was developed for peer-to-peer electronic cash transactions by Satoshi Nakamoto (2008). However the Ethereum blockchain introduced another revolutionary feature called the smart contract. Smart contracts are programmable and self-executing contracts based on pre-determined conditions (Ahl 2019, Frankefield 2019). These contracts have important potential in

the financial services sector because they allow an asset or a currency to be transferred into a program (Bheemaiah 2017). To initiate smart contract transactions, tokens are needed. Ethereum uses a token standard called ERC-20, but other token standard variations exist.

2.3 Differences between public, private and consortium blockchains

The implementation of a given blockchain not only depends on different protocols, but also on different blockchain types. The three types of blockchains are public, private and consortium (Kuo Chuen 2017). These three types have various levels of decentralization as seen in Figure 4. The public blockchain is arguably a blockchain in its purest form, adhering most closely to Puthal's (2018) aforementioned blockchain capabilities, especially immutability and decentralization. In theory, anyone can access a public blockchain, as well as participate in the consensus mechanism (Hughes et al. 2019). The transactions on the public blockchain are conducted using tokens. The OECD (2019) characterizes these tokens into payment tokens, utility tokens and security tokens. They store value, represent a right to a good and represent equity respectively (OECD 2019). As there is no central authority to maintain the validity of the blockchain, a decentralized consensus mechanism is used (Puthal et al. 2018). The consensus mechanism used in public blockchains vary, but the most notable ones are Proof-of-Work (PoW) and Proof-of-Stake (PoS) (Puthal et al. 2018).

On the other hand, the private blockchain is the most centralized blockchain type and its functionality does not drastically differ from that of traditional databases (Kuo Chuen 2017). Private blockchains are regulated blockchains in which only permissioned individuals and groups have access to and can contribute to the blockchain (Kuo Chuen 2017). A trusted authority, node or nodes, is in charge of maintaining the integrity of the blockchain (Puthal et al. 2018). Essentially, in private blockchains, only this trusted authority can validate and confirm transactions (van Deventer et al. 2018). Because a single entity is in charge of maintaining the integrity of the blockchain, private blockchains can use much simpler and faster consensus mechanisms (Guegan 2017). However, the centralized nature of private blockchains means that they are not immutable and can be reversed by permissioned authorities. The centralization also makes the blockchain susceptible to the risks of traditional database management, as there exists a central point of attack for hackers to exploit (Guegan 2017, Lindsey 2018). Additionally, private blockchain consensus mechanisms do not necessarily use

cryptography, making them arguably less secure than public blockchains (Guegan 2017).

The consortium blockchain is a hybrid blockchain that combines the features of the private and the public blockchain (Kuo Chuen 2017). Consortium blockchains are partially centralized and managed by selected validator nodes (Kuo Chuen 2017). Similarly to private blockchains, consortium blockchains rely on “voting or multi-party consensus algorithms” for maintaining the integrity of the blockchain (Mao et al. 2018).



Figure 4. Representation of private, consortium and public blockchains (Points represent nodes) (Evans 2015)

3 Review of the literature on public blockchain use in the financial services sector

The results are addressed from the point of view of this thesis’ three research questions. Sections 4.1-4.3 discuss RQ1: How valid are the current concerns over public blockchain use in the financial services sector? Section 4.4 discusses RQ2: What would be the advantages of public blockchain implementation in the financial services sector? Section 4.5 discusses RQ3: What is the future of public blockchains in the financial services sector?

3.1 The Blockchain Consensus Dilemma

Before it is feasible for the financial services industry to adopt public blockchains, the issues with public blockchains’ consensus mechanisms have to be addressed. While the consensus mechanisms for private blockchains are quick and sustainable, due to their inherent centralization, the mechanisms for the most notable public blockchains such as Bitcoin, Litecoin and Ethereum have been often criticized for their energy use and long-term unsoundness (Frankenfield 2018). The original consensus mechanism for

public blockchains, the Proof-of-Work (PoW), is still used by the most popular blockchains (Frankenfield 2018). PoW relies on solving complex mathematical puzzles by the miners, or validators of the network (Kulhari 2018). The miners, in turn, receive a reward for their validating efforts in the form of cryptocurrency, or the transaction tokens of blockchains. While the PoW mechanism creates unique security advantages, it is criticized for its energy consumption, the ability for the blockchain network to be attacked if 51% of the mining power is controlled by a malevolent entity and the decreasing incentive for the miners to mine due to decreasing rewards received for each verified block (Auer 2019). Indeed, in 2017, Bitcoin used more power than many nations (Blinder 2018), and the blockchains that use the PoW are not as impervious to blockchain network attacks as previously thought (Frankenfield 2018). Moreover, Bitcoin mining is not as decentralized as often assumed, since the five biggest Bitcoin mining pools, or groups of collaborating miners, currently control more than 51% of the mining power (Zheng et al. 2017, Tuwiner 2019).

