Norwegian School of Economics

Bergen, 2018

Blockchain in Financial Markets and Intermediation

A Qualitative Exploratory Study of the Impact of Blockchain Technology on the Financial Market Infrastructure and Financial Services

Jørgen Brastad & Philip Alexander Stendahl

Supervisor: Tommy Stamland

Master Thesis in Finance

NORWEGIAN SCHOOL OF ECONOMICS

Abstract

A blockchain is an open, decentralized ledger that provides a cryptographically secure way of transacting without the need of trusted third parties. The technology has garnered a variety of claims and perceptions regarding the future of financial institutions. Originally introduced to circumvent the incumbent financial intermediaries, blockchain technology has increasingly attracted interest from the very institutions that it was meant to replace.

In this exploratory study, we seek to analyze the impact of blockchain technology on the current market infrastructure by conducting a literature review and in-depth interviews with experts and stakeholders from the financial industry. Our findings suggest that smart contracts can automate and potentially decentralize a variety of transactions. Moreover, the introduction of initial coin offerings has brought about a new means of peer-to-peer fundraising in a space previously dominated by venture capital firms, but financial intermediation will likely remain to support the effective functioning of financial markets by resolving information asymmetry.
Furthermore, we find that the distributed and immutable nature of blockchain technology provides a robust and secure infrastructure by increasing the integrity of data. This will interconnect institutions across financial markets by streamlining settlement- and verification processes and potentially expanding global financial services in ways previously neglected. The foundation of the financial system will, however, remain. We have considered various aspects such as regulatory concerns and market designs to unfold the extent of potential gains and limitations provided by blockchain technology.

We conclude that there are yet many unknowns with respect to the extent and speed with which blockchain technology will impact financial services and intermediation. However, the technology will improve efficiency in current infrastructures, as well as facilitate new decentralized ways of transacting.

Acknowledgements

This thesis was written as a part of the Master of Science program in Economics and Business Administration at the Norwegian School of Economics (NHH) and concludes both our studies. We have sought to get a better understanding of blockchain technology and the possibilities it brings. The writing process has been both interesting and challenging.

First, we would like to thank all our informants. Their time, insights and valuable input made writing this thesis possible.

Finally, we would like to express our gratitude to our supervisor, Tommy Stamland, for his insightful and valuable feedback throughout the research process.

Contents

List of Figures

List of Tables

1 Introduction

> *The one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A. The way I can take a $20 bill hand it over to you and then there's no record of where it came from.You may get that without knowing who I am. That kind of thing will develop on the Internet.*
>
> – Milton Friedman, (S. N. Hanke, 2014).

The emergence of blockchain technology can be traced back to the introduction of Bitcoin, a peer-to-peer electronic cash system proposed by the pseudonymous Satoshi Nakamoto (Nakamoto, 2008). Prompted by the lack of confidence in the financial system, Nakamoto introduced a decentralized system which intended to replace trusted third parties with cryptographic proof, thereby enabling parties to transact directly with each other. A reference to Nakamoto's distrust in the mainstream banking system can be found to this day in the Bitcoin network's very first block, the "genesis block." In it, he encoded the front page headline from that day's *Times* of London: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"(Redman, 2017).

The whitepaper titled "Bitcoin: A Peer-To-Peer Electronic Cash System" was published in the aftermath of the 2007-2008 financial crisis (Nakamoto, 2008). In 2007, Lehman Brothers reported record profits and revenue (Merced, 2017). The company's financial statements were endorsed by their auditor, yet, nine months later, the company was bankrupt. Lehman Brothers and the financial crisis stand as reminders of the potential cost of trusting the internally devised numbers of centralized entities (Casey & Vigna, 2018). Disintermediating financial transactions and making these powerful financial third parties obsolete was the very motivation for Nakamoto's electronic cash system. Advocates of blockchain technology promulgate the potential promise of the technology to overturn the entrenched, centralized financial institutions.

Blockchain technology has spurred many expectations about disintermediating the financial system, and as such, we were motivated to uncover and identify this notion by exploring its disruptive effect within financial markets. Our analysis will unfold the attributes of blockchain with respect to its integrity and applications that have made it possible to circumvent and replace trusted third parties by cryptographic mechanisms and self-executing contracts, consequently unlocking an alternative method to raise capital by privately issuing cryptocurrencies in the form of tokens, referred to as initial coin offerings. Moreover, as the crypto-economy is gaining broader acceptance among regulators, unbanked regions may experience increased access to financial services.
Attracted by the innovative technology, financial institutions have gauged its lucrative features to potentially reshape the financial market infrastructure.

While blockchain technology has been proclaimed as the solution to countless problems, our paper further aims to clarify the extent of its potential gains. The unique property of a distributed database increases transparency by sharing an immutable record of transactions across a network of participants. With a transparent and automated record of ownership, and without a single point of failure, blockchain possesses the possibility to enhance both the efficiency and security of the current underlying infrastructure. As such, we examine the potential cost-cutting cases within settlement processes and verification procedures of audit trails.

We analyze these topics by conducting a literature review and in-depth interviews with experts and other stakeholders. By sampling informants from relevant industries directed toward specific themes, we are able to collect a broad set of information within the field of financial services and information technology.

We hereby seek to analyze the impact of blockchain technology on financial intermediation and the financial system with regards to potential benefits and limitations.

2 Introduction to Blockchain Technology

In this section, we will explain the conceptual principles of blockchain technology, exemplified through Bitcoin, the very first blockchain. We will further elaborate on how different types of blockchain will differ in their attributes. Lastly, smart contracts will be introduced. This technical introduction will lay the foundation for the subsequent analysis of blockchain's potential in financial markets and intermediation.

2.1 Asymmetric Encryption and Digital Signatures

To explain the basic concept of blockchain, imagine a group of friends who keep a communal ledger to record their debts and payments. The ledger could be a piece of paper or a public ledger on the internet, which everybody in the community can access and to which they can add transactions. At a pre-determined time of settlement, payments are netted. This works well in a trusted community; however, more difficult implications arise within a group of untrusted individuals spread over a decentralized global network. If everybody has access to the ledger as well as the right to add transactions, how does one know that nobody will falsify payments to benefit themselves? This issue is essentially what is known as the Two Generals Problem or more generally the Byzantine Fault Tolerance and was for the first time solved by Nakamoto (2008) in his whitepaper: "Bitcoin: A Peer-to-Peer Electronic Cash System.
In the blockchain space, transactions are verified by encrypted digital signatures. To ensure the integrity of the signatures, Nakomoto used a mathematically asymmetric encryption method called public key cryptography (Sharma, 2018).

$$Signature = f(x, y) \tag{1}$$

$$Verify = f(signature, y, z) = TRUE/FALSE \tag{2}$$

where x = *Private key (constant)* y = *Message / Transaction ID* z = *Public key*

The signature is a function of both the message itself (e.g., transaction) and the senders identification, as seen in equation (1)(Lin et al., 2018). As a result, the public signature will always be different, preventing others from copying and reusing a signature to falsify transactions (Driscoll, 2013). Moreover, the verification will then include the public key, which identifies each sender to ensure that indeed the signature belongs to this person without actually seeing the private key, as shown in equation (2) (Lin et al., 2018).

2.2 The Blockchain Ledger and Network Consensus

Thus far, we have determined how transactions are verified and entered into the ledger. The next question is: "How does the blockchain know the amount of money or funds of each individual?" In the case of overspending funds, the transaction will fail to be verified and thus will be rejected. This requires knowledge of the entire history of transactions up to the point of verification (Driscoll, 2013). For this reason, each verified ledger is converted to a block, and all subsequent blocks of transactions are linked together with that block, essentially creating a blockchain. Thus, the account balance of an individual is computed by the underlying algorithms, simply by checking all valid transactions ever occurring on the blockchain (Driscoll, 2013). Consequently, users cannot spend more than they own, however, it is still possible to double spend because the transactions might not be in the correct order of which they were created (Driscoll, 2013).

In order to ensure that all transactions are correct, the network must agree on a single history where transactions are in the same order and that they have not been tampered with (Nakamoto, 2008). This is solved by the consensus algorithm. In the traditional financial system, transactions are recorded by a central authority such as a bank. In the blockchain world, the record of transactions are distributed to the entire network of *"nodes"*. The nodes refer to the participants of the network that are maintaining the blockchain. Each payment will then be broadcasted to the network for all other nodes to record on separate ledgers. The problem is that every node in the network should have the same copy of ledgers, including equal transactions and in equal order; if not it would be impossible to know which ledger is the correct one. This issue is solved by the proof-of-work algorithm, a cryptographic hash function that acts as a puzzle, granting the solver of the function the right to create a block,

such that all blocks of verified transactions are equal and in the same order. As such, a block of transactions will only be valid if it contains a proof of work. To connect the blocks in the right order, all blocks will be initialized with the previous solution of the proof of work such that each block is referenced by the subsequent block (Driscoll, 2013).

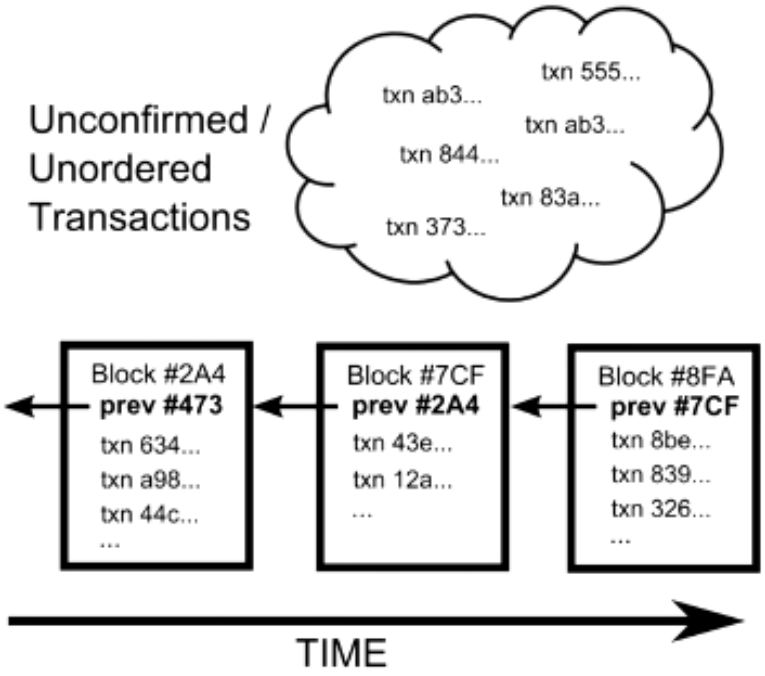

Figure 1: The blockchain. From "How Bitcoin Works Under the Hood," by Driscoll, 2013. Copyright 2013 by Scott Driscoll. Reprinted with permission.

In the Bitcoin space, the creators of blocks are called "miners". Miners compete to create the new blocks of transactions. Solving these hash functions requires significant computational power; thus, to incentivize users to create blocks, miners are rewarded with newly issued Bitcoin tokens, as well as receiving transaction fees from all the transactions included in the block. The mining function is regulated by built-in algorithms that adjust the difficulty of the problem that miners must solve (Antonopoulos, 2014, p. 2). A correct answer is found, on average, every 10 minutes, regardless of how many miners and hashing power are working on solving the problem. The rate at which Bitcoins are created is halved every four years, and the total supply of Bitcoins is fixed at 21 million coins.

Inconsistencies among the different copies of the ledger may arise if blocks arrive at nodes at different times, or in the unlikely event that two miners happen to solve the puzzle at the same time. The protocol resolves this by ensuring that nodes always select and try to extend the longest chain of blocks (Antonopoulos, 2014, p. 204).

2.3 Blockchain Architecture and Governance

Blockchains can be classified according to the different types of permissions that are granted to their network participants. Hileman and Rauchs (2017a) defined three major permission capabilities that must be considered when configuring a blockchain network:

- **Read:** Who can access the ledger and see transactions.
- **Write:** Who can generate transactions and send them to the network.
- **Commit:** Who can update the state of the ledger, that is, who can participate in the network as nodes.

The *read* capability determines the first classification of blockchain network type:

- **Open/Public:** Anyone can access the ledger and see transactions.
- **Closed/Private:** Access to the ledger is either restricted to an authorized set of participants or a limited set of nodes, or it may be fully private.

The *write* and *commit* capabilities, which together make up the verification process, determine the second classification:

- **Permissionless:** Anyone can generate transactions and update the state of the ledger.
- **Permissioned:** Only authorized participants, a subset of these, or the network operator can generate transactions and update the ledger.

2.3.1 Permissionless Networks

Permissionless blockchains are open networks operating in a global and untrusted environment, functioning on the crypto-economics ran by unknown users, incentivized to act honest (Hileman & Rauchs, 2017a). The prime example of such a network is Bitcoin. Everyone can access the blockchain, read every transaction that has ever occurred, and contribute to maintaining the system and add blocks to the chain by the mining mechanism (Tasca, Aste, Pelizzon, & Perony, 2016).

Blockchain types			Read	Write	Commit	Example
Open		*Public permissionless*	Open to anyone	Anyone	Anyone*	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorised participants	All or subset of authorised participants	Sovrin
Closed		*Consortium*	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple banks operating a shared ledger
		Private permissioned ('enterprise')	Fully private or restricted to a limited set of authorised nodes	Network operator only	Network operator only	Internal bank ledger shared between parent company and subsidiaries

Table 1: Main types of blockchains segmented by permission model. From "Global Blockchain Benchmarking Study," by Hileman and Rauchs, p.20, 2017. Reprinted with permission.

2.3.2 Permissioned Networks

In contrast to permissionless networks, a permissioned blockchain is centralized and controlled by a set of authorized nodes. In some cases, permissioned networks are open for anyone to access and read, however restricted from generating and committing transactions. Private permissioned networks are fully closed by authorized participants in a centralized environment, often an enterprise, or ran by more than one centralized node in the case of a consortium, typically consisting of several enterprises.

2.4 Smart Contracts

Smart contracts were introduced by Nick Szabo (1996), who described a smart contract as "*A set of promises, specified in digital form, including protocols within which the parties perform on these promises.*" Smart contracts are self-executing contracts enforced by cryptography. Szabo illustrated the concept of smart contracts by their primitive ancestor, the vending machine. The vending machine promises the customer goods in exchange for coins, through a simple mechanism. Anybody with coins can participate in an exchange with the vendor,

and the storage of the coins and contents is sufficiently safe so that vending machines can be profitably deployed.

The model of the smart contract can vary along a spectrum from being entirely embedded in code to being written in natural language with only an automated encoded payment mechanism (Smart Contracts Alliance, 2016). The set of promises referred to in Szabos definition is dependent on the smart contract model. The promises may comprise contractual terms, rules-based operations, or a combination of both. The promises are specified in digital form, that is, the contractual clauses are embedded as code within software and is operated electronically. A protocol in the form of an algorithm determines the set of rules governing how each party should process data in relation to the smart contract. Smart contracts will automatically execute, and once initiated the contracts will typically be irrevocable.

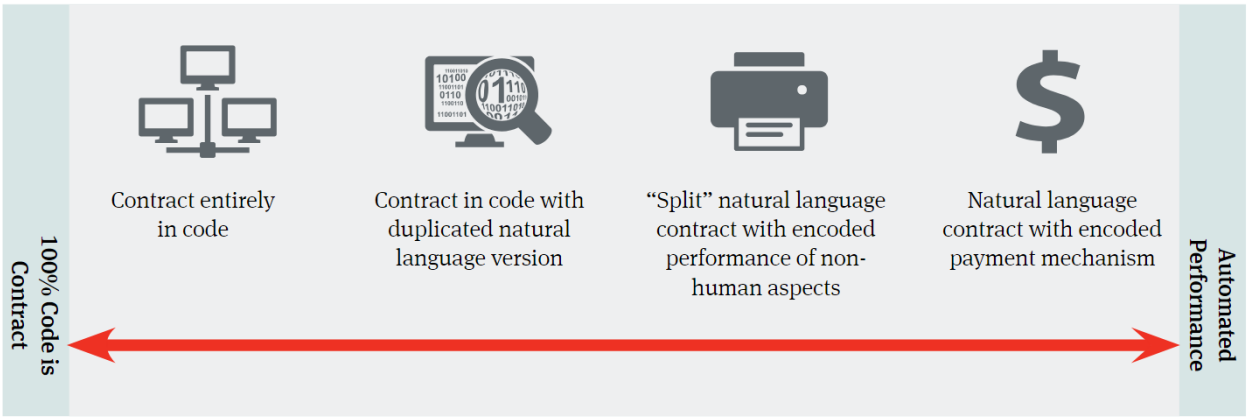

Figure 2: Smart contracts lie on a spectrum. From "Can smart contracts be legally binding contracts?" by Norton Rose Fulbright, p.13, 2016. Copyright 2016 by Norton Rose Fulbright. Reprinted with permission.

Smart contracts can be implemented both in distributed- and non-distributed ledger systems (Cant et al., 2016). In the realm of distributed ledger systems, the smart contract program logic is situated within a block (Smart Contracts Alliance & Deloitte, 2016).