However, there are alternative consensus mechanisms that do not require any significant energy consumption and rely on very different types of mining (Kulhari 2018). One of these alternative mechanisms is the Proof-of-Stake (PoS) mechanism (Kulhari 2018). Blockchains such as Cardano, Nxt already use this mechanism, while Ethereum is in the process of switching from the PoW to the PoS mechanism (Auer 2019). Instead of cryptographic hashing, the mechanism relies on validating the blockchain through a process called staking (Kulhari 2018). In addition to saving energy, the PoS mechanism disincentivizes the 51% attack as the attacker would suffer oneself from a fall in the value of the blockchain associated with a malicious attack (Frankenfield 2018). However, the PoS mechanism is not beyond criticism either. Auer posits (2019) that PoS contains no efficient method when distinguishing between two blockchains with alternative histories, which opens it up for fraudulent betting on alternative blockchain histories. Whereas the PoW mechanism resolves such a problem by choosing the longest chain, no such tangible criterion exists for the PoS mechanism (Auer 2019). Auer (2019) also argues that alternative consensus mechanisms such as the Proof-of-Stake, Delegated Proof-of-Stake and Proof-of-Importance can only succeed if a degree of institutionalization and thus centralization is present (Auer 2019). Such presence of centralization undermines the value of decentralization and exposes such blockchains to some of the very same shortcomings that the private blockchains face.

Finally, while the public consensus mechanism is one of the revolutionary aspects of blockchain technology it also creates problems that are solved rather simply under the

private blockchains. For instance, in the past, Bitcoin has not been able to improve performance “because the miners could not reach consensus on how to improve the algorithm” and the Ethereum blockchain has been split into two separate blockchains over disagreement on how to proceed after a hack on its smart contracts (Jun 2018). As a result, the public blockchain consensus mechanisms make public blockchain operation slower and less scalable, which is an important consideration for the financial services sector.

3.2 Scalability issues

The speed of transactions is a key consideration for companies in the financial services sector, however, the biggest and arguably most trusted public blockchains, Bitcoin and Ethereum, remain very slow as they can process only 4.6 and 9 transactions per second respectively, versus Visa’s approximate 1,700 transactions per second (Jun 2018, Li 2019). While the daily transaction volume on public blockchains keeps developing upward and the scalability issue is not solved, transaction times will increase and become more expensive as seen in Figure 5 (Auer 2019). In the figure, the supply curve represents the amount, which tends to be constant, of transactions that can be processed at any given time on the blockchain. Because the supply is constant, increased demand not only slows down the average rate at which the consumers can conduct their transactions on the blockchain, but increases the transaction fees as well. As these networks grow, by virtue of being accessible to everyone, public blockchains become slower and more expensive to use (Auer 2019). While the biggest and most trusted blockchains such as Bitcoin and Ethereum are currently not viable options for frequent day-to-day transactions due to their slow transaction speed, there are ways blockchains can improve this speed through solutions such as second blockchain layers, sharding and alternative consensus mechanisms (Auer 2019). These are explained next.

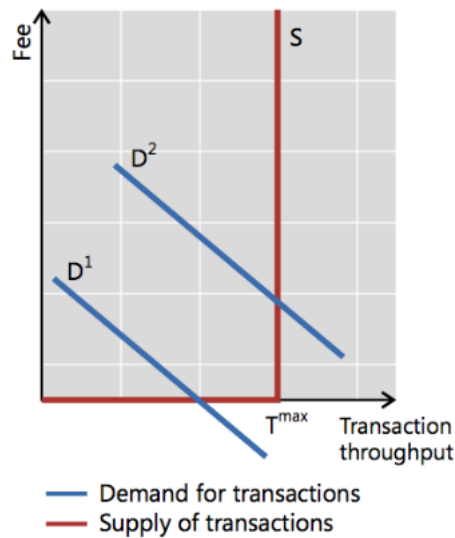


Figure 5. Blockchain network congestion (Auer 2019)

One of the proposed solutions for blockchain scalability and higher transaction speed has been to shift blockchains from the currently dominating single chain solution to a multi-chain architecture (Yu et al. 2019). One way to achieve this architecture is through an off-chain protocol such as Bitcoin’s Lightning Network (Zhong et al. 2019). The network uses sub-chains independent from the main blockchain to handle the details of transactions. Only final outcomes of the sub-chains are then committed to the main blockchain (Yu et al. 2019). This significantly reduces the capacity pressure of the blockchain, however, critics state that these off-chain payment systems can support at most 800 million users and are in contradiction with the principles of blockchain as the off-chain transactions cannot be validated by the public (Yu et al. 2019, Zhong et al. 2019).

Another proposed solution to the scalability problem is a mechanism called sharding. In January 2019, the Zilliqa blockchain was the first blockchain to implement sharding (Baker 2019). Other public blockchains, such as Ethereum, are seeking do so in the near future. In the current public blockchain protocols, each node of the blockchain network is responsible for storing the entire history of the blockchain and processing all the transactions on the blockchain. Sharding proposes that the blockchain should be divided into smaller divisions called shards and that each shard would be verified by only some of the nodes in the blockchain, as seen in Figure 6 (Chauhan et al. 2018, Zamani et al. 2018). This would allow many transactions to be processed in parallel, instead of linearly, leading to less computing and storage per node, thus faster performance, faster transaction times and better scalability of the blockchain to larger networks (Chauhan et al. 2018, Zamani et al. 2018). As a result of sharding, the

aforementioned Zilliqa can conduct 2,828 transactions per second versus the existing public blockchain average of 7-15 transactions (Zilliqa 2019). However, some argue that sharding poses certain security concerns such as the single-shard takeover attack (Chauhan et al. 2018). Some other drawbacks of sharding include the added complexity that is needed to handle the transactions between different shards and the decreased blockchain decentralization as the number of shards increase (Fanti & Viswanath 2019).