3 Methodology

Our goal is to analyze and assess the impact of blockchain technology on banks and other intermediaries and uncover its potential within financial services. Due to the nature of this

research question, we chose to apply an exploratory qualitative methodology. Qualitative methods require observation and interpretation to uncover patterns of inter-relationships among previously unspecified concepts (Brannen, 2017) - a description suitable for a study exploring the recent phenomenon of blockchain technology. Furthermore, our methodological approach attempts to preserve unbiasedness, credibility, and validity by assessing common aspects such as heterogeneity and positive- and negative loaded bias of the sample.

3.1 Data Collection and Sampling

Our study aims to implement an in-depth analysis of our research topic, which requires information and insight from experts. Though, both surveys and interviews are appropriate research methods, interviews tend to provide higher quality of information due to their intimate, tailored and detailed manner (Walle, 2015). It is therefore a natural choice for us to conduct interviews with a representative sample of expert informants as a primary source of data, whereas secondary sources of data will be obtained from the existing literature, providing the foundation and intellectual justification of our research topic.

For our sample, we invited people from various areas globally, including economists, computer scientists, and lawyers, and with various backgrounds and respective expertise in the financial industry (see Appendix B). With this strategy we constructed a heterogeneous sample, which is in line with research methods explained by Saunders, Lewis, and Thornhill (2016), as this strategy allows us to describe and explain key themes that emerge in the collection of data. Furthermore, Saunders et al. (2016) suggested that a sample size of 12-25 should be sufficient when conducting interviews, and accordingly to stop sampling when no new information or themes are obtained from the data.

3.1.1 Interviews

Walle (2015) described three different types of interviews: unstructured, semistructured and, structured. Highly structured methods, the most rigid, scripted forms, might blend into surveys, whereas semistructured and structured methods have many similarities, such as open-ended questions to specialized informants. While the semistructured method is more

bound to an agenda, unstructured interviews are often seen as in-depth interviews, giving the informants more freedom to respond in any manner they see fit (Boyce & Neale, 2006). This flexibility provides the interviewer with the ability to effectively communicate and gather data from a diverse and unexpected array of information that is not limited to an agenda. Our study aims to assess a specific research question in a specific industry, geared to carefully selecting a tailored sample and gathering relatively specific information, thus arguably fitting both interview approaches. However, unstructured interviews often resemble sophisticated and specialized conversations between peers, thus requiring higher expertise of the interviewer, as suggested by Walle (2015). As a result, the study may lack validity as our research largely relies on the expertise of our informants. Carrying out a semistructured approach may therefore provide the best value for our research. Additionally, this method allows for a more specific agenda, directed toward our research question and simultaneously providing freedom to our informants to respond in an idiosyncratic manner (Walle, 2015). Note that the views and opinions expressed by our informants in this paper do not necessarily reflect those of the various companies.

3.2 Biases, Credibility, and Validity

A significant consensus exists in the world of methodology: researchers must preserve a neutral stance, meaning that research studies are to be reported in an impartial and objective manner, as pointed out for example by Walle (2015). With this in mind, it is important to construct a heterogeneous and representative sample in order to capture different perceptions and correspondingly limit subjectivity.

Another way to ensure objectivity is to control for positively- and negatively loaded informants, which we have done by incorporating control questions into our agenda (see Appendix C). Accordingly, we are able to alleviate some or all of the biases caused by this tendency. Moreover, in accordance with Saunders et al. (2016), informants should be able to prepare themselves for the interview by receiving a brief list of themes to be discussed. Our interview request therefore provide all key themes that were to be discussed (see Appendix A), allowing the informant to prepare and collect information that otherwise could not easily be obtained immediately.

According to Payton (1979), sampling techniques is one of the key considerations in terms of external validity. That is, if the findings of a study are to be legitimately generalized, the sample must truly be representative of the whole population. However, generalization is a rather difficult task in qualitative research, and as such, interpretation and possible applications may be left to the readers perception. Consequently, generalization requires adequate reported results to ensure the credibility of the research and furthermore, Walle (2015) pointed out the importance of the sample in the setting of informant-oriented reality. This is often the case in a qualitative study, as there may be more than one truth based on the subjective perspectives of the informants. In contrast to quantitative research, where "the one and only truth" has to be consistent, qualitative methods aim to capture a particular reality based on consistent agreement by the informants' perceptions. In this regard, by collecting various data from a carefully selected heterogeneous sample of experts as described above, we may be able to aggregate the subjective data into a consistent truth.

4 Financial Market Infrastructure

Blockchain technology has spurred a variety of discussions regarding the impact on the financial system and the future of financial intermediation. Banks and other financial intermediaries have streamlined the financial system for centuries. Over the past few years, however, technological evolution has challenged the traditional market by facilitating peer-to-peer platforms as well as regulatory shifts such as PSD2, which allows tech-giants to deliver payment services. Moreover, the emergence and diffusion of blockchain technology could potentially undermine the conventional system. Its decentralized system has created a new foundation of economic trade where parties interact in nearly untrusted networks with no centralized authorities.

4.1 Fundamental Concepts of Financial Intermediation

Greenbaum and Thakor (2007) defines financial intermediaries as entities that "intermediate between providers and users of financial capital." The fundamental explanation for our need

for financial intermediaries is that we live in a world of imperfect information. Since the 13th century, banks have existed as centralized intermediaries connecting those with funds and those without (Haldane, 2013). Financial intermediaries alleviate problems associated with asymmetric information, as described by Akerlof (1970), through screening, monitoring, selection and diversification of risk (Garbade et al., 2012).

Financial intermediaries connect complementary transactors and allocate capital to its presumed best use. These activities are referred to as *brokerage* and *qualitative asset management*, respectively, and are fundamental to financial intermediation (Greenbaum & Thakor, 2007). The brokerage function of financial intermediaries alleviates informational problems both before and after the two parties to a transaction enter into a contract.

The former, *precontract informational asymmetry*, involves adverse selection and duplicated screening. Adverse selection may arise in the case of borrowers overstating their creditworthiness, which in turn may result in the lender compensating for this by increasing the loan interest rate. Consequently, low-credit-risk borrowers are the most likely to turn elsewhere, thus leaving the lender with only "lemons." By performing various credit risk assessments, a financial intermediator can intermediate between borrower and lender, thus minimizing this adverse selection problem.

Duplicated screening relates to situations in which adverse selection may be avoided by individuals conducting the same costly screening procedures. Financial intermediation could make such potentially wasteful expenditure unnecessary by exploiting the re-usability of information. Furthermore, the potential cost savings of reusing information scale with size and any skill advantage the intermediator has over the general populace would increase its relative advantage (Greenbaum & Thakor, 2007).

In regards to resolving information asymmetry, the brokerage function is essential within the primary market, that is, issuing new securities and initial public offerings (IPOs). As described by Garbade et al. (2012), seeking finance in the primary market requires the involvement of several financial intermediaries that support the roles such as analyzing demand, structuring and designing the funds to be borrowed, type of funds (debt or equity), features of debt securities (e.g., maturity and coupon rates), management of cash flows and validation, and monitoring of performance.

During a transaction, the parties may act in an opportunistic manner which damages the interest of the counterpart. As such, there remains a risk of *post-contract information asymmetry*, potentially leading to moral hazard, which is difficult to observe for the exposed party, as described by Greenbaum and Thakor (2007). Further, they point out that borrowers may be motivated to select exorbitantly risky projects because a disproportionate amount of downside risk is absorbed by the bank, consequently increasing the risk of future default. Financial intermediaries may alleviate such post-contract moral hazard by monitoring and evaluating borrowers' business operations and financial conditions and may also, in certain circumstances, intervene in strategic decisions and operations (Greenbaum & Thakor, 2007).

Qualitative asset transformation relates to the transformation by financial intermediaries of asset attributes, such as duration, divisibility, liquidity, credit risk, and numeraire (Greenbaum & Thakor, 2007). In this manner, financial intermediaries provide a better alternative to finding a counterpart for every transaction. When financial intermediaries purchase a mortgage financed through deposits, deposits are in principle exchanged for mortgages (Greenbaum & Thakor, 2007). The deposits represent issuance of liability, and have different attributes to that of the mortgage. Thus, attributes of the assets are changed, and the intermediary is compensated for the service via the interest rate spread between deposits and mortgages.
Noteworthy, is that, despite differentiating between brokerage and asset transformation as separate intermediation services, the same intermediaries can perform both, even in combination (Greenbaum & Thakor, 2007).

A commercial bank is an example of an entity whose business model is primarily based on qualitative asset transformation. This model involves trusting these banks to safeguard customers' money and to guarantee future transactions and the withdrawal of their funds. Deposits that may be withdrawn without prior notice are referred to as *demand deposits*. Additionally, commercial banks act as distributors of currency to the market, constituting the role of administering the community's payments (Greenbaum & Thakor, 2007). The asset side of the balance sheet largely consists of future claims on lent capital, typically to private customers and small- and medium-sized enterprises (SMEs), as larger corporations generally rely more on directly placed debt, as suggested by Diamond (1991).

Start-up companies and entrepreneurs are often unable to obtain funds from banks due to credit constraints and are therefore financed by venture capitalists who specialize in the financing of entrepreneurial companies (Greenbaum & Thakor, 2007). Hellmann and Puri (2002) show that the value added by venture capitalists in the development of start-up companies have proven significantly beneficial. Venture capital-backed companies such as Apple, Yahoo, and Intel are examples of companies which have proven to be very successful in the development of their organizations. Venture capitalist provide two essential attributes to start-up firms: capital and management expertise (Greenbaum & Thakor, 2007). Venture capitalists will typically have an equity claim in the firm in order to actively engage in and promote certain business processes and support the development of management (Greenbaum and Thakor (2007); Hellmann and Puri (2002)), thereby preventing potential moral hazards.

4.2 Emergence of Blockchain Technology

4.2.1 Network Integrity and Trustworthiness

Throughout history, we have placed our trust in banks and similar institutions and expected them to facilitate frictionless exchange without having to worry about incentives of moral hazard. For decades, trust has been the foundation of banking and intermediation built up by customer relationships and reputation and was said to be impossible to replicate, as pointed out by Garg (2018). In his article on Bob's Guide, an online finTech platform, Garg explained how trust alone might not be sufficient to compete against IT companies, referring for instance to a survey by Toit and Burns (2017), suggesting that consumers find big technology companies, such as Google, Amazon and Facebook, more trustworthy than banks.
Furthermore, the emergence of Bitcoin may potentially have shifted trust further away from intermediaries towards the cryptographic mechanisms of blockchain. The proof-of-work concept has manifested the possibility of trading directly between two parties without the need of a trusted third party by solving the Byzantine fault tolerance. The idea of removing intermediaries was exciting for many actors, as a decentralized financial system could change the market infrastructure entirely, and the emergence of Bitcoin was precisely that trigger to spur the expectations of a "trustless" market, undermining the strong economic efficiency of relational contracting and financing affiliated with the current centralized market. How-

ever, this phenomenon is relatively controversial, as the notion of trustless exchange is often misunderstood, a perspective also shared by one of our informants.

> *Many do not understand blockchain. Many do not understand what blockchain really does. Many talk about blockchain being a "trust-machine," and that you will have confidence in the machine. Trust is subjective. I can trust someone or something that you or somebody else do not trust. It doesn't mean that [the blockchain] is trustworthy. However, verification, on the other hand, means either "yes" or "no." That is binary. And binary objects can be handled by machines. That's the key to blockchain. We can have a variety of data to verify, not have confidence in. Trust has nothing to do with the blockchain world.*
>
> – Bjørn Bjercke, *EY*

Most blockchain networks facilitate peer-to-peer exchange without the need of trusting any intermediary party, but it is important to note that trust and integrity of a blockchain network is limited to the underlying cryptography (Hileman & Rauchs, 2017a), that is, the verification mechanism, as explained by Bjørn Bjercke. In the Bitcoin realm, this means placing trust in a decentralized network of nodes. Everyone may join the network and act as an operator of the blockchain, thus validating transactions through the consensus algorithm, and it will function as "trustless" as long as the majority of the network is controlled by honest nodes, or as Nakamoto (2008) puts it, *"The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes."* This refers to the 51% attack, which we will discuss in more detail in section 5.1.2.

To preserve network integrity, institutions are developing their own permissioned blockchains, where trust is yet again placed in a centralized authority. In a permissioned network, investors have to trust the operator(s) and/or the validators, such as in the Ripple network.[1] Another permissioned solution, is the R3 consortium, facilitating a distributed ledger infrastructure across several institutions.[2] Although the network is permissioned, its integrity is distributed

[1] Ripple connects banks and payment providers through the RippleNet and additionally facilitates exchange with its own digital currency, Ripple XRP. See: https://ripple.com

[2] R3 is an enterprise software firm, facilitating distributed ledger technology, whose consortium is the

within the consortium where several institutions serve as nodes in the network, thereby engendering a more decentralized effect compared to fully private blockchain networks.

Permissioned blockchain solutions are particularly beneficial for what may arguably be the primary challenge of blockchain; interacting with off-chain data. Blockchains function on their own respective cryptographic assets (e.g., Bitcoin and Ethereum), commonly referred to as "native tokens." These tokens only exist within the blockchain and are therefore protected by cryptographic algorithms, thereby eliminating the need for a trusted third party. However, implications arise when dealing with the outside world. In the blockchain realm, real-world events do not exist, meaning that someone will have to pass information about these events or assets to the chain. For instance, if an individual is insured against flight delays or cancellations and these events actually occur, this would be considered an off-chain event, hence the encoded algorithms cannot know what happened to the flight unless this information is transferred to the blockchain.

> *Obviously, you have an immutable blockchain, and everyone knows that you know, this is the data and it has never been altered. But when you enter the data into the system, this is the weak link.*
>
> – Stylianos Kampakis, *UCL Centre for Blockchain Technologies*

> *[Blockchain] only has an overview of everything created on the blockchain itself and can track what's happening on the blockchain. So, once something is transferred to it, like an asset that does not live native on the blockchain, you will need an intermediary that you have to trust, and then you lose some of that security provided by blockchain... Many talk about tracking physical assets on a blockchain but even if you verify that the asset has switched hands on a blockchain, nothing is enforcing that asset, in other words, verifying that the person who's actually supposed to own the asset actually received it.*
>
> – Johan Torås Halseth, *Lightning Labs*

largest collaborative group of its kind in financial markets. Information on its DLT solution, R3 Corda, can be found at: https://www.corda.net

This suggests support for intermediation, as a trusted third party will be required to mitigate that vulnerability. Blockchain technology may thus circumvent third parties in the case of native exchanges but cannot, however, solve the trust issue of non-native events. As such, an intermediary will be required as a trusted third-party to generate a link to the real world. This may also include *"tokenization"* which is the process of representing off-chain assets on the blockchain, similar to issuing securities or public offerings. A brokerage could thus support the structuring, designing and selling the asset being tokenized. In this regard, Hileman and Rauchs (2017a) points out the importance of determining who has the right to issue non-native assets on the blockchain and to clarify whether they need to be fully backed in custody. However, once the asset is on the blockchain, much of the manual intervention such as managing cash flows of tokenized securities and performance valuation, may be mitigated and streamlined.

Thus far, there is no decentralized solution to solve the problem of off-chain assets, often referred to as the "oracle problem." This particular issue is widely recognized among public blockchain platforms, because it brings you back to square one: trusting an intermediary party, thereby eliminating the decentralization nature of blockchains.

> *To transfer data into the blockchain, is attempted to be solved by the so-called "oracle service." ... Basically, you have an information source which everybody in the network trusts, and that's something you actually don't like, at least in the original blockchain mindset where you shouldn't need to trust the network. However, once you need information from the outside world, on which everybody agrees, you'll need an information source to verify that information.*
>
> – Peter Frøystad, *Fintech Innovation*

In this regard, Thomson Reuters, a multinational mass media and information firm for professional markets, has developed a "smart oracle" to act as an information source in the blockchain and distributed ledger ecosystem. This application, called BlockOne IQ,[3] collects market data, such as share prices, exchange rates, cryptocurrency rates, corporate actions,

[3]For more information, see: https://blockoneiq.thomsonreuters.com/

and accordingly provides these data to the blockchain. BlockOne IQ is currently a beta version, only compatible with Corda, Ethereum and Quorum, but as stated by the developers themselves, other platforms will follow according to demand. This opens up the possibility for an oracle service within decentralized ecosystems, though it contradicts it's very own nature. It would, however, be a viable solution to include real-world market data into the blockchain space.

4.2.2 Global Payments

In our previous discussion, we showed that trust and integrity of the blockchain networks are limited to, but yet powerful in, its native space. As such, Bitcoin, Ethereum, and many other cryptocurrency systems have challenged banks and other financial institutions on their field of transactions. The global payments infrastructure entails cumbersome and inefficient processes, which result in high costs and up to five days settlement time (He et al., 2017). The open-source architecture of permissionless blockchains has created an ecosystem in which payments can be sent near-instantaneously and with lower costs than in the traditional system and without any third-party involvement. However, while the Bitcoin network tended to enjoy transaction fees of less than $0.10, increased demand of Bitcoin led to significantly higher fees with the median fee peaking at almost $35 per transaction at the time of the Bitcoin boom at the end of 2017, as seen in Figure 3.[4]

Figure 3: *Bitcoin and Ethereum median transaction fees, USD*

The spike in transaction fees did illustrate the often cited scalability issues embedded in the

[4]Figure retrieved from BitInfoCharts - Cryptocurrency statistics: https://bitinfocharts.com/

Bitcoin network (Kasireddy, 2017; Simonite, 2017). Its hard-coded block-size limit of one megabyte results in a maximum throughput of seven transactions per second (Croman et al., 2016). This raises the issue of how the Bitcoin network will handle the transactions if the network continues to grow. For cross-border payments, Hileman and Rauchs (2017b) found that 86% of surveyed payment companies use the Bitcoin network as their primary payment rail. Bitcoin is only one of many cryptocurrencies, and there is the possibility of other networks with different consensus mechanisms more suited for scalability taking the place of Bitcoin as the leading cryptocurrency. In the case of Bitcoin, *Segregated Witness* went into effect in August 2017 to alleviate some of the capacity problems the network experienced. Segregated Witness is a software upgrade that separates the cryptographic transaction signatures from the rest of the blockchain data, thus making transactions smaller in size (Lee, 2018b). Consequently, more transactions can be included in a block. The separated signatures are not counted toward the block-size limit, which effectively makes Segregated Witness a block-size increase. If all transactions use this format, the network's capacity would roughly double (Lee, 2018b). Adoption of the software among users has been slow, however, with 40% of Bitcoin transactions using Segregated Witness as of May 2018 (Ivancic, 2018). Segregated Witness provides a breathing room, however, further increases in network activity will require more drastic changes to avoid congestion.

The Lightning Network is the community's long-term solution to Bitcoin's scalability problem and can expand the Bitcoin network's capacity by moving transactions off-chain (Lee, 2018b). The protocol operates as a second layer, and while designed for Bitcoin, it could be implemented on top of any blockchain (Stark, 2016). Payment channels are created through two-of-two multi-signature (multi-sig) transactions on the blockchain, allowing the two parties to instantly transact with each other without broadcasting the individual transactions to the entire network. Multi-sig mechanisms require multiple private keys to execute a transaction and are typically implemented such that two out of three private keys must be provided (Davenport, 2015).

Every payment channel generates one transaction to open it, and a second to close it. These payment channels enable near-instant transactions at a rate potentially far surpassing what is currently processed by any payments system, and at very low- or no fee at all. By connecting the payment channels a network is created, enabling users to make payments to many dif-

ferent people through a chain of open payments channels (Lee, 2018a). Multi-sig and smart contracts ensure that the user can send funds through other users functioning as nodes on the network without needing to trust them as intermediaries. However, similarly to Segregated Witness, adoption of Lightning may take time (Lee, 2018b). Further, the technology is not necessarily well suited for all kinds of transactions, as emphasized by one our informants:

> *It does not replace all the possibilities you have with a regular on-chain transaction; first, both endpoints in the payment, both the payer and the recipient, must be online to make a payment. Payments, where you send money to someone who is not online, is not possible with lightning, at least not today, but maybe it will be possible in the future. Thus, you still have on-chain payments that can be of great use. High-value payments are usually much easier to get done on regular on-chain payments because it depends on the capacity on the route between the recipient and the sender, and then, the chance that the capacity is available will be progressively less the greater the payment is. Hence, Lightning is best suited for quick transactions up to a certain size.*
>
> – Johan Torås Halseth, *Lightning Labs*

The fact that both sender and recipient must be online when the payment is made may be a challenge for certain kinds of payments. In the case of payments between mobile devices, for instance, this may not be case:

> *One thing may be mobile to mobile; if you pay your friends, both must be online when that payment is made, and there may be some technical limitations on the current mobile operating systems, where Apple, for example, does not allow apps to run in the background. Thus, there are some small technical questions related to it, but there are suggestions for solutions. So I do not think that there is any particular kind of payment that cannot be done on lightning, it's more the technical aspect that you have to work around, and to make sure both are online when done.*
>
> – Johan Torås Halseth, *Lightning Labs*

Further, the hashing power entailed by Bitcoin's proof-of-work consensus mechanism results

in high energy consumption. As of June 18, 2018, the network consumes electricity close to the electricity consumption of Chile (Digiconomist, 2018). The Lightning Network will reduce the number of transactions recorded on the blockchain as they are taken off-chain. However, this will not represent a significant reduction in electricity consumption, as nodes use little energy to record transactions (Copeland, 2018). Thus, as long as miners contribute hashing power to the network, energy consumption per transaction will remain high.

While the Lightning Network and other solutions are being developed to resolve the widely recognized scalability implications, Bitcoin and any other cryptocurrencies may not necessarily function as a universally viable means of payment.

> *Right now, crypto assets are a little too volatile to pose a threat to existing payment systems and fiat currencies. They don't enjoy the same amount of trust as current systems do, but we see developing critical mass in terms of innovation... For Bitcoin, it's really too volatile to become an everyday currency, but possibly over time it will, since its value proposition is solving the double spending problem and it does it very well. We'll see second-layer applications, we'll see developments in that space that will make it easy to use, that will make it ready for mass adoption where the users won't even know they are using Bitcoin, or won't even know they are using blockchain. They will be able to digitally trade, transact, do commerce and cross-border transactions, as if they are using cash.*
>
> – Miguel Cuneta, *SCI Ventures Inc.*

The diffusion of blockchain-related payment solutions has put pressure on banks and other payment providers, forcing them to adapt in order to stay competitive against fintech entrants. The provision of financial services associated with cryptocurrencies among banks is commonly suggested by our informants.

> *"What I think we will see first, most importantly, and what will distinguish those who are future-oriented from the others, is who will start to offer services to the clients associated with [cryptocurrencies]. Five percent of Norway's population states that they own a cryptocurrency, but there are no Norwegian banks that can keep it for*

you.... So I think what's going to happen is that banks are going to see opportunities in this space, and they will offer services in that niche."

– Thorbjørn Bull-Jensen, *Menon Economics*

In fact, this year, U.K. based investment bank, Barclays, made a deal with Coinbase, one of the worlds largest cryptocurrency exchange and wallet provider. However, the banking industry in particular is a heavily regulated industry and therefore any engagement in the decentralized blockchain space may put these institutions at risk. Cryptocurrencies may be used for criminal activities such as money laundering or may be used on unregulated platforms that provide illegal products. If such activities are neglected and not overseen, financial institutions cannot deliver any related services due to these risks. In fact, this appears to be a common impediment to the widespread adoption and provision of financial services. According to EY (2018), which conducted a poll at EY's Global Blockchain Summit in New York, regulation is the greatest barrier to broader blockchain integration. This was also emphasized by one of our informants:

[Crypocurrency-related financial services] I think that cryptocurrencies have come to stay. And then we must deal with it in a proper manner.... Our problem is that authorities have not yet been able to decide, but we hope they will very quickly. Many in our management have publicly called for the Financial Supervisory Authority to come up with rules so that we know what we have to deal with. So, what we've told our customers for the time being is that, right now, we cannot provide these services, but we hope the authorities are able to decide so we can do so in the future. So, I think banks will eventually have to [provide financial services] of these cryptocurrencies.

– Lasse Meholm, *DNB*

Regulatory support is a critical element in the blockchain and cryptocurrency space. Thus far, financial services associated with cryptocurrencies seem to be limited, however, not absent. With guidance from the Swiss Financial Market Supervisory Authority, Hypothekarbank Lenzburg, a commercial bank in Switzerland, recently announced their acceptance of

account holders who are engaged with cryptocurrencies (Kelso, 2018). Also outside the cryptocurrency space, institutions are recognizing the benefits provided by blockchain and are increasingly focusing on delivering customer experience, for instance by facilitating instant payments to meet consumers' demand for immediacy, as suggested by one of our informants:

> *I would also like to say that from a perspective of customer experience, perhaps one of the biggest challenges we face today is that customers have less and less patience when entering a payment, invoice, or transaction... If you're in the store and need money and therefore want to [make a transfer], it is not sufficient if the money is transferred to the counterparty in a day or two. Therefore, immediate payments are introduced, it's not blockchain technology, but it serves the same purpose, to ensure that settlement and transactions take place on a real-time basis.*
>
> – Marte Kopperstad, *Nordea*

Blockchain technology and cryptocurrencies may undermine some of the functions of intermediation, however, as pointed out by Batlin, Jaffrey, Murphy, Przewloka, and Williams (2016), the tendency of falling bank revenues from transactions has been present for years, long before blockchain. As discussed previously, intermediation is more than simply payments.

> *I think people dont really have full grasp of the complexity of our financial systems and institutions.... Banks are far more complex than just payment processing institutions and storing of my monthly salary. I mean, they do a lot more for society and I think this is important to remember as well.*
>
> – Leeor Groen, *Blockchain Valley Ventures*

Despite the original intentions of circumventing intermedation, developments of blockchain seem less about decentralization and more about improving current market practices.

> *"...this time however, it is the banks and insurance companies who lie on the edge, at least initially. But I don't think blockchain will remove workplaces to any large extent. New workplaces will emerge. I think banks will survive and also the current financial ecosystem will remain for a very long time. We will not remove it.*

> *We didn't develop cryptocurrencies to replace the current market. We developed cryptocurrencies to build a new way doing things."*
>
> – Bjørn Bjercke, *EY*

Blockchain technology also provides significant solutions for intermediaries to stay competitive by enabling low fees and near-instantaneous transactions, thereby increasing customer satisfaction. Blockchains and cryptocurrencies, however, are currently limited by regulatory power. Common grounds have to be established to achieve a sufficient trade-off where both users and the operators of financial markets can benefit.

4.2.3 Smart contracts

Smart contracts may have the potential to replace and streamline certain contracts by its self-executing mechanism. A smart contract is linked to the blockchain and executed in accordance with some predetermined- and automatically validated conditions. This can potentially mitigate some aspects of contract management related to monitoring and enforcement. However, smart contracts are not apt for every type of contract. In a sense, smart contracts are "complete" as they provide little flexibility. Any condition has to be encoded ex ante, thereby anticipating any conceivable scenario which necessitates changes to the contract (Chu, Ream, & Schatsky, 2016). As described by Grossman and Hart (1986), "complete" contracts refer to contracts in which future outcomes are known by every agent. As such, contractual relations will require proper management throughout its lifecycle. Minahan (2005) defines contract lifecycle management as "*the process of systematically and efficiently managing contract creation, execution and analysis for maximizing operational and financial performance and minimizing risk*", which may include performance measure (e.g., monitoring, analyzing data, reporting), variations, and dispute resolution. Blockchain-based smart contracts, such as those running on Ethereum, cannot be altered, nor can they be discharged, due to the immutability property of blockchain.

Developing long-term and complex smart contracts may therefore be significantly challenging. This is not a surprising observation, considering that contracts often deviate considerably from ex ante initialization, as presented by Williamson (1993). Therefore, the immutabil-

ity property of smart contracts may entail certain risks. Any flaw of incompletion can be exploited, such as in The DAO attack. The DAO is a particularly known decentralized autonomous organization. A decentralized autonomous organization has no centralized authority, which is achieved by codifying both the rules and the decision making of the organization(Falkon, 2017). The entity operates through smart contracts, and its financial transactions and rules are encoded on the blockchain. Approximately one month after the launch, a hacker discovered a bug in the code and thereby managed to drain The DAO of ether tokens worth over $60 million at the time.

The solution to solve or fix a bug that has already occurred on an immutable blockchain is often to hard fork the chain. If the majority of the network is in favor of a fork, the chain would be reversed to the point prior to the bug's origin, thereby creating a parallel blockchain. Notably, in the aftermath of The DAO attack, a minority group of nodes disagreed about the fork and therefore continued the original chain, which today is known as Ethereum Classic. The resolution of hard forking entails consequences for the value of the tokens, but as suggested by Antonopoulos (2016) most blockchains will be resilient to such attacks and activities in the long-run. Forks occur due to disagreements about or flaws in the blockchain protocol. To avoid hard forking, Tezos, a decentralized blockchain platform, developed a built-in autonomous governance structure, allowing the protocol to remain flexible and adopt to changes. Stakeholders are able to vote on proposals to modify the rules of the network, which are automatically implemented upon network consensus (Breitman, 2017).

The immutability of smart contracts depend on the rules of the network, and how the consensus mechanism operates, as suggested by one of our informants, Mariana Bontempo. That is, the rules originate from the protocol itself. Hence, a permissioned blockchain may provide more flexibility.

> *You could have relatively complex smart contracts as long as you have a relatively centralized system, in order to reverse and stop a transaction, if the automation should prove to be a result of a bug, hack or opportunistic operator. When it comes to entirely autonomous and self-enforcing contracts, such as those running on Ethereum, I am very sceptical of the possibility to develop considerable complex contracts, and history thus far has shown how problematic it is, for instance with The*

> *DAO, which ran exactly as programmed. So, it shows what problems are involved with codes and unclarity.*
>
> – Torbjørn Bull-Jensen, *Menon Economics*

As such, it is possible to incorporate a multi-sig arrangement into the contracts which can alleviate some of the implications self-enforcing contracts entail by providing contracting parties some control over the execution of the contract. However, relying on a trusted third-party contrasts the decentralized trust made possible by the blockchain.

Further, Mainelli and Milne (2016) suggested that short-term smart contracts would be a more viable solution in the near future, thereby endowing the possibility to encode a smart contract in its entirety by limiting the time frame of potential uncertainty, dispute and opportunism. In this regard, Bjørn Bjercke proposed a solution to integrate several short-term contracts:

> *So we can develop small, very small smart contracts which trace a small specific instance. But you'll have to develop many of them, in order for enforcement to condition on a previous triggered event, subsequently, trigger another event ... etc. So this way, you could develop very complex contracts.*
>
> – Bjørn Bjercke, *EY*

As such, long-term smart contracts can be developed by limiting contingencies of each contract; thus, if the outcome of a contract deviates from the predetermined conditions of the subsequent contract, the series of contracts will automatically cease. One such solution can be found in Hyperledger. Having one original contract distributed among trading parties, Hyperledger Fabric facilitates a break-down into subcontracts, which at any point in time are linked to the original parent smart contract.

As pointed out by Peter Frøystad, dividing contracts into subcontracts is merely an acceptable programming practice, as it will make it easier to update the terms. Appropriate development of smart contracts will thus be a critical role within contract management. If there is an oversight, the outcome might as well be more dramatic than in a traditional contract

(Deloitte, 2016). According to Breitman (2017), formal verification of on-chain codes may prevent flaws in the codes, although it is not guaranteed. Formal verification allows developers to mathematically prove the correctness of the smart contract codes, but are however, no substitution for human analysis and reasoning (Posnak, 2017). Nonetheless, the distributed property of blockchain can provide stakeholders with real-time updates on relevant matters and developments, which the Australian National Audit Office (2012) described as a critical role within contract management.

Furthermore, there is yet one crucial element that amplifies the difficulties of smart contracts, namely external sources, as we discussed in the previous section. The blockchain cannot verify that all parties or stakeholders involved in the contract meet their obligations and that the contract is progressing in accordance with deliverables or any other terms if these are subject to external data.

> *"Obviously, there are going to be issues with smart contracts because the information that is on the chain, that's what you're able to do with smart contracts. If the information is off-chain, it has to be verified on the chain. So until it gets on the chain, it cannot be verified."*
>
> – Collin Thompson, *Intrepid Ventures*

> *"[Regarding off-chain assets] Smart contracts seem to provide an automated solution to many different kinds of transactions, for instance invoicing, supply chains, legal, etc. However, when there are humans involved, someone still needs to sign this off. So you're not solving the problem, If you just assign this responsibility to a single entity, a single person or a company, you're not really solving the problem, you're deferring the problem to something else. So I think this is something where blockchain cannot really help. This has to be solved on a different level."*
>
> – Stylianos Kampakis, *UCL Centre for Blockchain Research*

The oracle problem seems to limit the usage of smart contracts. However, a smart contract may be constructed to trace external data that serve as an oracle, as pointed out by one of our informants, who put forth an example involving insurance for shipping purposes.

> *[I]f we initially assume frictionless piloting and a storm suddenly hits, there will be several oracles, such as world weather report, Google weather, sky weather, and the such, which subsequently report and together build an oracle which interacts with the smart contract and accordingly triggers the insurance... A good oracle is aggregated by several instances, which then computes an average value.*
>
> – Bjørn Bjercke, *EY*

This example illustrates one solution to eliminate some dimensions of the weak link between the blockchain and the physical world. However, this a relatively simple contract, involving some instances of external data that may be traced online. As long as these external sources are traceable by the blockchain, an aggregated smart contract may streamline much of the intermediary functions involved in contract management, however, not completely remove them. There will be a need for human involvement in the event of a dispute, re-negotiations or variations in the contract terms due to unforeseen circumstances.

Disputes could, for instance, relate to the meaning of the code. Even if a sophisticated natural-language contract were successfully encoded in its entirety, disputes could still arise if the code did not perform as the involved parties anticipated. In a distributed, permissioned, blockchain, an administrator might be granted the power to execute arbitrary or remedial transactions onto the ledger. Thus, with the consent of the parties to the contract, the administrator may resolve any disputes related to contracts on the ledger. The consent to granting the administrator this right could be either restricted to the particular contract or it could be included in the terms and conditions required to accept, in order to participate in the permissioned ledger. The provision for delegating the dispute to an arbitrator may be encoded in the smart contract or expressed in a natural language-version of the contract (Norton Rose Fulbright, 2016). As Norton Rose Fulbright (2016) points out, however, the latter assumes congruence between the natural language version and the delegation mechanism in the contract code. Such a solution may prompt disagreements regarding the delegation mechanism, in which case recourse to the courts could be necessary.