Some public blockchain protocols inherently support fast blockchain transactions as a result of their consensus mechanism. One example of this is the EOS.IO blockchain which can scale up to 100,000 transactions per second (Chauhan et al. 2018). It uses a variation of the aforementioned Proof-of-Stake consensus mechanism, called Delegated Proof-of-Stake (DPoS). In the DPoS consensus mechanism, the blockchain “token holders select the block producers by continuous voting procedure” (Chauhan et al. 2018). Consequently, less time is needed to produce a new block by a single producer and a given transaction on the EOS blockchain will be confirmed within 1.5 seconds with a 99.9% certainty (Chauhan et al. 2018). On the other hand, the DPoS mechanism paves the way for centralization as, in practice, it does not allow regular users to audit the blockchain (Chauhan et al. 2018).

Overall, the current concerns regarding public blockchain scalability are realistic and especially the low speed of transactions is a considerable limitation for public blockchain use-cases in the financial services sector. However, although the performance enhancements are still at their infancy, public blockchain performance will certainly increase in the future with more research and time (Jun 2018).

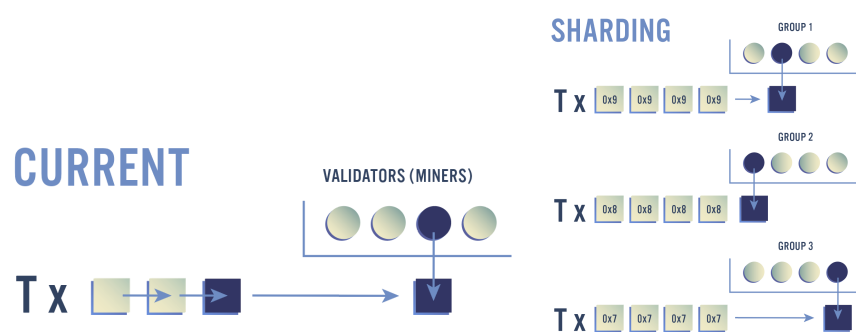


Figure 6. Current validation structure versus sharding (Imbrex 2017)

3.3 Privacy, Security, and Practical Concerns

One of the strongest motives for the financial services sector's willingness to operate on private and not public blockchains, is the inherent lack of data privacy in current implementations of most public blockchains. The financial services sector relies on private data "such as personal identity (sex, age, name, address and etc.), health record, private keys, or ownership of assets" yet most public blockchains are open-source (Victor 2019) and operate under the protocol of transparency (Jun 2018). It has been found that even though transactions on the Bitcoin and other public blockchains are anonymous, the identity of the transaction initiator can be determined if enough data is gathered about the initiator (Kruglova & Dolbezhkin 2018, Goldfeder 2017). Thus, including private data on public blockchains is currently not entirely safe and even somewhat unrealistic.

However, a solution to this problem may have already been discovered with cryptographic algorithms such as the zero-knowledge-proof (Jun 2018). It has already been implemented in privacy-centric blockchain projects such as Zcash, which supports private transactions "where sender, receiver and amount are not revealed; and yet, an outside observer can still distinguish between a valid and non-valid transaction" (Bowe et al. 2019). However, the downside of these privacy features is increased computational time (Dib et al. 2018). Further development is needed to reach an optimal level of privacy with a great transactional speed.

There are also security and practical concerns that need to be addressed before the financial services sector can further explore the possibilities of public blockchains (Kruglova & Dolbezhkin 2018). Despite the inherent security public blockchains provide, there is still a concern over loopholes in the blockchain code, as the DAO attack on Ethereum went to show, and over a secure ways to store large quantities of blockchain tokens or cryptocurrencies (Kruglova & Dolbezhkin 2018, Jun 2018). Furthermore, in part because trading of these cryptocurrencies is open to all, their price has been extremely volatile (Kjærland et al. 2018). This is a significant hinderance to the day-to-day reliability of the public blockchain, as among other things, it makes financial modelling and forecasting based on blockchain transactions difficult. However, it is to be noted that Bitcoin's price volatility has displayed a decreasing trend over the past seven years (Bitcoin Volatility Index 2019).

3.4 The advantages of public blockchain implementation

One of the main advantages of public blockchains is the incorruptibility that their complete decentralization provides. Complete decentralization protects “the users of an application from the developers by establishing that there are certain things that even the developers of an application have no authority to do” (Buterin 2015). We could imagine that this could bring financial stability and even certainty to financial service operators in politically unstable countries. In theory, these operators could not be coerced to change their blockchain protocols to serve, for example, an oppressive political regime. This could also make subsidiary activity safer in such countries. Overall, the decentralization of the blockchain governing structure paired with the absence of a central point of attack for hackers to target (Lindsey 2018) would make financial services operation more secure in less stable environments.

In addition, relinquishing centralized control in favor of the public blockchain could improve financial institutions’ perceived public image through increased transparency. A YouGov survey found that 66% of adults in Britain still do not think that banks have society’s best interests in mind (White 2018) while a Facebook IQ (2016) survey revealed that only 8% of millennials trust financial institutions. Private and consortium blockchains still allow the protocol of the blockchain to be modified by authorized members, namely these same institutions for whom the public has little trust. Giving up some control may be a way to regain the public’s confidence the financial services sector lost after the last financial crisis.

Reduction of intermediaries is another advantage public blockchains have over private, and even consortium, blockchains. As the public blockchain is open to everyone and is used by a wide range of assets, it facilitates network effects and financial freedom unavailable to private, or even consortium, blockchains (Buterin 2015). For example, one can send Bitcoin anywhere in the world regardless of bank holidays and merchants can expand to areas where credit cards are not available (Davradakis & Santos 2019). Regarding transactions that previously used third parties to manage counterparty risk, the public blockchain is able to reduce and stabilize fees for these, regardless of how much money is transacted (Davradakis & Santos 2019, Buterin 2015). Another important consequence is that anyone can issue and purchase an asset on the public blockchain. As a result, this reduces cost and complexity of listing a company, which decreases the barriers to entry to the financial markets (Hays & Valek 2019).