If there is no administrator, regardless of whether the distributed ledger is permissioned or permissionless, or if the parties to the contract do not consent to assigning the dispute resolution power to the administrator, dispute resolution becomes significantly more challenging.

In such cases, a dispute resolution mechanism could be embedded into the smart contract itself, by allowing for encoded rules in the code to trigger delegation to some other arbitrating entity.

Within the spectrum of possible smart contract models, many challenges arise. It is not clear that encoding a complex commercial contract is viable. Legal phrases, of which legal analysis may be necessary for interpretation, may not be suitable for encoding within a smart contract (Norton Rose Fulbright, 2016). This is further highlighted by Werbach and Cornell (2017), who argued that certain contractual clauses such as "best efforts" cannot be expressed through formal logic as they imply human judgment. They further make the point that enabling computers to interpret and evaluate contracts in a way similar to humans is the domain of artificial intelligence. Multi-sig arrangements could reintroduce human judgment in resolving disputes relating to uncertainty. However, as argued by Werbach and Cornell (2017), this does prevent some of the benefits of the approach as the smart contract then resembles a conventional contract with an arbitration clause. One of our informants further highlight the challenge of standardizing smart contracts:

> *If you are transferring it in codes, that is quite challenging especially since there are different standards, different ways of doing it. And then we're still locating harmonization, so you are creating sort of new deltas if you like, but there are initiatives like the Accord Project, which is doing I believe a great job and trying to harmonize in particular the way the encoding is being done and smart contracts are set up, and the mechanics behind it. So, there's a way to go, but I believe its moving there, but again its a totally new concept to translate legal elements into code.*
>
> – Dr Guenther Dobrauz, *PwC Legal*

The Accord Project is an initiative to develop open source technology and standards, both technical and legal, for smart contracts (Aitken, 2017). The project has released its first working prototype, Ergo, the infrastructure of which is "blockchain agnostic", that is, it is not tied to any specific blockchain protocol (Hernández, 2018). Such standards, developed and supported by leading law firms, could help parties avoid potential pitfalls and repeating mistakes, as argued by Werbach and Cornell (2017). Further, the prototype enables lawyers to

write out the logic of their contracts in natural language before it is translated and structured into code. However, it is still more technical demanding to translate the contract with Ergo than simply writing it it natural language. Thus illustrating that the adoption of legal smart contracts may shift the expertise and services provided by lawyers towards aiding in the creation of smart contracts.

Despite the moniker "smart contract," it is not necessarily correct that it represents a legally binding contract. The distributed and pseudonymous nature of many blockchains raises particular problems. According to the common law of many jurisdictions, a contract must be entered into by a person having the legal capacity to do so by an authorized person such as a corporation to be legally valid (Norton Rose Fulbright, 2016). Additionally, some jurisdictions require sufficient certainty regarding the identity of the contracting party. Identifying the other party to a smart contract on a permissionless blockchain may be challenging.

Norton Rose Fulbright (2016) have analyzed whether smart contracts give rise to legally binding contractual relations. They found that this may vary depending on both the jurisdiction and the type of smart contract at issue. In particular, separate "follow-on" contracts may not necessarily bring about a legally binding contract in some jurisdictions. A "follow-on" contract refers to a contract brought about by provisions in a previous smart contract that enter the parties into a new contract, for instance concerning some specific performance.

4.3 The Token Economy

4.3.1 Peer-To-Peer Exchange

Technological innovation has made it easier and faster to gain access to liquidity through alternative funding channels in instances when intermediation funding cannot be obtained. One well-known type of peer-to-peer lending is crowdfunding. Crowdfunding may be described as the practice of acquiring capital for a project by raising small amounts of money from a large number of investors. This type of funding can be shown to eliminate frictions of traditional loans, for instance those related to geographical distance (Agrawal, Catalini, & Goldfarb, 2011) and interest rate costs (Butler, Cornaggia, & Gurun, 2010). Such fundraising platforms have complemented financial markets by improving credit supply efficiency,

as pointed out for example by Butler et al. (2010).

For the scope of our study, we divide crowdfunding into two types, which we consider the most relevant in terms of potential impacts on financial intermediation and their roles described previously: (i) lending-based crowdfunding, involving interest bearing debt, and (ii) equity-based crowdfunding, involving shares of a company. According to CrowdExpert (2015), peer-to-peer lending represented roughly 75% of the total funds collected from crowdfunding platforms in 2015, while equity-based crowdfunding counted for merely 7%. Equity rewards of future returns involve high complexity and uncertainty in terms of information asymmetry and have thus been substantially penalized by regulation. In fact, equity-based crowdfunding initially was widely restrained due to the high risks involved; hence it was limited to only accredited investors who coincided with wealth requirements. However, government initiatives toward alternative financing have been rising and have led fintech businesses to develop innovative solutions that are more accessible and faster than traditional funding methods (Tasca et al., 2016). For instance, in 2016, the Financial Conduct Authority authorized SyndicateRoom, one of the largest crowdfunding platforms in the U.K., thereby allowing institutions to go public through that platform (Williams-Grut, 2016).
Independent of the fund-raising choice, it is important to note that peer-to-peer funding significantly entails information asymmetry, which notably restrains access to financing. We previously argued that intermediaries mitigate adverse selection, as they are experts in these fields and therefore are more informed than are borrowers. As such, Berger and Gleisner (2009) found that intermediaries who were paid by peer-to-peer lending platforms in the U.S. improved information symmetry, thereby reducing credit spreads of the borrowers.

Empirical evidence shows that a significant increase of crowdfunding relates to credit supply shocks, in the event of economic distress. In line with much empirical work examining ventures' availability to funding, Tasca et al. (2016) developed a model analyzing the relationship between venture attributes and the likelihood to use crowdfunding, which proved to have a greater effect when banks were stressed from economic impairment. The model significantly supports three variables: creditworthiness (credit rating received from credit agencies), size of the venture, and the fraction of tangible assets. Smaller firms with low credit rating and tangible assets were most likely to use crowdfunding due to credit constraints, while

more mature ventures relied on bank debt and IPOs in the case of equity funding. This is in line with Diamond (1991), whose findings we alluded to earlier, and suggests a positive relationship between reputation and access to funding.

From this discussion, it seems that for fintech start-up firms and SMEs in particular, commercial bank loans and venture capital sources have been superseded by crowdfunding and peer-to-peer lending. In contrast, larger and more creditworthy firms likely stick to bank loans and conventional methods of seeking financing in the public market where intermediary support has proven excessively important. This indicates that these types of financial institutions seem to hold up against the disrupting trends of peer-to-peer and crowdfunding.

4.3.2 Initial Coin Offerings

The initial coin offering (ICO) mania took hold during 2017. By the end of 2017, $6 billion had been raised in 871 ICOs (ICOdata, n.d.-b). In contrast, no more than $94 million had been raised in 30 ICOs during 2016 (ICOdata, n.d.-a). An ICO is a form of crowdfunding, in which a company sells a quantity of privately issued cryptocurrency to investors in the form of tokens. The tokens are most commonly sold in exchange for other cryptocurrencies, but they also can be exchanged for fiat currency.

An ICO is a hybrid transactional form between venture capital, IPO, and crowdfunding. The funding is typically undertaken at an early stage, akin to venture capital. The tokens are also commonly liquid assets saleable to a broad group of people, comparable to an IPO. At the same time, the funding resembles crowdfunding, as the investors receive a token granting access to a platform if it is ever built. As the organization issuing the token can design its use in any manner the organization likes and the token may represent any asset, the type of claim the token represents can vary from equity to debt, or some hybrid of the two. Mougayar (2017) defined a token as *"a unit of value that an organization creates to self-govern its business model, and empower its users to interact with its products, while facilitating the distribution and sharing of rewards and benefits to all of its stakeholders."* In much the same way that sovereign governments issue currency and determine its terms and governance, organizations may set the terms and governance concerning their privately

issued cryptocurrency. Tokens can serve a wide range of roles and purposes within the crypto economy where they operate, and a token can be used in any way the organization designing it decides.

The terms "cryptocurrency," "token," and "coin" are used interchangeably, both in our thesis and in the blockchain literature. Cryptocurrency refers to a digital currency in which encryption techniques are used to verify and secure the transfer of funds and generation of units of currency. Thus, all coins and tokens are regarded as cryptocurrencies. However, the term *cryptocurrency* is in this regard something of a misnomer, given that a currency serves as a medium of exchange, as a store of value and as a unit of account. While the question of whether cryptocurrencies such as Bitcoin satisfy these technical requirements will not be addressed here, it should nevertheless be clear that many tokens do not meet that threshold. Tokens are designed to fulfill different purposes, and one of these may be to serve as what we commonly associate with a currency. However, the purpose is frequently to enable a network and to bring about its growth. The token would then be intended to have functionality within a particular network or application. A comprehensive framework for classifying tokens along several dimensions, presented by the think tank Untitled INC (n.d.), refers to such tokens as *network tokens*. Tokens could also be intended to represent an investment in either an underlying asset or the issuing entity, often referred to as *investment tokens* or *share tokens*.

The framework further suggests broadly classifying tokens as *usage tokens* and *work tokens* along the dimension of utility (Untitled INC, n.d.). These are subcategories of what are commonly referred to as *utility tokens*. It is also important to note that even though most tokens are referred to as utility tokens by their issuers, it should not be taken for granted that such is the case, as an emphasis on the token being a utility could be necessary for the token not to be regarded as a security by regulators (Euler, 2018). Usage tokens are tokens required to access a network and to use service features. This could be in the form of a fee to use the blockchain infrastructure, as is the case for both Bitcoin and Ethereum. The token can also be used as a payment method, enabling organizations to process payments inside these closed systems without going through traditional financial settlement options. As for work tokens, these enable individuals to contribute to the network. Tokens can be used as a unit value of exchange, allowing users to both earn value and spend it on services internal

to the ecosystem. The two classifications are not mutually exclusive, and tokens with both characteristics are aptly referred to as *hybrid tokens*.

The majority of cryptocurrencies are issued on top of another blockchain, or what is often referred to as the protocol layer. These are non-native protocol tokens, as opposed to blockchain-native tokens, or the blockchain level, such as Bitcoin. The most common example of non-native protocol tokens is the ERC20 standard, defining a common set of rules for tokens issued on top of the Ethereum blockchain. Raising funds through non-native protocol tokens is in principle very easy, and for the funding mechanism itself in the case of Ethereum one simply needs to create a wallet address in which to receive crypto-denominated funds without depending on any bank or third party service. To launch new blockchain-native tokens on new codebases is far more technically challenging. The most obvious example of this is the Bitcoin system, which was the pioneer. Another prominent example is Ethereum itself, which drew inspiration from Bitcoin but was engineered from scratch to be more programmable. Tokens can also be issued on new chains using forked code, that is, independently developing source code from another software system. Examples of this are Dash and ZCash, both tokens initiated on separate blockchains based on Bitcoin but having developed among other privacy-preserving innovations. Lastly, tokens may be issued on both a forked chain and forked code. Both Bitcoin Cash and Ethereum Classic are examples of this, where disagreements among the respective users and developers led to the creation of separate chains. The disagreements leading to the Ethereum fork raised fundamental issues regarding decentralized autonomous organizations, a particularly novel form of organization in which tokens could represent a claim.

The Decentralized Autonomous Organization (DAO) was launched in 2016 and intended to operate like a venture capital fund with no human governance (Falkon, 2017). The DAO was intended to allow anyone to pitch investment ideas to the community, and everyone with DAO tokens could vote on which projects to fund. Those holding DAO tokens would in turn receive rewards if the chosen projects returned profits.
The ICO of The DAO was launched with a 28-day funding window beginning April 30, 2016. During this window anyone could send Ether to a unique Ethereum wallet address in exchange for DAO tokens. During the funding window, 12.7 Ether was raised, which was

worth around $150M, making it a record crowdfund at the time.

It seems reasonable to ascribe parts of the rapidly increased attention ICOs have attained to the enormous profits associated with many high-profile projects. Those participating in the token sale of Ethereum in 2014, which raised $18.4 million over a period of 42 days, would have achieved a return of approximately 250,000% if tokens were held until the time of writing.[5] Brave, a web browser employing tokens as a means of payment among users, publishers, and advertisers, raised $36M in about 25 seconds in an ICO in 2017 (Adham, 2017). The price of the token quickly appreciated once it was listed on cryptocurrency exchanges, and after six days ICO participants could realize profits of nearly 600%. The return for those still holding the tokens would at the time of writing be almost 1,200%.[6] The largest raising of capital from token sales to date was that of Telegram, a messaging service advertised to preserve the privacy of its users. The company raised a total of $1.7 billion through two separate cryptocurrency presales in February and March 2018 (Liptak, 2018). But many projects have also fared poorly, and others have been outright scams from the very beginning. Among the outright scams are what have become known as exit-scams, where the founders run off with the money. The largest scam of this kind to date[7] was executed by the Vietnamese-based company Modern Tech, which allegedly stole $660M raised through the sale of a fictitious token (Suberg, 2018). In 2017 a coin aptly named PonziCoin raised more than $250,000, despite featuring a public declaration on its website that it was a scam (Kean, 2018). Not surprisingly, the founder took off with the contributed capital.

More than $6 billion was raised by ICOs in the first quarter of 2018 (Coindesk, 2018). Despite prevalent stories of scams, investors are apparently not put off. An analysis of 226 ICOs during 2017 found that only one in 10 tokens was in use following the ICO (Kharif, 2017). This does not in any way necessarily indicate malicious conduct, but might at the very least suggest unsuccessful projects or projects that did not necessitate a token. The latter was highlighted by one of our informants.

Many of the platforms that have been created do not have the need to have their own

[5] Calculated using prices in USD, June 22, 2014 to April 29, 2018.
[6] Calculated using prices in USD as of April 30, 2018.
[7] April 30, 2018.

> *coin. I have been contacted by many people who plan to make coin offerings from Norway and have asked me for advice. I ask them why they do not use ether or Bitcoin, because its use is only for payment. "No, we have to find out why we need a coin because we need something to sell." So you introduce unnecessary technical complexity by having an extra coin, unnecessary currency risk for those who use your platform, unnecessary hassle because you have to find the coin you need, just to have something to sell.*
>
> – Thorbjørn Bull-Jensen, *Menon Economics*

The apparent abundant use of tokens in blockchain projects could be at least partly explained by the ease associated with creating them that the Ethereum platform offers. Creating a token ready for listing on an exchange can be done in as little as one hour and costs no more than $30 (Nachamkin, 2017). A prevailing sentiment that having been an early investor in the big-name cryptocurrencies would have led to riches today could also contribute to explaining the somewhat euphoric situation seen both during 2017 and in the first two quarters of 2018, in which celebrities like Floyd Mayweather have been used to promote several ICOs, one even raising as much as $32M (Kharpal, 2018). At the same time, many of our informants indicated that projects with little concrete evidence other than marketing may contribute to there being relatively few successful ICOs. Such projects would naturally also be potential candidates for malicious intent. As expressed by one of our informants,

> *We have had a big rise in investments, and in my opinion, some projects and solutions that didn't have a proper base, meaning they were asking for money without having a solution in place or development team. So, they actually did not have anything except the white paper and the marketing website.*
>
> – Mariana Bontempo, *Applied Blockchain*

Many of our informants expressed a view that the valuations of ICOs during 2017 and the first two quarters of 2018 have been high. Both the accessibility of participating in ICOs and the extensive media coverage the phenomenon has received have been highlighted as contributing factors.

> *Obviously, one reason they're able to raise that much is the fact that for an ICO it's very easy to reach an international audience, it's very easy for anyone to invest whether they're in New York or Bangladesh or London or China or whatever, so that must have played a significant role. However, I think there's also a speculative element in it, because at some point in the previous year or so ICOs and cryptocurrency have been everywhere in the news, so I think many of the people investing in ICOs might not be entirely sure what they're getting into.*
>
> – Stylianos Kampakis, *UCL Centre for Blockchain Research*

A commonly highlighted aspect of ICOs among our informants is the way ICOs offer investors new investment opportunities.

> *[T]he entire crypto/blockchain community tries to open up the very attractive investment space of venture capital, and all those things that are ICO funded are by and large ventures from a risk-and-reward profile, so the idea behind this is that people like us, who understand the technology, or part of the technology, who want to benefit in that and who are conscientiously taking that risk should be able to do that, because previously the chances were not there, because the venture fund was only open to qualified investors; retail investors and nonprofessionals couldn't get in there, and that was sort of the democratization of the asset class, which ICOs brought about.*
>
> – Guenther Dobrauz, *PwC Legal*

While there historically has been no shortage of either high-risk investments or schemes set up to rid investors of money available to the general public, ICOs do offer retail investors previously unprecedented access to direct investments in start-ups. Fletcher (2017) suggested that the emergence of crowdfunding demonstrates an appetite among the general public to participate in the early growth phases of venture-stage issuers. ICOs are clearly one way for those interested to gain access to high-growth private companies. This is not to say that there are no other options for retail investors. In the U.S., exemptions were offered in 2016 from the requirement to register public offerings with the SEC, which allowed non-accredited

investors to partake as venture capitalists (Cowley, 2016). The exemptions are subject to several conditions, among which is limits on the amount sold to any investor over a 12-month period. The current limits are whichever are the greater of $2,200 and 5% of the lesser of annual income or net worth for investors with an annual income or net worth of less than $100,000 and 10% of annual income or net worth, but the aggregate amount sold not to exceed $107,000, for investors with both an annual income or net worth equal to or greater than $107,000 (SEC, n.d.). Further, the company issuing securities relying on these exemptions is limited to raising a maximum aggregate amount of $1,070,000 in a 12-month period. These changes have led to the creation of equity crowdfunding platforms such as Republic, a spin-off launched by AngelList to address crowdfunding for non-accredited investors. However, as argued by Barnett (2016), a $1 million funding cap fails to account for current start-up funding needs.

> *It's new channels that are being opened up, so I mean, people are really able to engage with and participate in a lot of investment opportunities that they haven't traditionally been involved in or haven't had access too.*
>
> – Leeor Groen, *Blockchain Valley Ventures*

The required minimum investment amount to participate in an ICO is decided at the discretion of the founders and thus varies. The sum, however, is commonly low, or there is no minimum requirement. The decentralized nature of ICOs may also overcome potential geographic barriers that traditional venture capital may entail. Wessel (2013) found that start-ups outside the traditional geographic venture capital hubs in the U.S. spend longer time searching for both Series A and Series B funding, as well as taking longer from the point of founding until the first publicly announced funding takes place, compared to their counterparts located within the traditional hubs. With ICOs the entire funding process typically takes place online, from marketing to the project's whitepaper. The only geofencing taking place is usually to avoid regulatory risk, most commonly by not allowing investors in the U.S. or China to participate. Not only can the process of attaining venture funding be simplified and hastened by the use of ICOs, but similar arguments may hold in regard to initiating an IPO. Regulatory oversight and requirements, in addition to often entailing a lengthy process,

may be both costly and themselves represent a separate, complicated task, distracting the founders and development team from launching the product itself.

Our informants varied in their view on ICOs as a threat to venture capital. Some saw it as a threat that potentially could replace the current industry:

> *[I]f there is a democratization, to use your word, of the access to capital why do I need an intermediary?*
>
> – Collin Thompson, *Intrepid Ventures*

This view is in concurrence with our argument outlining how ICOs allow people to invest directly in ventures in a previously unprecedented manner, and in many instances circumventing the current financial intermediaries altogether. Through 2017 and the first two months of 2018, start-ups related to blockchain technology[8] received more than 3,5 times as much capital from ICOs than from VC funding (Rowley, 2018), and in June and July 2017 ICO fund-raising even surpassed that of angel and seed VC funding for internet companies (Kharpal, 2017). A 2017 survey of 869 venture-backed start-up founders found that one in three founders believed ICOs could compete with traditional venture capital (State of Startups, 2017). Other informants viewed ICOs as an opportunity, rather than a threat, for VCs:

> *No, on the contrary, they just have to adjust their business. They've got a golden opportunity to pivot a little bit and join in something that is even bigger and better than ever. I think the world of crypto with ICOs and so forth has strengthened the position of venture capitalism to a much greater degree than it has decreased it.*
>
> – Bjørn Bjercke, *EY*

This view could arguably be supported by the fact that the ICO space has attracted participants in the VC industry. Renowned firms such as Andreessen Horowitz, Founders Fund, Sequoia Capital, and Union Square Ventures are investors in Polychain Capital, a hedge

[8]Companies classified in Bitcoin, ethereum, blockchain, cryptocurrency, and virtual currency categories.

fund investing in tokens (Shin, 2017). Blockchain Capital and Pantera Capital are examples of other investment firms with funds dedicated to investing in tokens. Additionally, there has been a trend among founders in the blockchain space towards launching token pre-sales ahead of the official ICO. This was emphasized by one of our informants:

> *What we see now is that a lot of VCs actually get exclusive access to the pre-ICO, or that they have like a first round where only VCs can invest and get tokens to an even better price.*
>
> – Lukas Wohlgemuth, *Strategy &, part of the PwC network*

This has been the case in Telegram's fund-raising; in its pre-sales of tokens to accredited investors, participants included established venture capital firms such as Benchmark and Sequoia Capital (Schleifer, 2018). Our informants further argued the benefits of receiving funding from VCs:

> *VCs doesn't only give you money, they also give you network and expertise. So I think they will be able to do a bit of both. Like always there's some part of the traditional VC business being disrupted, but at the same time many VCs, or some at least, try to hop on the bandwagon and also make direct investments in ICOs.*
>
> – Lukas Wohlgemuth, *Strategy &, part of the PwC network*

> *I think there is absolutely a place for venture capital and the support that they provide in terms of leadership, experience, knowledge and industry connections...*
>
> – Leeor Groen, *Blockchain Valley Ventures*

The advice and counsel offered by venture capital firms would still benefit many companies involved in the ICO space. Token investors, like public market investors, may leave the company at any time with little to show for the effort other than the money raised. In contrast, VCs will typically be committed to their investment over a longer period.

Many of the advantages inherent in ICOs as a way to raise capital are related to the cir-

cumvention of regulation the practice entails. Thus, there is a worry in the ICO space that regulators will crack down on token issuers for selling the public something that should have been registered as a security (Vigna & Casey, 2018). This was the case in September 2017 when Chinese regulators announced a ban on organizations from raising funds using ICOs (Martin, 2017). A substantial decrease in the price of many cryptocurrencies followed, especially for Ethereum, the most commonly used cryptocurrency to host ICOs. The ban also led several exchanges in China to delist ICO tokens and to suspend services concerning these tokens, such as withdrawals and deposits (Althauser, 2017).

Issuing unregistered securities violates the Securities Act of 1933, thus raising the issue of whether tokens are securities. The SEC made it clear in its investigative report on The DAO in July 2017 that the tokens sold by the organization were securities and therefore subject to federal securities laws, and consequently disclosure, registration, and other requirements that few ICOs have complied with (US Securities and Exchange Commission, 2017). The SEC noted that whether a token should be regarded as a security "will depend on the facts and circumstances, including the economic realities of the transaction." Consequently, not all ICOs will be considered unregistered securities. Virtually every ICO previous to this SEC report had operated on the assumption that the tokens they offered for sale were not securities. If regulatory uncertainty previously characterized the ICO space, the stance of the SEC did not do much to alleviate this.

Participants in the ICO space have sought solutions to mitigate the regulatory uncertainty. A collaboration among several firms in the industry has led to the invention of the Simple Agreement for Future Tokens (SAFT) framework. The framework is modeled on the Simple Agreement for Future Equity (SAFE).[9] A SAFT contract can be sold to accredited investors, promising investors delivery of the tokens once they are functional on a network (Batiz-Benet, Santori, & Clayburgh, 2017). Once the tokens are created and delivered to the investors, they may be resold to the public by the investors as well as by the developers. The framework brings structure and a standard to the token financing, thus allowing institutional investors to more confidently participate in this form of financing. It seems evident that many investors

[9] A type of contract that provides investors with rights to future equity, similar to convertible notes, but without its debt characteristics.

are participating in ICOs in anticipation of profits. Further, the realization of these profits will in most cases hinge on the ability of the developers to build a platform that attracts users. These are both factors that may meet the so-called Howey test, a criterion used to determine whether a transaction qualifies as a security (Bennington, 2017). The SAFT contract is a security, thus requiring compliance with securities laws. The resulting functional tokens are not, however. By attempting to avoid regulatory uncertainty using SAFT contracts, it is only accredited investors who get to participate in the initial funding process. To be considered an accredited investor in the U.S., one needs to fulfill requirements such as having an income of at least $200,000 or a net worth of at least $1,000,000 excluding one's primary residence (Electronic Code of Federal Regulations, 2018). Consequently, SAFT contracts are in our opinion a step away from the democratization of capital raising alluded to previously.

Evaluating ICOs represents a challenge for investors. With the circumvention of VCs and crowd-funding platforms, qualified due diligence may not occur. As argued by venture capitalist Rob Boardman (2017), the general populace may not be capable of effectively evaluating these start-ups. As most organizations issuing tokens have no product, the basis to evaluate the ICO relies on the information provided by the issuer in the white paper and other forms of communication. Further, social influencers are often engaged by the issuer to leverage a hyped market sentiment (Sehra, Smith, & Gomes, 2017). A plethora of websites and ratings agencies has emerged that analyze business models and development teams associated with ICOs. The rating agencies differ in their approach. ICORating.com delivers what is advertised as independent ratings by its own staff. Others, like ICObench, let anyone apply as an expert to conduct ratings. Such rating agencies could potentially alleviate problems related to asymmetric information and increase the legitimacy of ICOs. However, legitimate questions arise regarding the independence of these agencies:

> *They're more like media channels, in a sense that they provide an asset which is attention for a certain kind of experience, which is investing in an ICO. And they sell that to anybody who purchases it. So they will give you a good rating if you buy it.... Now the second part to that is, does that inform investors well? I would say no. So, are they needed? I would say yes. However, with the caveat that what needs to happen is that there needs to be a trusted source of verifiable information,*

> *and a track record of providing highly graded investor protection and transparency in ICOs, and to this day, there are a very few that do that.*
>
> – Collin Thompson, *Intrepid Ventures*

It is not clear that the current ICO rating agencies provide a trusted source of verifiable information to alleviate the problem of asymmetric information. This view also found concurrence with another of our informants:

> *I haven't come across a single rating agency that I would say is a reliable source in today's market, I mean just the incentives, the way the industry works and is evolving - how do you evaluate and compare an ICO?*
>
> – Leeor Groen, *Blockchain Valley*

Rating agencies have thus far not been subject to regulation nor monitoring. This raises the question of whether market forces will provide sufficient incentives for rating agencies to act as trusted investment advisers. At the very least, rating agencies may contribute to rid the market of frauds.

4.4 Concluding Remarks

As a novel phenomenon, blockchain has gained an enormous amount of attention, triggering a variety of perceptions and claims about the future of intermediation and financial services, some of which suggest that banks in particular will become redundant. The aftermath of the financial crisis challenged the trustworthiness of intermediaries, redirecting more confidence toward technology. As such, blockchain was often regarded as "trustless" and therefore possessing the ability to entirely disrupt financial markets. Indeed, markets are constantly affected by new emerging technology; however, blockchain has not yet proved to replace trust in its entirety. Trust is limited to the underlying consensus mechanism and thereby placed in the network. Furthermore, our analysis thus far shows that the key point of blockchain is a new way of verifying and auditing proof of ownership on a immutable history of records, which may streamline many processes.

The developments of blockchain, disregarding its contribution to peer-to-peer and crowdfunding, mostly affect the world of financial exchange. Bitcoin, Ethereum, Litecoin, and many other cryptocurrencies have proven that it is possible to transact directly between peers without the need for an intermediary and without necessarily trusting the counterparty. We therefore argue that blockchain technology may disrupt and replace certain dimensions of financial transactions.

Decentralized infrastructures additionally raise regulatory concerns, as dispute resolutions may be significantly challenging due to lack of authority, pseudo-anonymity, and immutability of such decentralized blockchain platforms. Arbitration may be needed in the event of a dispute, initialization of a contract must be conducted by a person having legal capacity in order for the contract to be legally valid, and finally, jurisdictions may require certain transparency to identify the contracting party. In this regard, smart contracts may require new and independent jurisdictions to coordinate the gap between identifiable legal phrases and meaning of codes.

ICOs have thus far offered investors new ways of investing directly in start-ups, as well as new and novel ways of organizing economic activity. Thus far mostly operating in a regulatory vacuum, the space has been characterized by both innovation and widespread fraud. Blockchain enables peer-to-peer capital raising, circumventing both venture capital and crowdfunding platforms altogether, and has consequently shown itself as a contender to the traditional financial intermediaries. However, as many of the appealing aspects of the ICO space may be related to the regulatory vacuum it has found itself in, the future of ICOs as we know them may hinge on the next step of regulators. Despite the substantial amounts of capital obtained by ICOs, the combination of expertise and financing offered by venture capitalists will remain in demand.

Nonetheless, most distributed ledger systems that are being developed seem to be less about decentralizing business processes, and more about building a shared infrastructure, upon which institutions and entities can collaborate using different blockchain frameworks, as shown in a study by Hileman and Rauchs (2017a). Blockchain technology has sparked many visions about the future of finance and intermediation. As our analysis has uncovered thus

far, blockchain technology will not cause intermediation to become redundant, but rather introduce an opportunity to embrace and adapt new ways of providing financial services.

5 Financial Technology

In the previous section, we found that blockchain arguably might be be a revolutionary technology that will disrupt and reshape the financial market infrastructure. The interest in the innovative technology has been growing exponentially since the launch of Bitcoin and has thus attracted the institutions that initially were intended to be circumvented. As such, we will examine the core attributes of blockchain technology as a standardized infrastructure capable of facilitating secure and robust business processes and additionally uncover whether blockchain technology may facilitate the provision of financial services to undeveloped nations.

5.1 Technological Infrastructure

Financial technology has experienced a steep growing trend in recent years, and accordingly most banks and other financial institutions invest significantly in digital transformation. Bansal (2012) found that banks in 2013 globally set aside nearly $13 billion for investments in digital channels, of which one-third was dedicated to mobile banking. That is, a lot of focus is directed toward customer experience and convenience by innovating front-end features, while the core operations are run by legacy systems, dating back to the 1970s (Mainelli & Milne, 2016). This trend has left banks with severe maintenance costs. Falato, Coumaros, Buvat, and KVJ (2013) estimates that banks spend 90% of their technology budgets on maintenance of legacy systems while having a significant number of personnel working on paper-based back-office processes.

> *We have the SEPA system for payments, we have Mastercard and Visa, and that's a really old system. It's from the 70's I guess.... I think blockchain will revolutionize that system and also give a chance to the start-up companies who move into a field with fewer costs because they can take the Ethereum blockchain, for instance, and*

work with it.

– Yusuf Barman, *KPMG*

Evidently, banks have neglected the digitization of their core infrastructure due to the long and cumbersome process of changing a company's core infrastructure which will have a significant impact on its day-to-day operations.

To change the core banking system is an enormous operation. We, therefore, do it in iterative steps... However, it is a huge and risky operation. I think that's why many banks have refused to do this; many have commenced and failed.

– Marte Kopperstad, *Nordea*

Much focus has been directed towards improving front-end applications such as mobile banking and other convenient applications for customers to better meet their needs, while inefficient back-office operations have resulted in costly processes, for instance emphasized by Falato et al. (2013). The same study also estimated that document management systems and digital signatures could improve manual and paper-intensive business processes. While these solutions aim to automate back-office operations and improve customer experience, the overall efficiency of the underlying infrastructure, however, remains in question.

5.1.1 Standardization and Universal Interoperability

To extract and exploit blockchain technology, a uniform standard is necessary, thereby facilitating a shared infrastructure that connects different institutions across the financial ecosystem. This may include collaboration among market participants and consensus on standardization of various asset classes, trading and settlement, accounting standards and record keeping (Schneider et al., 2016). This is essentially a crucial requirement to eliminate cumbersome, manual, back- and middle-office processes and move toward a more efficient and interoperable infrastructure.

Standards are important. In terms of payments, banks have been working for decades, maybe the 30-40 previous years in order to create standards. SWIFT has in some

way made a standard for interbank protocols for international payments... Around hundreds of millions of dollars have been used internationally to create standards for everyone to follow. That does not yet exist in the blockchain world. But it must come.

– Lasse Meholm, *DNB*

Companies controlling their own blockchain-implemented systems will still need to be able to exchange information or transaction information with other companies and digitally sign the transaction with other companies. There will be a standard or a few standards, just like Microsoft or Apple, that will generally be compatible with other companies' technology where you can sign inter-company transactions.

– Yusuf Barman, *KPMG*

Just like SWIFT (the Society for Worldwide Interbank Financial Telecommunication) or the internet and its universal language, TCP/IP, blockchain needs a common distributed ledger protocol on which it is possible to develop use-specific applications. Examples of such a solution are the ERC20 token standard for decentralized applications and permissioned solutions such as R3 Corda and RippleNet. However, as the latter solutions have gained increased popularity, markets have yet to establish a definite standard across the financial ecosystem.

While standardization initiatives are being developed and aggregated, Standards Australia may be the leading player striving to implement such initiatives. Its development of ISO/TC 307, which is being adjusted according to a series of consultations of 2016 and 2017, aims to create relevant international standards to support the broad use of blockchain technology (Meguerditchian, 2017). Much work is also put into the application level that facilitates interconnectivity among the many blockchain protocols.

What some [fintech companies] do is building a bridge between these different technologies. I'm sure more companies will do the same. So, if you have an application, for instance real estate turnover located in Ethereum and the payment located in

> *Hyperledger, then it is possible to connect the two together... I'm sure we will see more of these bridges being built between these technologies in order to connect the whole thing.*
>
> – Lasse Meholm, *DNB*

One such solution, as suggested by one of our informants, is called atomic swaps which uses a "Hashed Timelocked Contract" between two parties, allowing the exchange of cryptocurrencies of different blockchains. This contract uses a multi-signature mechanism to ensure both transactions are executed on the relevant blockchain (Peaster, 2018). Thus far, atomic swap transactions are only compatible with a few tokens such as Bitcoin, Decred and Litecoin and require both blockchains to share the same cryptographic hash functions (Nielsen, 2018). As such, having a standardized protocol would enhance interoparability between the various blockchain networks by interconnecting atomic swaps and second layer applications.