Public blockchains are uniquely opening up the financial markets to new participants, especially to retail investors as well as small and medium-sized enterprises (Hays & Valek 2019). In addition to opening up fundraising to smaller companies, public blockchain technology has the potential to increase the liquidity of primary and secondary markets. The most promising development in this field is the securities token offerings (STOs). The STOs are a new way for companies to raise funds by converting securities into asset-backed blockchain tokens (Browne 2019). While both private and public blockchains are pursuing this innovation, the public version of the STOs has the potential to truly democratize retail investors' access to the capital markets, create a larger pool of investors, increase market transparency, increase liquidity and speed as well as offer around the clock trading (Chester 2019). Thus far, there have been promising public blockchain STO projects. One of them is Polymath, which has developed a new blockchain token standard called the ST-20 (Polymath 2019). The ST-20 is an extension of Ethereum's ERC-20 token used for smart contracts and introduces an additional functionality that allows transfers of blockchain tokens to be restricted, which allows the tokens to comply with securities trading regulations (Polymath 2019). While this is perhaps a divergence from a purely public blockchain, as these tokens are not accessible to anyone due to restrictions dictated by securities trading regulations, it accomplishes many of the touted benefits of public STOs: it makes securities trading more accessible to the unbanked, enables 24/7 access to markets and allows companies to customize their equities issues through programmable code (Polymath 2019). Specifically, the propositions to increase liquidity, equity customization, speed and decreasing settlement times are something the financial services sector could greatly benefit from. The potential of digitized assets on the blockchain will inevitably be explored further in the future. Whether this will continue to thrive on the public or the private blockchain, remains to be seen.

The possibilities of decentralized blockchains are slowly starting to be realized by the innovators of the financial services sector. For example, the subsidiary of Société Générale, the 16th largest bank in the world, issued €100 million in covered bonds in April 2019 onto Ethereum's public blockchain (Société Générale 2019). This was a significant milestone as it was the first large financial services institution to create an STO on a public blockchain. In its own words, the bank was motivated by increased product scalability, computer code automation and reduced time to market, which would improve transferability and settlement of the bonds (Société Générale 2019). Significantly, the credit rating agency Moody's agrees that the use of blockchain has a positive effect on the credit rating, due to the increased transparency and decreased

intermediaries, both strengths of public blockchains, compared to the traditional bond issuing mechanism (Baydakova 2019, Moody's 2018).

However, due to the prevailing business model in the financial services sector, adopting the public blockchain could actually hurt many players in the financial services sector. In addition to decreasing company-specific control, Moody's (2018) states that the decentralization aspect of public blockchains will cause a pressure on revenue due to decreased processing fees, commissions and gains on foreign exchange transactions. Many banks still rely heavily on fees and commissions (Moody's 2018). Thus, truly accepting a decentralized blockchain would require a more fundamental change to the financial services sector's business model and the discovery of new revenue streams (Deloitte 2018). As it stands, it is unlikely that big players in the industry will promote significant upheaval to the system that has been advantageous so far.

3.5 The future of public blockchains in the financial services sector

Currently the financial services industry is relying on consortium blockchains, not public blockchains, to capture the benefits of the technology, due to a desire for complete operational certainty and speed. It seems that the public blockchain space is more compelling to small, even subversive, companies and startups in the financial services sector. Bigger enterprises seek to maintain the current framework by creating consortium blockchain networks that retain their current leadership status in the sector. Deloitte (2018), for instance, divides the financial services sector companies into the more traditional enterprises and the more innovative emerging disruptors.

The lines between public and consortium blockchains are starting to diminish. The consortium blockchains are becoming bigger with increasing memberships. According to Deloitte's (2018) global survey, 29% are already a part of consortium blockchain and 45% are likely to join one. On the other hand, public blockchains are creating private implementations for corporations. For example, J.P. Morgan Chase's Quorum consortium blockchain is built on Ethereum's public blockchain (J.P. Morgan 2019). Both blockchain types seek to increasingly capture the benefits of the other type. It is likely that synergetic consortium-public and private-public blockchain structures, represented in Figure 7, will be increasingly common.

It is evident that the financial services sector will keep building on consortium blockchains due to their advantages in key categories like privacy and scaling, however, some are questioning the innovation of consortium blockchains (Dib et al. 2018). While

these blockchains will undoubtedly improve the speed and ease of transactions in the financial services sector, consortium networks may create barriers to entry, cause uneven power distribution within the consortium and may even hamper innovation (Dib et al. 2018). The uneven power distribution is inherent in the consortium blockchain membership structure. They are divided into premium and general members, who pay \$250,000 and \$5,000 to \$50,000, respectively, per year in membership fees (Irrera 2017). Many consortium blockchains have also ran into cooperation problems among the consortium members as well as funding problems, which explains why several big companies, such as J.P. Morgan Chase, have left consortiums and joined others or created their own (Irrera 2017). In this context, well-developed public blockchains have the advantage of having had constant development and a well-defined modus operandi. Thus, due to the relatively untested nature of consortium blockchains, it remains to be seen whether these will bring about revolutionary innovation in the financial services sector, or whether they will succumb to their weaknesses and shift industry interest toward public blockchain implementation.