> *A lot of blockchains cannot be interoperable because they are doing different things. It's not just payments. For example, Ethereum is not really a payment system, unlike Bitcoin. So, I think that there are some different things going on like atomic swaps. And atomic swaps want different types of cryptocurrencies running on different blockchains to be interchangeable, instantly. Basically, if they are running the same consensus mechanisms, you will be able to swap them without going through third-party exchanges. So, I think thats one solution.*
>
> – Miguel Cuneta, *SCI Ventures Inc.*

Bulding a universal standard, upon which multiple institutions and countries can operate is a challenging task. As pointed out by Lasse Meholm, it took the financial system decades to reach the point at which it exists today. Blockchain technology has quickly grown its roots into the financial industry by aiming to interconnect the underlying infrastructures. The results may be game changing. The lack of interoperability in the current systems has led to high costs and inefficient processes. We will further discuss the rising benefits of an interconnected financial system, empowered by blockchain technology.

5.1.2 Security of blockchains: The consensus algorithm

Cyberattacks have increased exponentially in recent years, and unlike traditional bank robberies which happened rather infrequently and for which the consequences were limited to the bank being robbed, modern cyberattacks affect thousands of individuals and result in severe losses for corporations. Although the majority of such cyberattacks fail, corporations cannot afford the severe consequences if an attack were to be successful, as pointed out by Mathias Leijon, Nordea Global Co-Head of Corporate & Investment Banking, in an interview by Trocmé (2018). According to Statista (2018), losses from reported cyber crimes to the Internet Crime Complaint Center (IC3) have increased on average approximately 24% annually from 2013 to 2016, peaking at $1.330 million in 2016, and have an even greater increase going back to the early 2000s during the rise of the internet, as seen in Figure 4.

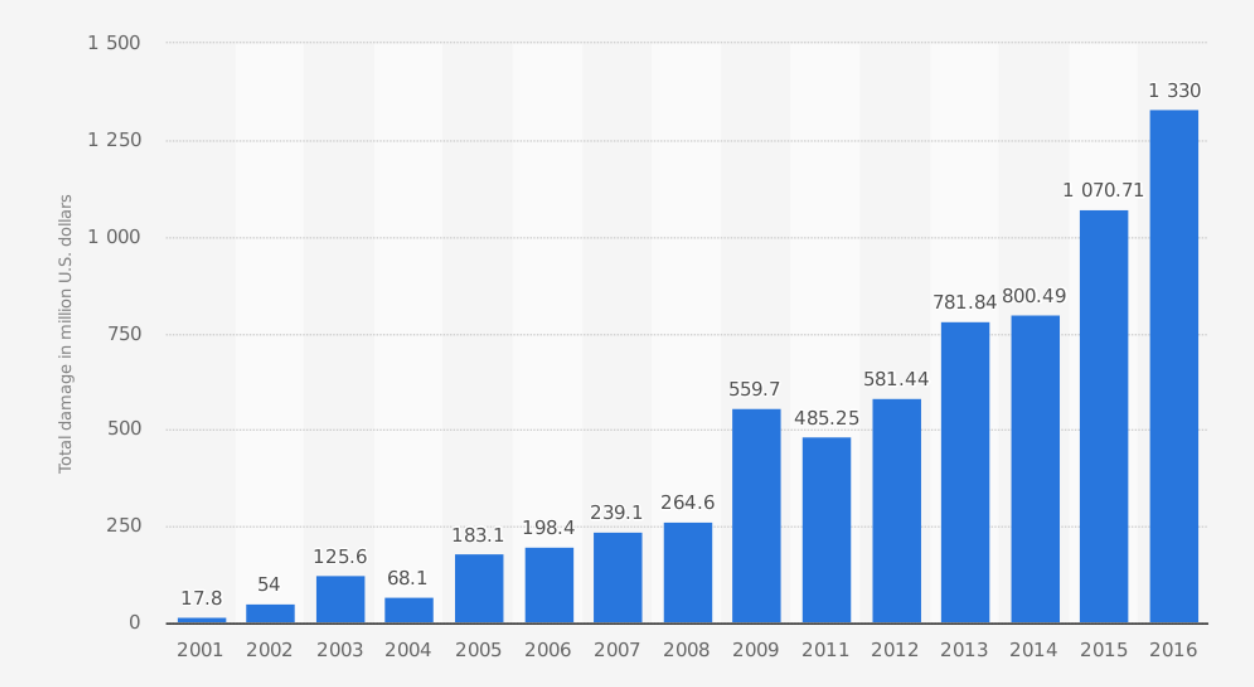

Figure 4: *Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2016 (in million U.S. dollars) (Statista, 2018)*

As a result, considerable financial outlays are spent on security to ensure that these hacking attempts never succeed. Unfortunately, it seems that corporations are not impervious. In the interview (Trocmé, 2018), Mathias Leijon said:

> *I think that we are not as prepared as we should be. I had a very eye-opening experience during a seminar with one very bright hacker working for Nordea. He asked the audience if anyone dared him to try penetrating their system. One brave company volunteered, and he hacked their system live on stage; it literally took him a few minutes! That seminar made it clear to me that an IT system is never stronger than its weakest link.*
>
> – Mathias Leijon, *Nordea*

It is therefore crucial that blockchain is capable of managing today's cyber-security requirements entailed by corporations, and perhaps, even improve them. In a blockchain, security depends on the underlying consensus algorithm. In a decentralized network, such as Bitcoin, transactions were believed to be nearly impossible to hack, though several flaws of the sophisticated system of Nakamoto (2008) have been uncovered. Earlier, we alluded to the 51% attack, which makes it possible for a group of miners to maliciously alter records of the blockchain, for instance by reversing or double-spending transactions if they were to control more than 50% of the hashing power. In fact, this has already happened, for instance in Bitcoin, Litecoin, and Dogecoin, where the majority of hashing power was temporary controlled by a single miner or pool of miners. (Courtois, 2014).

Nonetheless, Nakamotos idea is as such: if a colluding group attempts to modify a block of transactions, it would have to redo the proof-of-work, not only for that particular block but for all subsequent blocks, to replicate the validated blockchain, which (by the general rule) is the longest chain, thereby surpassing the work of the honest nodes. In this regard, Nakamoto showed that the probability of success by the colluding group diminishes exponentially if the majority of nodes are honest. However, this does not completely justify the security of these consensus mechanisms, that is, believing in the longest chain because it is the most profitable to mine. Hashing power is accessible for everyone through cloud hashing providers (Tasca et al., 2016). Note that you only have to temporary "control", rather than physically own, 51% of the hashing power (Courtois, 2014). This means that one person could rent hashing power for a short amount of time (within the time horizon of one block being validated) from miner pools and take control of the majority of the network, without physically owning any hashing power. This process of displacing hash power is very common in the crypto-community and

apparently occurs frequently according to (Courtois, 2014). This is a significantly concerning matter, as the network could become exposed to moral hazard, and thus, the longest chain might not be the correct and honest chain. However, it is important to note that the core Bitcoin protocol has never successfully been hacked (Antonopoulos, 2016), and our informants additionally pointed out the strength of large blockchain networks in the event of a majority attack.

> *I do not worry about a 51% attack... In a smaller network, yes, but in a larger network such as Bitcoin, and even Ethereum, I do not worry about that. It's very expensive.*
>
> – Collin Thompson, *Intrepid Ventures*

> *Even with 51%, it is significantly challenging. With 60, 70 or 80%, it would be much easier. However, you could still not go back 15 blocks. You might be able to go 3 blocks back in time. That is the maximum of what I see as possible, at least for [blockchains] such as Bitcoin, because of its size, and Ethereum as well for that matter.*
>
> – Bjørn Bjercke, *EY*

Despite the technical feasibility of rewriting the history of a blockchain, it seems that there is a substantial limitation to how many blocks it is possible to redo by the proof-of-work, due to the immense computational power that is required and it also is not likely sustainable over time, for instance in the case of rented hash power. But this does not change the fact that there is a short-term vulnerability. This is why it is essential to wait some time to ensure the credibility of the validated blocks.

Thus far, we have addressed the proof-of-work algorithm, as found in Bitcoin and Ethereum. The second most popular consensus algorithm is the proof-of-stake, which may be found in cryptocurrencies such as Dash and Neo. Ethereum is also close to officially launching its Casper protocol, following the proof-of-stake concept, as it is more efficient in terms of

computational power.[10]. The security of proof-of-stake consensus is however more uncertain. To become a forger, one must make a security deposit called a "stake." The principle of this consensus mechanism is that the stake will always be higher than the amount being validated, which will be lost if a falsified block is evident, thus eliminating any incentives for moral hazard. However, the risk of a 51%-attack cannot be ignored. Since the chances of validating are proportionate to the market capitalization (approximately $50.5 billion[11]) of the currency being forged, one could obtain 51% of the votes and outvote the rest of the validators. Although the chances of acquiring 51% are small due to the enormous amount needed, the consequences are severe.

> *If you have 51% in proof-of-stake, you can take full control of the network. It costs you nothing to rewrite the history... The whole point of proof-of-work was that it would be very expensive to do a 51% attack or a reorganization. It will cost a lot of energy, so you do not have an incentive to do so.*
>
> – Johan Torås Halseth, *Lightning Labs*

Additionally, the possibility of constructing pools and agreeing upon malicious validation is still present, and may also reduce the costs of opportunistic behavior.

> *[Regarding proof-of-stake] then we're back to trusting a third-party; thus there's a question of trust once again. Technically, it is possible, but from a human perspective, I believe it will be challenging when we're talking about billions of dollars, [to trust] actors to not collude in order to gain benefits.*
>
> – Bjørn Bjercke, *EY*

We cannot, however, generalize the variety of consensus algorithms, as they differ across blockchains.[12] These mechanisms must be developed to fit their use case. For example, R3

[10]For a comprehensive guide of the proof-of-stake algorithm and Ethereum's Casper protocol, see for instance: https://blog.bitmex.com/complete-guide-to-proof-of-stake-ethereums-latest-proposal-vitalik-buterin-interview

[11]Market capitalization as of June 10, 2018

[12]For a list of different consensus algorithms, see for instance: https://steemit.com/cryptocurrency/@killjoy/the-different-proofs-of-crypto-currency

Corda's use-case is designed particularly for the financial services industry (Brown, 2016). Furthermore, the ability to develop applications on top of existing protocols may eliminate specific risks associated with that blockchain protocol.

> *I think we're going to reach a point where we'll see many private blockchains being used in the industry. So if I'm a corporation and I want just to use Ethereum, I can develop my own blockchain to use internally, which means many of the risks associated with external threats will be reduced.*
>
> – Stylianos Kampakis, *UCL Centre for Blockchain Technologies*

Another factor pointed out by Stylianos Kampakis is that, in the blockchain space, the weak link is often the human link, that is, the link to the real world, as discussed in Section 4.2, which may be prone to mistakes or malicious conduct. In this regard, we argued that intermediation likely remains the most secure link in this manner.

In the case of Bitcoin, its proof-of-work algorithm is arguably superior to most proof-of-work solutions in terms of security, as indicated also by one of our informants, Lukas Wohlgemuth. However, it is important to note that running the Bitcoin network is substantially costly and thus the possibility of downsizing the network in the future cannot be disregarded.
Thus far, we have addressed the security characteristics of the blockchain protocols themselves. Our informant additionally highlighted an important aspect regarding the security of blockchains:

> *I think blockchains themselves are super secure. I think Bitcoin is probably the most secure blockchain that we have at the moment. The risk we have there is just all those wallets and all those providers, providing, storing the private keys. This is the weakness, I think. Mostly those wallets or exchanges get hacked. So, there people have to be careful and maybe store their private key at a secret place. Those are the two things that have to be distinguished carefully: the blockchain itself and how you actually store and access the private key.*
>
> – Lukas Wohlgemuth, *Strategy &, part of the PwC network*

It seems that the major risk of blockchain lies within the management of private keys. As such, we are back to trusting an intermediary to provide an exchange platform or a digital wallet, thereby controlling the users private keys. If these are compromised, thereby providing attackers full access to the entire history of records as well as the ability to alter transactions (Hileman & Rauchs, 2017a). This is a highly significant risk and could lead to severe consequences. There needs to exist a proper system for managing private keys. The simple solution is to store the private key offline, for instance on physical paper or in a hardware wallet, such as the Ledger Nano S.[13] This may work well for private investors, though it may not be in their interest due to the risk of losing their key. As suggested by Peter Frøystad, developing a multi-signature mechanism into the blockchain application could considerably diversify the risk of cyberattacks. In a consortium, this risk may be further diversified by diffusing validation across several institutions.

Biometric-linked private keys have also been suggested as a possible solution to mitigate or circumvent this risk (Perlman, 2017). Biometric authentication generates a link between the private key and specific individual characteristics, hence the user will have to authenticate transactions physically.

Finally, a proper recovery system is essential in case of losing one's private key. Current solutions commonly involve "seed phrases" which consist of several random words that must be correctly arranged to recover the private key. Other solutions are based on Shamir's Secret Sharing, for instance introduced by Zheng, Zhao, Fan, and Wang (2017). This particular cryptographic scheme splits a secret into several pieces and may thus be recovered by combining a predetermined number of these pieces (Shamir, 1979). As such, a multi-party recovery system may be integrated among trusting participants which will make the blockchain secure and robust if a private key is lost or obtained by attackers.

From our discussion, we find that blockchain technology is capable of delivering a robust and secure infrastructure. The Bitcoin protocol, consisting of a market capitalization of approximately $130 billion[14], has not yet successfully been hacked. Moreover, it seems that decentralized blockchain architectures, built by the proof-of-work consensus algorithm, are

[13] Ledger Nano S is a hardware wallet for storing cryptocurrencies. More details may be found on: https://www.ledgerwallet.com/products/ledger-nano-s

[14] Market capitalization as of June 7, 2018

more secure than closed and permissioned architectures, due to the large size of the network. The issue of such architectures, however, is the risk of downsizing the network if, for instance, Bitcoin miners would substitute Bitcoin for more profitable protocols.
In a permissioned network, the number of nodes is substantially reduced, forming a centralized authority. The underlying security of closed and permissioned blockchain networks will therefore depend on the signature mechanisms, involving management of private keys and multi-signature mechanisms. Furthermore, the distributed nature of blockchain will keep the system robust, thereby eliminating the risk of a central server failure (Mainelli & Milne, 2016).

5.1.3 Privacy and GDPR Compliance

Certain concerns may be raised within the blockchain space regarding privacy compliance. One regulation that recently came into effect and has raised many questions, is the EU's General Data Protection Regulation (GDPR). Non-compliance with these policies may cost corporations 4% of global annual turnover (Dobrauz, Hofmann, Khiar, & Sahin, 2018). We will address these concerns in the light of four key challenges identified as most relevant by Dobrauz et al. (2018): replication (distribution of personal data), encryption (who has access to the data), immutability (right to be forgotten) and data controllers- and processors (who controls the data).

In public blockchains, by means of their decentralized nature, transaction data are shared with the entire network. This does not comply well with data protection laws if a corporation were to operate on distributed ledger technology, nor will it be in the corporation's interest to share all of its information with the entire network. Simply encrypting the data does not mean that it is compliant with regulation, and even so, encryptions may be broken in the future. This is a significant challenge facing blockchain concepts.
One solution may be to limit the transparency on the chain by zero-knowledge proof, that is, only storing partial data or solely hashes (Hileman & Rauchs, 2017a). In a partial data storage scheme, a reference to the underlying transaction identity may be stored on the chain using hashes referenced to the real data which are located off-chain. For example, Enigma, which is a second layer application, stores all private data off-chain by using a multi-party

sharing mechanism (Zyskind, Nathan, & Pentland, 2015).

Zero-knowledge proof is also used in permissioned networks. In the RippleNet, validators only see the cryptographic cases that the system uses to mathematically verify that each institution has fulfilled the conditions required to execute the payment and does not require information of the payment data itself (Ripple, 2016b). That is, no third party or other participants can see sensitive data or details of the transaction or agreement, and additionally, the data stays within the closed network, as opposed to public blockchains, in which data are distributed among the entire public community.

R3 Corda's solution is called CorDapps, which has similar properties and additionally provides a self-sovereign solution, giving individuals full control over their own data.[15] However, unless explicitly stated by law, there is no guarantee that such pseudo-anonymous solutions, by simply encrypting data, will be in accord with regulators. According to the directive, full anonymization requires removal of the relation to an individual. Consent would be required if data are simply hashed, aggregated, or otherwise pseudonymized (Article 29 Data Protection Working Party, WP 240).

That said, distributed ledgers encounter another obstacle, namely the right to be forgotten, referenced by Article 17 (2), implying erasure obligations, and storage limitations no longer than is necessary for the purposes for which the personal data are processed, as expressed in Article 5 (1). First, the immutability attribute of blockchain violates GDPR requirements. One potential solution could be to delete or throw away the encryption key, in which case the data, in theory, never can be reaccessed. However, the information still exists and consequently this does not guarantee satisfaction for the GDPR policy mentioned above.