On the face of it, the public-consortium blockchain debate draws comparisons to Harvard Professor Clayton Christensen's Disruptive Innovation theory. According to the theory, existing market leaders unwillingly lose market share and are eventually overcome by a disruptive innovation. Disruptive innovation is defined as something that "allows a whole new population of consumers at the bottom of a market access to a product or service that was historically only accessible to consumers with a lot of money or a lot of skill" (Christensen 2019). Significantly, this innovation strongly reminds of public blockchains' goal of democratizing the financial markets and empowering the marginalized, through developments such as the STO and low-commission money transfers. While in reality the narrative is not as straightforward, public blockchains tend to represent complete reorganization of the financial services sector, while consortium blockchains represent an improvement of the existing paradigm.

Currently, using public blockchains for day-to-day operations is still not entirely viable, however, with each improvement public blockchains are showing increasing potential to disrupt the financial services sector as a whole. In the future, the viability of public blockchain use in the sector will be linked to the blockchain's ability to improve its operability and the ability of the sector to recognize the benefits that public blockchain technology provides. Moreover, as it took a long time for companies to adopt first private, then consortium blockchains, similarly it will take time for the financial

services sector to build confidence for the relatively untested public blockchain. It will take a compelling use-case and a successful large-scale implementation of the technology, for momentum to start building. That being said, it appears that, even today, there could be a place for both blockchains. As discussed, private blockchains are currently better suited for internal and the more data sensitive operations, while public blockchains are valuable in a supplementary capacity in areas where intermediaries are untrustworthy or non-existent, such as in politically unstable countries, in areas where intermediaries may want to be minimized, such as international money transfers, and in areas where network effects want to be maximized. Thus, it is likely that in the near future we will be moving increasingly toward public-private and public-consortium blockchain collaboration.

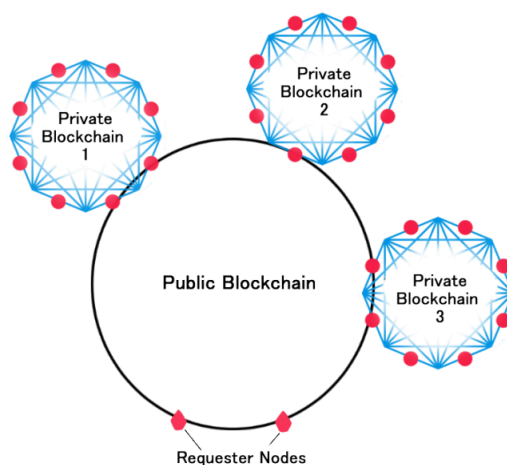


Figure 7. Possible private-public blockchain symbiosis (Ali et al. 2018)

4 Discussion and conclusions

We started this thesis with three research questions: How valid are the current concerns over public blockchain use in the financial services sector, what would be the advantages of public blockchain implementation in the financial services sector and what is the future of public blockchains in the financial services sector?

Through a literature review we distinguished the most pertinent concerns with public blockchains regarding financial services sector implementation. The first concern is the demanding and slow consensus mechanisms. This is a valid concern in that the Proof-of-Work consensus mechanism is slow, energy intensive and susceptible to network takeovers. We found, however, that there are alternative consensus mechanisms such

as the Proof-of-Stake and Delegated Proof-of-Stake that are faster and less energy intensive than the Proof-of-Work, yet these too have shortcomings.

The second concern with public blockchains is scalability. We found that scalability of public blockchains needs to be improved in order to prevent network congestion and slower transaction speeds. Before this is done, significant adoption by the financial services sector is unrealistic. There is currently promising research on the matter and possible solutions to the problem are already being implemented.

The third major concern with public blockchains is the lack of privacy. Public blockchains are severely disadvantaged in comparison to private blockchains in this category. However, new privacy enhancing algorithms, such as the zero-knowledge-proof are in the process of mending the situation. Despite their promise, these too need further development, as increased privacy on public blockchains decreases transaction speed, something crucial to the financial services sector. Overall, the current concerns with public blockchains are valid, but are becoming less obvious with new research and constant development.

Despite the shortcomings of public blockchains, they offer unique advantages over private blockchains. Public blockchains offer a uniquely transparent way of governing companies that may benefit the public image of financial services sector companies. Public blockchains also entirely dispose of intermediaries, which promotes even greater network effects than those of consortium chains, increases transaction efficiency and lowers transaction costs. Public blockchains also have the potential to streamline the securities markets, create more liquid financial markets and provide new financial opportunities where they did not exist before, with developments such as the STOs. A few players in the financial services sector, have recognized the potential of public blockchains in streamlining the securities markets, but we are still far away from the widespread acceptance of these benefits. Crucially, the financial services sector's current reliance on fee-based revenue streams means that several of the public blockchain benefits may actually hurt existing companies in the sector.

Finally, we established that the aforementioned shortcomings of public blockchains place them currently at a disadvantage relative to consortium blockchains in the financial services sector. However, public blockchains have the potential to revolutionize the sector a step beyond consortium blockchains. Moving forward, public blockchains will continue to improve their main shortcomings: energy efficiency, scalability, transaction speed and privacy management. This should increase interest in

public blockchain implementations in the financial services sector. However, one of the biggest problem with public blockchains is that they represent a complete remodeling of the financial services sector, which may be a concern for the major players who do not want to risk losing influence in the industry. Thus, public blockchain viability will largely depend on the financial services sector's desire to innovate and to remodel itself. In the meantime, synergetic solutions between private, consortium and public blockchains are likely to be pursued.