> *In parallel we had the rise of, in particular, the blockchain, where the concept of the blockchain is that you do not erase any information but that it is internalized, if you like, that it can't be manipulated and so forth, so that sort of stands head to head with blockchain concepts and GDPR requirements. This is a huge challenge.*
>
> – Günther Dobrauz, *PwC Legal*

The last challenge facing blockchain privacy properties is to determine the role of the nodes

[15] See for instance: https://docs.corda.net/cordapp-overview.html

in the network. Who is controlling the data and who is processing it? According to the European Commission, the role of the data controller (alone or jointly with others) is to determine the purpose and means of personal data processing, whereas the processor is the one actually processing the data on behalf of the controller, as stated in Article 4 (7-8). These roles may vary broadly depending on the blockchain design. The most challenging design in this regard is a open permissionless blockchain. As everyone controls the network, meaning that everyone is its own data- controller and processor, such a design will entail certain implications. In a permissioned blockchain or consortium run by one or more organizations, validators are preselected and authorized to act as controllers of the data (e.g., Ripple), whereas i a consortium, such as R3 Corda, specific nodes of entities operate in a joint controllership, in accordance with Article 4 (7) of the GDPR directive.

One of our informants pointed out that many proposed solutions within centralized ecosystems will most likely clash with legal provisions. However, it may become easier for customers themselves to manage their identities on a distributed ledger, which in turn will make it easier for corporations to lay claim to verification procedures. Most of our informants believed that blockchain will be particularly suitable for GDPR in this manner.

> *I think that GDPR is actually in alignment with most of the blockchain and cryptocurrency culture because it provides more power to individuals, and less power to the holder. So, I think it's a very welcoming thing to a lot of people in the cryptocurrency- and blockchain space.*
>
> – Collin Thompson, *Intrepid Ventures*

> *Another [opportunity] is digital identity... issuing and enabling individuals, perhaps even organizations, to have better ways of having a digital identity. So, when you need to share a particular information by using blockchain you dont need to share all, because you have methods that you can use to only disclose to particular counterparties. You can show the other person, the counterparty, only what you want to disclose.*
>
> – Mariana Bontempo, *Applied Blockchain*

One such solution is IPFS,[16] which stores data entries and pointers to the particular data on a shared database.

> *You keep ownership of the data, but IPFS keeps the pointers to all the changes that have happened to the data ... You can have ownership of your data without having a centralized system controlled by someone else who could also be hacked. So I think basically blockchain can be very useful for automatic appliance for GDPR regulations. I think in the next few years we will see more and more of that.*
>
> – Stylianos Kampakis, *UCL Centre for Blockchain Technologies*

Thus, instead of a centralized authority controlling the data, individuals themselves may have ownership of their data stored on their own device, tracking any changes automatically, and due to the off-chain property of this system, it may comply with privacy policies.

GDPR has raised many concerns about distributed ledger technologies. Although it is subject only to the European Economic Area, the regulation highlights important aspects regarding the processing of personal data. After the Facebook scandal in particular, we believe it is fair to say that similar regulations are likely to be implemented, and consequently, many blockchain platforms will be affected.

> *As a regulation, I think the provisions on where we're heading are in the right direction, to give people control over their data and know what is out there about them. I think these regulations are necessary, and the European Union, in particular, has done a fantastic job in ensuring that they can provide this level of control to people because that's what it is at the end of the day.*
>
> – Leeor Groen, *Blockchain Valley Ventures*

From our discussion we can conclude that permissionless networks, in particular, are in conflict with privacy policies, in contrast to permissioned solutions. However, any design is likely to violate GDPR regulations, as pointed out by Dr. Günther Dobrauz.

[16] IPFS is a distributed file system that seeks to connect all computing devices with the same system of files. Source: https://medium.com/@ConsenSys/an-introduction-to-ipfs-9bba4860abd0

> *"Bottom line, I would say the entire GDPR does not work for any kind of blockchain applications.... There are conceptual ways of how you could sort of technically achieve the conceptual requirements, but obviously, we don't have any confirmation if this will be satisfying as required. So yes, I do believe [permissioned solution] is a way to achieve the same ends, as are to be achieved according to the regulation, but whether it is acceptable or not, whether that is the way to do that, we will only know once regulators have spoken about it."*
>
> – Dr. Günther Dobrauz, *PwC Legal*

Regulations are not developed in harmonization with the inherent attributes of blockchain technology. Permissioned networks are essentially attempting to resolve these issues by transmuting the core attributes of blockchains. Günther Dobrauz pointed out that regulation is often based on issues of the past, which consequently cannot confront an entirely new reality engendered by rapid innovation. As such, characteristics of blockchain and distributed ledger technology should be incorporated into these policies.

> *" My hope is that there will be a revision at some point to actually factor that in and sort of revisit that in a smart way and come up with a conclusion ... The dominant design or solution is not quite here yet. I am also trying not to jump to conclusions, but rather trying to familiarize regulators with the concept, how it actually technically works, then offer solutions that can be a workaround, but first of all, you need to get the concepts right, which is the biggest challenge."*
>
> – Dr. Günther Dobrauz, *PwC Legal*

John Mathews, chief finance officer for Bitnation, also stated this perspective in an article written by Meyer (2018), suggesting that GDPR is outdated from a blockchain point of view. Directing the focus on decentralized systems, he stated: *"The GDPR was written on the assumption that you have centralized services controlling access rights to the user's data, which is the opposite of what a permissionless blockchain does"*. It seems to be a common agreement, not only among our informants but also across the financial industry, that GDPR and other regulations need to incorporate concepts of blockchain and distributed ledger. At

this moment, we can conclude that most blockchains are likely in conflict with GDPR, in particular, and likely also in conflict with other regulatory rules. There are conceptual applications being developed to solve the issues addressed above, and if arranged correctly in cooperation with regulators, blockchain technology may be significantly compatible with privacy policies.

5.2 Transaction Processing and Settlement

5.2.1 Cross-Border Transactions

Payments are one of the fastest growing areas of the financial sector worldwide, with payment revenues representing 20%-25% of global banking revenue and a total value of global payment transactions amounting to $420 trillion in 2016 (Badi et al., 2017). Customers are exposed to an average cost of 7.68% of transferred funds (Bruno, McWaters, Galaski, & Chatterjee, 2016). The current international payment structure involves many intermediary stages involving processes such as bilateral know-your-customer (KYC) and anti-money-laundering (AML) depending on the pre-existing relationship, transferring and clearing funds across borders, currency conversion, reporting and documentation, and other regulatory compliance (Bruno et al., 2016). Delays and errors are may occur due to the comprehensive procedures of bilateral transfers. There are also certain risks involved, such as counter-party risks due to liquidity requirements and foreign exchange risks, in particular within regions exposed to volatile currency situations and political instability (Seel, 2016). One of our informants also pointed out the complexity in the current payment systems.

> *Me exchanging money, paying a friend for lunch, or transferring my rent, this is the cornerstone, the easiest thing for banks to do and even that requires huge amounts of processing power, vast amounts of institutions, you need my bank, your bank, the SWIFT system. The infrastructure behind is vastly complex, and for such a small thing as payments.*
>
> – Leeor Groen, *Blockchain Valley Ventures*

Blockchain technology may deliver significant cost-cutting benefits and streamlining of pro-

cesses. Ripple, among others, aims to disrupt the costly and time-consuming payment system. The Ripple Global Settlement Network claims to cut costs by as much as 60% (Ripple, 2016a). Among other factors, Ripple aims to deliver low-value cross-border payments, for which the Real Time Gross Settlement system is inappropriate, thereby facilitating an infrastructure more accessible and with greater reach which eliminates much of the costs involved with managing multiple accounts across geographic borders (Griffin & Zagone, 2015).
However, the Ripple network is not solving all the factors mentioned above. As we discussed earlier, blockchain technology needs some standards across markets to fully manifest its potential. We currently find ourselves in a transition phase where agents operate across entirely different systems. Until there is a broad acceptance for the Ripple network, R3 Corda, or any similar blockchain infrastructure, institutions will find themselves between two different systems, where some will stick to traditional methods, such as SWIFT (Seel, 2016). As such, the need for bilateral relations will remain present, and be prone to cumbersome and often inefficient processes. Nevertheless, within the blockchain ecosystem, significant benefits may be seized, given a certain level of standardization and interoperability. Digital identities on the chain will establish the grounds for efficient and instant KYC-processes through smart contracts (Bruno et al., 2016). Our informants also emphasized this advantage.

> *One of the biggest confinements that we have, meaning the banking industry in general, is following customer regulations. A lot of resources are used in all banks to ask these questions, overseeing transactions, receive an ID, establish bank ID, etc. There has been an attempt between the major banks in the Nordic region to use blockchain technology to do this once and for all. So, if you've been identified by DNB, and they've followed KYC regulations, which the authorities in Europe and Norway require, I will then be able to access this technology to extract a certificate from this customer. That will significantly streamline this process and could be a huge win for all banks.*
>
> – Marte Kopperstad, *Nordea*

> *So we have been internally working on a KYC-related blockchain solution and we think that it is a really good use-case for blockchain technology. If done right, it's*

> *going to save a lot of trouble for financial institutions because if you could ensure interoperability of KYC-processes, while protecting privacy and the data itself, then that will be huge for the financial services industry.*
>
> – Miguel Cuneta, *SCI Ventures Inc.*

As such, an interoperable infrastructure will eliminate much of the manual intervention across all intermediary stages, by automatically verifying identity authentication from the blockchain, thereby significantly reducing the corresponding costs, in particular for low-value cross-border payments such as remittances, which we will discuss in more detail in Section 5.5.1. Reducing settlement time will also mitigate foreign exchange risks, however not completely remove them. As long as there is a short latency window, even a few seconds, this may result in foreign exchange losses, depending on the stability of the given currency.

5.2.2 Post-Trade Clearing and Settlement

One of the most widely discussed applications of blockchain technology is its impact on trade clearing and settlement, in terms of cost efficiency, counterparty risk, and time to settlement. While the execution of securities trades has been streamlined for many years, it is the underlying post-trade clearing and settlement infrastructure that remains complex and costly (Schneider et al., 2016). Notably, the process of clearing and settlement itself is quite efficient; however, this process entails inconvenient manual reconciliation and affirmation of trades among several participants such as controllers, internal- and external auditors and regulators (Steenis, Graseck, Simpson, & Faucette, 2016). According to Peterhoff, Miller, Romeo, Patel, and Holroyd (2014), revenue from settlement, custody, and collateral management amounted to $40-$45 billion in 2013, and Gokey (2015) estimates that the industry spends $17-$24 billion per year in trade settlement and processing, of which $6-$9 billion represents highly standardized asset classes such as fixed-income securities. The lack of interoperability in legacy systems[17] and inefficient back-office processes result in a complex and hence costly trade process. Schneider et al. (2016) estimate $2 billion in cost savings in the

[17]Legacy system is a term often used for an old and relatively outdated method, technology, computer system, or application.

U.S. and $6 billion globally.

> *"We believe blockchain could drive greater efficiencies in the U.S. cash equities market, primarily through streamlining the post-trade settlement and clearing processes. By reducing the duplicative, often manual affirmation and reconciliation of trades across buy-side clients, broker-dealers, trust/custody banks, and the Depository Trust & Clearing Corporation, we believe blockchain could result in an estimated $2 billion in annual cost savings in the U.S. On a global basis, the benefits would likely exceed $6 billion in annual savings."*
>
> – Schneider et al. (2016), *Goldman Sachs*

The costs of post-trade processes are partly due to a complex chain of participating intermediaries involved with one single transaction (Benos, Garratt, & Gurrola-Perez, 2017). For example, Steenis et al. (2016) stated: "*For many banks, especially investment banks in 2016, a radical reduction and simplification in processing costs would be a blessing.*" Blockchain technology has uncovered many potential solutions to payment settlement systems and might be that blessing. Batlin et al. (2016) suggested that distributed ledger technology could significantly reduce the transaction costs for banks and other financial institutions involved with trade processing, such as trade management, clearing, and reconciliation, as well as counterparty risk. To give an example, the Australian Securities Exchange is currently moving closer to adopting distributed ledger technology, thereby becoming the first major stock exchange in the world to use a blockchain-based solutions for post-trade processes (Australian Securities Exchange Ltd., 2018).

Mainelli and Milne (2016) described three functions of clearing and settlement: i) ensure mutual and accurate agreement between trading parties to finalize settlement, ii) ensure legal compliance of the trade, and iii) handle exceptions due to breaches in trust and legal compliance. In the previous section, we discussed the magnitude of smart contracts, of which we identified certain characteristics that may constitute challenges to fulfilling the two latter points above. Nonetheless, for less complex trades, such as retail payments and trade finance where legal frictions and breaches are minimized, clearing may be more automated and standardized by the use of smart contracts, hence improving efficiency in clearing and settlement

processes, but will likely not be facilitated by full automation, in particular when it comes to more complex transactions, such as securities trades. According to Antonopoulos (2016), centralized clearing agencies are highly efficient and can operate billions of transactions per second, which is implausible for current blockchain protocols to replicate due to scalability issues, as addressed previously.

Arguably, the most important aspect of clearing is the management of counterparty credit risk, as emphasized by Benos et al. (2017). For instance, the financial crisis in 2008 resulted in a highly fragmented financial market and spurred many concerns about risk and inefficiencies in post-trade processing. As a result, regulation and supervision was strengthened, especially liquidity requirements (Basel III) (Bank for International Settlements, 2017), and henceforth markets became increasingly concerned with managing counterparty exposure, among other risk factors (Boston Consulting Group, 2012). In order to reduce this risk, clearing agents provide netting benefits, which offsets a net position of the trading party, thus narrowing the spread of liquidity requirements. This is a core element of the market structure, as the majority of trading comes from market makers, involved with high-frequency trading (Schneider et al., 2016). For instance, the Depository Trust & Clearing Corporation reduces the volume of trades for finalization by approximately 97% through netting procedures (Mainelli & Milne, 2016). The advantage of clearing houses and netting processes was also emphasized by one of our informants, from the Norwegian Central Securities Depository (CDS).

> *Provision of security through certainty requires a lot of liquidity from the market. Using a central counterparty clearing house (CCP) will reduce liquidity requirements due to netting procedures for each CCP participant (one net settlement position per ISIN* [18] *per participant). A settlement batch, such as that of CDS, all transactions are netted and optimized for maximum settled value (multilateral netting), to provide as much liquidity as possible to the market, which cannot be achieved by real-time gross settlement.*
>
> – Ketil Qvam Andersen, *Oslo Stock Exchange CSD*

[18] The International Securities Identification Number

As indicated by Ketil Qvam Andersen, real-time settlement likely results in less liquidity. However, shortening the post-trade settlement cycle from three days to as little as one day may free up the amount of tied capital, hence reduce the amount of risk and liquidity requirements (Boston Consulting Group (2012); Schneider et al. (2016)). That is, because collateralized clearing funds depend on time and volatility, among other factors, a shorter settlement window would decrease the collateral requirements (Boston Consulting Group, 2012). However, these studies found little support for near-instantaneous settlement, revealing that most agents consider a T+0 system to be infeasible, a perspective also shared by Steenis et al. (2016), who suggested that markets today with instantaneous settlement processes have less liquidity and more volatility than markets with longer settlement cycles. One reason, as indicated by Mainelli and Milne (2016), is that trading parties rarely have securities or cash positioned prior to trade execution, in which case, instant settlement would engender implications. Benos et al. (2017) also pointed out that instant settlement could lead to implications for liquidity management due to the requirement of prepositioning cash or securities.

> *Delayed settlement is a design choice involving deep economic market structures, not least of which is leverage and liquidity. A shift to near real-time settlement, say a few minutes after trade will bring costs as well as benefits. Yes, it will economize on the commitment of cash and collateral, but it will require a major change in business processes, with the holding of securities and cash having to be positioned prior to trade and greater exposure to liquidity risks.*
>
> – Mainelli and Milne (2016), *SWIFT Institute*

> *[Netting and settlement] This can be done in a T+0 settlement, though the standard today is T+2. In a system with "instant settlement" in which money needs to be put on the table prior to trading, will likely lead to less liquidity on the marketplace due to the increase of tied capital of the trading parties.*
>
> – Ketil Qvam Andersen, *Oslo Stock Exchange CSD*

Existing technology and clearing processes already have the ability to facilitate T+0 settle-

ment without blockchain technology. There are certain implications involved, for instance with capital markets transactions, which prevent shorter settlement windows. Notably, this only involves trading in the market, as pointed out by Ketil Qvam Andersen. For instance, OTC securities are traded through a dealer network, and settlement time is therefore agreed upon between the parties, which can range from T+0 to any point in time that is desired. Nonetheless, for market trading, liquidity plays a key role in post-trade settlement, and regulatory factors are also significant due to the large and often complex transactions involved (Steenis et al., 2016). By using smart contracts constructed for netting purposes, margins of risks may be dynamically calculated, thus automatically facilitating variations in demand of collateral (de Velde et al., 2016). As such, liquidity requirements may be minimized, and finalization of settlement may be automatically triggered at the closing of the trade, simultaneously securing delivery versus payment.[19]

Another aspect to be taken into consideration is the validation and certainty of blockchain transactions. In Bitcoin, blocks are validated every 10 minutes on average, and to ensure that these transactions were valid, and that nobody has tampered with them, the general rule is to wait approximately an hour to ensure credibility of the transactions. This credibility is a question of security, and will, therefore, depend on the blockchain protocol and the network, as we discussed in Section 5.1.2. A smaller network, such as a permissioned network, will likely require more time to be considered credible. As such, certain latency may be desirable to prevent risks of fraudulent transactions.