4.1 Implications to practice

This thesis reveals several practical implications to the financial services sector and public blockchains. First, despite the attraction of private and consortium blockchains, companies should try to pursue, arguably blockchain technology's greatest strength, decentralization. While the more private blockchains offer greater speeds there is more potential to be drawn from blockchain technology as a whole than just that.

Second, even the biggest institutions in the financial services sector should be vigilant about the possible changes to the sector. While public blockchain implementation in the sector has an uncertain future, historically many small innovators in various fields have undercut the market share of, and even displaced, many established players in these fields. Thus, the entire sector has a vested interest in keeping up to date with public blockchain innovation.

4.2 Suggestions for future research

In part due to the novelty of the topic, surprisingly little differentiation exists in research between public, consortium and private blockchains in current research. The three types are often lumped together in current blockchain technology discussion despite offering distinct value propositions and having different requirements. More research differentiating these three is needed. As research has established a relatively strong case for the use blockchain, we are increasingly shifting from the question of whether blockchain should be used to what kind of blockchain should be used. More clear differentiation of these three blockchain types would help us answer that question.

Limited research was found on public blockchains' implementation, in practice, in the financial services sector. Some of the earlier research on Bitcoin discounted the technology as impractical for the financial services sector, however much has changed

since then. Even with Société Générale's first steps into public blockchain implementation for bond issues, research has been left notably outdated on public blockchain use in the financial services sector. Consequently, a large part of the information on current developments came from news outlets and not academic papers. As we update our knowledge on public blockchains, further research should be conducted to reflect these changes. Moreover, the majority of research still focuses on Bitcoin, and to a lesser extent, Ethereum. Additional in-depth research on other public blockchains would be beneficial, as it would give an insight into the different ways to structure public blockchains.

The interoperability of public blockchains and cryptocurrency volatility mitigation should also be researched, as public blockchains' success in the financial services sector heavily depends on their scalability and practicality. For example, it would be interesting to research whether the high volatility of cryptocurrencies could be counteracted in day-to-day operations via some form of indexing, or other means, assuming cryptocurrency volatility will not abate.

References

Aggarwal, R. (2017). Blockchain and Financial Inclusion: The role blockchain technology can play in accelerating financial inclusion. *Georgetown University Center for Financial Markets and Policy*. Available at: <http://finpolicy.georgetown.edu/sites/finpolicy.georgetown.edu/files/Blockchain%20and%20Financial%20Inclusion%20120417.pdf>

Ahl, A., Yarime, M., Tanaka, K., & Sagawa, D. (2019). Review of blockchain-based distributed energy: Implications for institutional development. *Renewable and Sustainable Energy Reviews*, 107(November 2018), 200–211. Available at: <https://doi.org/10.1016/j.rser.2019.03.002>

Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018). Applications of Blockchains in the Internet of Things: A Comprehensive Survey. *IEEE Communications Surveys and Tutorials*, PP(X), 1. Available at: <https://doi.org/10.1109/COMST.2018.2886932>

Auer, R. (2019). Beyond the Doomsday Economics of “Proof-of-Work” in Cryptocurrencies. *Federal Reserve Bank of Dallas, Globalization Institute Working Papers*, 2019(355). Available at: <https://doi.org/10.24149/gwp355>

Avgouleas, E., & Kiayias, A. (2019). The Promise of Blockchain Technology for Global Securities and Derivatives Markets: The New Financial Ecosystem and the ‘Holy Grail’ of Systemic Risk Containment. *European Business Organization Law Review*. Available at: <https://doi.org/10.1007/s40804-019-00133-3>

Baydakova, A. (2019). *French Lender Societe Generale Issues \$112 Million Bond on Ethereum - CoinDesk*. [online] CoinDesk. Available at: <https://www.coindesk.com/french-lender-societe-generale-issues-112-million-bond-on-ethereum> [Accessed 16 May 2019].

Belinky, M., Rennick, E., & Veitch, A. (2015). *Santander InnoVentures – Fintech 2.0 Paper*. 20. Available at: <http://santanderinnoventures.com/fintech2/> [Accessed 16 May 2019].

Bheemaiah, K. (2017). *The Blockchain Alternative*. Paris: Apress, p.58. ISBN 978-1484226735

- Bilder, M. (2018). *Making Cryptocurrency More Environmentally Sustainable*. [online] Harvard Business Review. Available at: <https://hbr.org/2018/11/making-cryptocurrency-more-environmentally-sustainable> [Accessed 16 May 2019].
- Bitcoin Volatility Index (2019). *Bitvol.info*. Available at: <https://bitvol.info/> [Accessed 21 May 2019].
- Bowe, S., Gabizon, A., & Green, M. D. (2019). *Financial Cryptography and Data Security* (Vol. 10958). Available at: <https://doi.org/10.1007/978-3-662-58820-8>
- Brakeville, S. and Perepa, B. (2018). *Blockchain Basics: Introduction to Distributed Ledgers*. [online] IBM Developer. Available at: <https://developer.ibm.com/tutorials/cl-blockchain-basics-intro-bluemix-trs/> [Accessed 16 May 2019].
- Browne, R. (2019). *Apple and Tesla shares on the blockchain could be the next big thing in crypto*. [online] CNBC. Available at: <https://www.cnbc.com/2019/01/07/bitcoin-security-token-and-sto-explained.html> [Accessed 16 May 2019].
- Buterin, V. (2015). *On Public and Private Blockchains*. [online] Blog.ethereum.org. Available at: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/> [Accessed 16 May 2019].
- Chauhan, A., Malviya, O. P., Verma, M., & Mor, T. S. (2018). Blockchain and Scalability. *Proceedings - 2018 IEEE 18th International Conference on Software Quality, Reliability, and Security Companion, QRS-C 2018*. Available at: <https://doi.org/10.1109/QRS-C.2018.00034>
- Chester, J. (2019). *Will Security Token Offerings Be The Future Of Raising Money?*. [online] Forbes.com. Available at: <https://www.forbes.com/sites/jonathanchester/2019/02/19/will-security-token-offerings-be-the-future-of-raising-money/#4ad7b6161826> [Accessed 16 May 2019].
- Christensen, C. (2019). *Disruptive Innovation*. [online] Clayton Christensen. Available at: <http://claytonchristensen.com/key-concepts/> [Accessed 16 May 2019].
- Davradakis, E., & Santos, R. (2019). *Blockchain, FinTechs and their relevance for international financial institutions*. Available at: https://www.eib.org/attachments/efs/economics_working_paper_2019_01_en.pdf

Deloitte (2018). *Breaking blockchain open Deloitte's 2018 global blockchain survey*. Available at:

<https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-2018-deloitte-global-blockchain-survey.pdf> [Accessed 16 May 2019].

Demirors, Meltem (2017), Oxford Blockchain Strategy Programme, Saïd Business School, University of Oxford, UK, Available at:

<https://www.getsmarter.com/presentations/uk/oxford-said/whatstakeholders-are-involved-in-the-blockchain-strategy-system> [Accessed 16 May 2019].

Dib, O., Brousmiche, K.-L., Durand, A., Thea, E., & Hamida, E. Ben. (2018).

Consortium blockchains: Overview, applications and challenges. *International Journal on Advances in Telecommunications*, 11(1–2), 51–64. Available at: <http://kei-leo.com/wp-content/uploads/2018/08/iaria-2018.pdf>

Evans, J. (2015). *Decentralize All The Things!* – TechCrunch. [online] TechCrunch.

Available at: <https://techcrunch.com/2015/01/10/decentralize-all-the-things/> [Accessed 16 May 2019].

Facebook IQ. (2016). *Millennials + money: The unfiltered journey*. (January).

Available at:

https://fbinsights.files.wordpress.com/2016/01/facebookiq_millennials_money_january2016.pdf

Fanti, G., & Viswanath, P. (2019). *Decentralized Payment Systems: Principles and Design*. Available at: [https://dtr.org/wp-content/uploads/2019/01/2019-01-16-](https://dtr.org/wp-content/uploads/2019/01/2019-01-16-Decentralized-Payment-Systems-Principles-and-Design.pdf)

[Decentralized-Payment-Systems-Principles-and-Design.pdf](https://dtr.org/wp-content/uploads/2019/01/2019-01-16-Decentralized-Payment-Systems-Principles-and-Design.pdf)

Frankenfield, J. (2018). *Consensus Mechanism (Cryptocurrency)*. [online]

Investopedia. Available at: <https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp> [Accessed 16 May 2019].

Frankenfield, J. (2019). *Smart Contracts: What You Need to Know*. [online]

Investopedia. Available at: <https://www.investopedia.com/terms/s/smart-contracts.asp> [Accessed 16 May 2019].

Gencer, A. E., van Renesse, R., & Sirer, E. G. (2017). Short paper: Service-oriented sharding for blockchains. *Lecture Notes in Computer Science (Including Subseries*

Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Available at: https://doi.org/10.1007/978-3-319-70972-7_22

Goldfeder, S., Kalodner, H., Reisman, D., & Narayanan, A. (2017). *When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies*. (Section V), 1–19. Available at: <http://arxiv.org/abs/1708.04748>

Guegan, D. (2017). *Public Blockchain versus Private blockchain*. HAL Id : halshs-01524440 Centre d' Economie de la Sorbonne Documents de Travail du Public *Blockchain versus Private blockchain*. Available at: <https://halshs.archives-ouvertes.fr/halshs-01524440/document>

Hays, D., & Valek, M. (2019). *Crypto Research Report, January 2019*. Available at: https://www.resource-capital.ch/fileadmin/reports/2019/Crypto-Research-Report-January_2019_EN.pdf.pdf

Hewlett Packard (2016). *Blockchain in the financial services industry*. Available at: <http://blockchainlab.com/pdf/4AA6-5864ENW.pdf> [Accessed 16 May 2019].

Hughes, A., Park, A., Kietzmann, J., & Archer-Brown, C. (2019). Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms. *Business Horizons*, 62(3), 273–281. Available at: <https://doi.org/10.1016/j.bushor.2019.01.002>

Imbrex (2017). *Sharding, Raiden, Plasma: The Scaling Solutions that Will Unchain Ethereum*. [online] Available at: <https://medium.com/imbrexblog/sharding-raiden-plasma-the-scaling-solutions-that-will-unchain-ethereum-c590e994523b> [Accessed 16 May 2019].

Irrera, A. (2019). *Blockchain consortium Hyperledger loses members, funding: documents*. [online] Available at: <https://www.reuters.com/article/us-blockchain-consortium/blockchain-consortium-hyperledger-loses-members-funding-documents-idUSKBN1E92O4> [Accessed 16 May 2019].

J.P. Morgan (2019). *Quorum | J.P. Morgan*. [online] Available at: <https://www.jpmmorganchina.com.cn/country/CN/EN/Quorum> [Accessed 16 May 2019].

Jun, M. (2018). *Blockchain government - a next form of infrastructure for the twenty-first century*. Available at: <https://doi.org/10.1186/s40852-018-0086-3>

Kjærland, F., Khazal, A., Krogstad, E., Nordstrøm, F., & Oust, A. (2018). An Analysis of Bitcoin's Price Dynamics. *Journal of Risk and Financial Management*, 11(4), 63. Available at: <https://doi.org/10.3390/jrfm11040063>

Kruglova, I.A. & Dolbezhkin, V.A. Oct 2018, "Objective Barriers to the Implementation of Blockchain Technology in the Financial Sector", IEEE, , pp. 47.

Kulhari, S. (2018). Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity. Baden-Baden, Germany: Nomos Verlagsgesellschaft mbH. Available at: <http://www.jstor.org/stable/j.ctv941qz6>

Kuo Chuen, D. L. (2017). Fintech Tsunami: Blockchain as the Driver of the Fourth Industrial Revolution. In *SSRN*. Available at: <https://doi.org/10.2139/ssrn.2998093>

Lindsey, N. (2018). *Blockchain and Its Impact on the Future of Cyber Security*. [online] CPO Magazine. Available at: <https://www.cpomagazine.com/cyber-security/blockchain-and-impact-on-future-cyber-security/> [Accessed 16 May 2019].

Mao, D., Hao, Z., Wang, F., & Li, H. (2018). Novel Automatic Food Trading System Using Consortium Blockchain. *Arabian Journal for Science and Engineering*, vol. 44, no. 4, pp. 3439-3455. Available at: <https://doi.org/10.1007/s13369-018-3537-z>

Moody's (2018). *Announcement: Moody's: Blockchain disruption to have mixed credit implications for global banking systems*. [online] Available at: https://www.moody's.com/research/Moodys-Blockchain-disruption-to-have-mixed-credit-implications-for-global--PR_381249 [Accessed 16 May 2019].

Nakamoto, S. 2019. *Bitcoin*. Available at: <https://bitcoin.org/bitcoin.pdf> [Accessed 16 May 2019].

OECD. (2018). *OECD Blockchain Primer*. Available at: <https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf> [Accessed 16 May 2019].

Polymath.network. (2019). *Polymath - ST20*. [online] Available at: <https://polymath.network/st20.html> [Accessed 16 May 2019].

Prashanth Joshi, A., Han, M., & Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing*, 1(2), 121–147. Available at: <https://doi.org/10.3934/mfc.2018007>

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. (2018). Everything You Wanted to Know about the Blockchain: Its Promise, Components, Processes, and Problems. *IEEE Consumer Electronics Magazine*. Available at: <https://doi.org/10.1109/MCE.2018.2816299>

Société Générale. (2019). *Societe Generale issued the first covered bond as a security token on a public blockchain*. [online] Available at: <https://www.societegenerale.com/en/newsroom/first-covered-bond-as-a-security-token-on-a-public-blockchain> [Accessed 16 May 2019].

Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., ... Kim, D. I. (2019). A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access*, 7(Vm), 22328–22370. Available at: <https://doi.org/10.1109/ACCESS.2019.2896108>

Wharton. (2018). *How the Blockchain Will Impact the Financial Sector - Knowledge@Wharton*. Available at: <https://knowledge.wharton.upenn.edu/article/blockchain-will-impact-financial-sector/> [Accessed 16 May 2019].

White, L. (2018). *British public don't trust banks 10 years after crisis, survey finds*. [online] U.K. Available at: <https://uk.reuters.com/article/uk-britain-banks/british-public-dont-trust-banks-10-years-after-crisis-survey-finds-idUKKBN1L11EL> [Accessed 16 May 2019].

Wild, J., Arnold, M. and Stafford, P. (2015). *Technology: Banks seek the key to blockchain | Financial Times*. [online] Ft.com. Available at: <https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64#axzz3qe4rV5dH> [Accessed 16 May 2019].

van Deventer, O., Berkers, F., Vos, M., Zandee, A., Vreuls, T., van Piggelen, L., Blom, A., Heeringa, B., Akdim, S., van Helvoort, P., van de Weem, L. & van de Ruit, D. 2018, "Techruption Consortium Blockchain – what it takes to run a blockchain together", European Society for Socially Embedded Technologies (EUSSET). Available at: https://dl.eusset.eu/bitstream/20.500.12015/3162/1/blockchain2018_06.pdf

Victor, F., & Lüders, B. K. (2019). Measuring Ethereum-based ERC20 Token Networks. *Financial Cryptography and Data Security*, Measurement. Available at: <https://fc19.ifca.ai/preproceedings/130-preproceedings.pdf>

- Yang, M., Zhu, T., Liang, K., Zhou, W., & Deng, R. H. (2019). A blockchain-based location privacy-preserving crowdsensing system. *Future Generation Computer Systems*. Available at: <https://doi.org/10.1016/j.future.2018.11.046>
- Yu, Y., Liang, R., & Xu, J. (2019). A scalable and extensible blockchain architecture. *IEEE International Conference on Data Mining Workshops, ICDMW, 2018-November*, 161–163. Available at: <https://doi.org/10.1109/ICDMW.2018.00030>
- Zamani, M., Movahedi, M., & Raykova, M. (2018). RapidChain: Scaling Blockchain via Full Sharding. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security - CCS '18*, 931–948. Available at: <https://doi.org/10.1145/3243734.3243853>
- Zhong, L., Wu, Q., Xie, J., Guan, Z., & Qin, B. (2019). A Secure Large-scale Instant Payment System Based on Blockchain. *Computers & Security*, 84, 349–364. Available at: <https://doi.org/10.1016/j.cose.2019.04.007>
- Zilliqa. Available at: <https://zilliqa.com/> [Accessed 20 May 2019].