Certainty of post-trade affirmation and finalization may be significantly more important than shortening the securities settlement window in terms of costs (Mainelli & Milne, 2016). Significant costs arise in the event of failing to preposition collateral. Thus, rather than narrowing settlement, blockchain may increase certainty and confirmation of the finalization time. Today, institutions keep their own records of transactions, which means that each party has to reconcile the party's own ledgers which, due to differences in infrastructures, lead to considerable costs (Steenis et al., 2016). With an interoperable blockchain enabled

[19]Delivery versus payment is a settlement system that ensures that payment must be made prior to or simultaneously with the delivery of the security. This system acts as a link between the trading parties, minimizing settlement risk, that is, instances where the seller receives a cash payment but does not deliver, for example due to liquidity issues.

infrastructure, one ledger would be visible to all parties involved, who can confirm agreements through multi-signature mechanisms, and accordingly, enforce agreements at the time of entry, thereby eliminating much of the manual interventions and costs involved with settlement procedures (Schneider et al., 2016).

> *In a blockchain infrastructure, one can imagine a solution where both trading and settlement are made in one system.... This can in principle be done by conventional technology, but in my opinion, DLT is more suitable if you want to implement such a solution.*
>
> – Ketil Qvam Andersen, *Oslo Stock Exchange CSD*

However, one concern remains: privacy. The transparent nature of blockchain technology is likely to be an issue for many institutions, especially for banks, as pointed out by de Velde et al. (2016). Anonymity is required among capital market participants; therefore, considerable measures have to be incorporated in this manner, limiting transparency to the parties involved, for instance through separate record keeping outside of the blockchain (Schneider et al., 2016), or encrypting transaction details, and accordingly, adequate management of private keys, as discussed in section 5.1.3.

To summarize, clearing and settlement procedures may be more automated by smart contracts but are however limited to short-term and less complex transactions, for which legal compliance and contractual breaches are limited, thus fulfilling all of the functions of settlement mentioned previously. Such transactions, for instance, include retail- and wholesale payments and trade finance. Long-term and complex transactions, such as capital markets transactions, may be streamlined but will, however, face particular challenges regarding legal compliance and exception management in the event of a dispute. Further, efficiency in reconciliation among institutions is also a viable benefit due to transparency properties involved with distributed ledger technology, conditional on the preservation of privacy.

We have also addressed the potential for near-instantaneous settlement, for which we found little support due to liquidity- and security implications. Settlement could be reduced to T+1, or settlement at the end of the day. Notably, while T+1 can be achieved without

blockchain technology, we may argue that the efficiency and integrity of blockchain may be more suitable. For this reason, to draw a general conclusion, the most significant benefits of blockchain technology in post-trade settlement are involved with eliminating the manual intervention of reconciliation and affirmation/confirmation, shortening the settlement window potentially to one day,[20] and thereby reducing counterparty risk and liquidity requirements for prepositioning collateral.

5.3 Financial Accounting and Auditing

The potential of blockhain technology to improve the quality of auditing and streamlining financial accounting has frequently been suggested by our informants. A system in which all transactions are written onto an immutable blockchain is further suggested by some scholars to potentially eliminate the need for manual audits of financial statements (Yermack, 2017).

5.3.1 Double-Entry Accounting

Modern financial accounting is based on a double-entry system. Double-entry bookkeeping allows companies to keep records reflecting what is owned and owed, as well as how much is earned and spent over a given period. Until the innovation of double-entry bookkeeping during the Renaissance, simple ledgers had been the standard for record keeping (Tyra, 2014). As companies were increasing in size, the records became big and complicated, effectively reducing the assurance of accuracy to their users. The double-entry system prevents fraud through its implementation of checks and balances. Managers can thus trust the validity of their books. These records became expected to be shared with outside stakeholders, and thus arose the issue of how these stakeholders also could trust the companies' records. Hence, the public auditor came along, whose role has been to verify the company's financial information. The stakeholders rely on the integrity of the auditor, who in turn is retained by the management. This has created an agency problem, for it is not entirely clear for whom the auditor is working (Ronen, 2010).

[20] See, Boston Consulting Group (2012), for a more comprehensive analysis on the shortening of the settlement window.

5.3.2 The Blockchain and Triple-Entry Accounting

The scholarly concept of triple-entry accounting was developed by the late Yuji Ijiri (Ijiri, 1986). The concept is an extension to double-entry accounting and is meant to serve as an improvement to the former system by integrating future transactions into the financial statements, thus improving the ability to make predictions. It is a common misconception that also adding each transaction to a blockchain is a third entry (Tyra, 2014). It is not, at least not in the sense implied by Yuji Ijiri. It is rather double-entry accounting executed in an additional step. Nevertheless, adding a company's transactions to a blockchain may be advantageous. A third entry to the blockchain can cryptographically seal accounting entries involving external parties. Instead of the two parties keeping only separate books, the information may also be included in a joint register. In this case, the joint register is a distributed blockchain ledger. Since the entries would be cryptographically sealed and distributed, falsifying or destroying them would be practically impossible.

The use of a public blockchain ledger to store a company's transactions has also been suggested by Lazanis (2015). The use of such a blockchain design would make the company's ledger visible to any interested party. As argued by Yermack (2017), this would increase shareholder's trust in the integrity of the company's data, but it comes at the cost of making proprietary information available to outsiders. A private blockchain, on the other hand, would allow only participants permitted by some administrator access to see transactions.

In the case of keeping immutable records of electronic files, the application of blockchain technology becomes particularly beneficial. Due to their nonphysical nature, electronic files are especially vulnerable to manipulation. Thus, a wide range of preventative measures is necessary to sufficiently guarantee integrity. By time-stamping the fingerprint immediately after the creation of the document, one can be sure of the electronic file not being altered. No particular preventative measures thus need to be implemented in storing the data, since alteration can be accounted for through comparing the fingerprints in the company's records with the ones written onto the blockchain. This should improve the degree to which the existence of a firm's financial statements can be trusted, and at the same time the cost associated with the record keeping could be reduced (Psaila, 2017). However, despite the input on the blockchain being immutable, the issue relating to the reliability of the initial

transaction put on the blockchain still makes itself relevant. This was emphasized by one of our informants:

> *You still have to go through everything. You still have to see, so it's okay for a company to say that we have spent so much traveling, so and so much in salaries etc. and can document this and hash all that and give us the hash key to see it, but the only thing we can do is to say that the hash string is correct and that when we do the same operations we get the same hash string. It makes no difference.*
>
> – Bjørn Bjercke, *EY*

Bible, Raphael, Riviello, Taylor, and Valiente (2017) argued that certain financial statement assertions could constitute sufficient audit evidence when accepted onto a blockchain. The example they gave of such an assertion was that of a Bitcoin transaction for an asset, where the transfer of Bitcoin is recorded on the blockchain. However, the auditor will not necessarily be able to determine the integrity of the asset from evaluating information on the blockchain alone. As suggested by Bible et al. (2017), recorded transactions may still be fraudulent, executed between related parties, or linked to separate side agreements off-chain. The issue related to off-chain side-agreements was also highlighted by one of our informants:

> *Today there may also be secret contracts on the side, but then the auditor has two jobs, the first is to check that the contract one sees is the same as reflected in the accounts. Blockchain solves that. The secret contracts, they are there today nonetheless, so I do not get any less or more work because one adds it to the blockchain. I save the work by seeing that the contract is there, but to reveal fraudulent activities outside of this I have to do additional controls in the future as well.*
>
> – Finn Kinserdal, *Norwegian School of Economics*

Keeping transactions on a distributed blockchain could drive cost efficiency by making the verification process simpler (Psaila, 2017). The transactions could be verified on the blockchain, thus eliminating the need for requesting confirmations from third parties and gathering bank statements from clients.

> *If it is alleged that there are 10 million in customer receivables, we will check that the invoices exist and send a letter to the customer for confirmation. This work can be solved with blockchain. We do not have to send out people anymore, I can simply enter the blockchain and then I can check that things are in place there. So that's an extreme improvement in efficiency on the day we get the blockchain in place within the audit, within the kind of transactions that are somehow proof that there's existence, as it's called in the world of auditing.*
>
> – Finn Kinserdal, *Norwegian School of Economics*

However, the gains in efficiency may still hinge on some process ensuring the integrity of the assets in question, as discussed in Section 4.2. As such, the practice of sample-based substantive testing will not be completely removed. Nonetheless, blockchain facilitates a tamper proof audit trail which may automate verification of transactions for which its existence occurred on the chain. This can also include confirmation and detection of specific incidents which do not originate off-chain such as double spending, changes in bank account and missing tax IDs (Gräslund, 2016). Hence, blockchain can potentially streamline certain auditing processes and reduce manual and paper based efforts.

Further, financial statements reflect managerial assertions. Auditors will still have to apply professional judgment when analyzing estimates made by management.

> *When it's about estimates and budgets, we dont work with samples, we go directly, we work with management, and we make our assessments, so I think that part will remain."*
>
> – Yusuf Barman, *KPMG*

> *Have people tampered with the numbers, are the estimates made correct etc., and the way in which the IFRS accounting rules are made now, there are much more estimates and valuations than it was 20 years back and you cannot put it in a machine. You need to make an assessment of where the management has obtained the information from, whether the valuation is done correctly, what estimates are*

> *made, compare it with other companies, and so on, then put an approval stamp on it. So I have no concern for the audit industry, but the scope and hours I think will be something entirely different.*
>
> – Finn Kinserdal, *Norwegian School of Economics*

The argument of blockchain technology enabling more automation was also made by Bible et al. (2017), who argued that deploying analytics and machine-learning capabilities could enable real-time reporting of unusual transactions, and any relevant party could be automatically alerted. Thus, the transparent nature of distributed ledgers may facilitate automated regulatory reporting, which today is a relatively complex process, as suggested by Hileman and Rauchs (2017a). However, such a solution could prompt regulatory response in error in the case of data errors. Hence, automatic regulatory reporting may require control mechanisms revealing input errors as well as ensuring the integrity of transactions on the blockchain.

Furthermore, writing a company's transactions onto a blockchain could also allow near real-time data access for auditors, thus potentially enabling audit firms to move toward a more continuous audit process. One of our informants, however, was more skeptic:

> *Establishing a continuous monitoring device is a challenging and expensive task. I do not think the auditor is going to deal with that any time soon. Internal auditors are going to do it, because they are looking for the internal routines being in place, and that there is no failure in internal control systems at the companies.... I think the external audit is still going to be a periodic audit, that is, confirming that things are correct at a certain point in time.*
>
> – Finn Kinserdal, *Norwegian School of Economics*

The possibility of internal continuous auditing may have the potential to redefine and improve credit risk modelling by allowing more focus to shift toward corporate governance and possible fraud detection. Bible et al. (2017) argued that automated audit processes may change the role of the auditor toward providing assurance to users of the technology. This was also emphasized by one of our informants:

> *Afterwards, the risk will be more focused on the human side, on the decision side and such processes.... If everything is automated, all the data you can capture, all the data you have, you can get assurance and make risk assessment with the numbers. But in the future, you will still have the human components, where decisions have to be made.*
>
> – Yusuf Barman, *KPMG*

Bible et al. (2017) further suggested that that this could entail auditors taking the role as administrators in permissioned blockchains, as arbitrators among participants in a consortium blockchain, or as auditors of smart-contract source codes. Adoption of blockchain technology may bring drastic changes to record keeping processes but will not replace financial statement auditing in the immediate future. However, the role of the auditor may adjust and focus towards fraud detection and assessment of side agreements, and additionally facilitate near-real time audit processes and corporate governance for internal auditors. Depending on the blockchain architecture, increased transparency and trust in the integrity of data may reduce moral hazard and agency problems in the profession.

5.4 Banking the Unbanked

There are around 1.7 billion unbanked adults globally as of 2017 (Demirgüç−Kunt, Klapper, Singer, Ansar, & Hess, 2017). These are people without access to standard banking services through accounts at financial institutions or mobile money service providers. Solving this issue is high on the agenda for governments, intergovernmental organizations and NGOs alike. In 2014, $31 billion was committed in international funding towards financial inclusion projects (Consultative Group to Assist the Poor, 2016). To "encourage and expand access to banking, insurance and financial services for all" is furthermore one of the targets of UN's agenda to end poverty within 2030 (United Nations, n.d.). In this section we will examine how blockchain technology may have the potential to help the unbanked by offering alternative financial solutions.

5.4.1 Remittances and Payments

Access to banks, the most common financial institution, is limited in many parts of the world. To open a bank account in much of the developing world, one will likely need to visit a branch in person (Tapscott & Tapscott, 2017). In sub-Saharan Africa, as of 2016 there were around five bank branches per 100,000 adults, with countries such as Chad and Niger having fewer than two branches per 100,000 adults (The World Bank, n.d.-a). In comparison, the corresponding number in the U.S. is 32.7 branches. The lack of financial infrastructure has brought about the widespread use of alternative financial solutions. M-Pesa was launched in Kenya, in 2007, by Vodafone's Safaricom, the country's leading network operator (The Economist, 2015). "Pesa" translates to money in Swahili, and the system represents a simple method of texting small payments between users. The service initially started out to allow for repayments of microfinance loans to be made by phone to reduce costs associated with the handling of cash, in turn facilitating lower interest rates. However, the service was quickly adopted as a more general scheme for transferring money. Cash can be deposited into the system at any of M-Pesa's agents, which commonly are local corner shops selling airtime, where the agent uses an agent phone to credit the depositor's account with e-money. For many, the decision to adopt this new way of both transferring and storing money was not a choice between their current banking system and M-Pesa, but between no banking system and M-Pesa.

The Economist (2015) suggested several factors contributing to the success of M-Pesa in Kenya. The high costs of sending money by other methods, as alluded to previously, are among these. Additionally, both Safaricom's dominant market position and the willingness of regulators to allow the scheme to take place on an experimental basis without formal approval are highlighted. Further, the political, economic and humanitarian crisis that followed alleged electoral manipulation in the 2007 presidential election are emphasized. The success of M-Pesa has since spread to several other countries in Africa, as well as to some countries in Asia and Eastern Europe. In 2016, the system processed approximately six billion transactions at a peak rate of 529 per second (Monks, 2017).

In the way that many sub-Saharan African countries have leapfrogged land-line telephony

in favor of mobile technology, the same could to some degree be said about the leap from little or no financial access to granting anyone with a mobile phone a bank account in their pocket. This begs the question of whether a similar path could apply for blockchain technology. For many of the same reasons that mobile payment solutions such as M-Pesa have been adopted in developing countries, it is easy to imagine the potential advantages that distributed blockchain ledgers could provide. In the case of M-Pesa, it remains a centralized solution prone to system failures. In fact, the Kenyan government has expressed concern regarding the potential systemic risk associated with failures in the system, given the number of transactions it handles (Masinde, 2016). The amount transacted through M-Pesa alone in 2015 was approximately equivalent to 44% of the country's GDP. Apart from certain security risks as described previously, such as a majority hash rate attack, total failure of a permissionless blockchain would in principle require a decimation of the internet as we know it today.

The average global cost for sending remittances was 7.13% in the first quarter of 2018, with sub-Saharan Africa being the costliest region to which money could be sent to with a recorded average cost of 9.44% (The World Bank, 2018). The majority of remittances are sent using traditional wire services such as Western Union, Moneygram, and RIA, with Western Union alone having a market share of nearly 20% (Buenaventura, 2016; SaveOnSend, 2018). According to the The World Bank (n.d.-b), cutting remittance prices by at least 5 percentage points could save up to $16 billion a year globally. Blockchain-enabled payment solutions could offer users both faster and cheaper transactions compared to current payment systems. However, as previously highlighted, the scalability issue of Bitcoin led to substantially higher fees. Consequently, some merchants stopped accepting payments in cryptocurrencies altogether, and others shifted to different blockchain networks not experiencing the same soaring fees. Fees in the Bitcoin network have since fallen to similar levels as seen before 2017. However, the spike in transaction fees did illustrate the often cited scalability issues facing the Bitcoin network (Kasireddy, 2017; Simonite, 2017).

Kahn and Roberds (2009) introduced the distinction between *account-based* payment systems and *store-of-value* payments. Account-based systems are founded on the transfer of a claim on some payment object, requiring the keeping of accounts in the name of the sender and

recipient with an intermediary. Credit cars and checks are examples of account-based means of payment. Store-of-value systems, or *token-based* systems, involve the transfer of a payment object, be it either notes or electronically stored value. Both commodity money and fiat money would be examples of such systems, which hinge on the ability to verify the payment object. Given that this is the case, participants can transact without knowledge of, or trust in, the counterpart to the transaction. This is illustrated by the widespread use of cash where trust in counterparties is low (He et al., 2017). Further, such transactions can be done with little financial infrastructure. Cryptocurrencies are another instance of token-based systems, allowing participants to exchange tokens electronically as a means of payment. The adoption of such systems thus shifts payments from account-based systems to token-based systems. By not necessitating the verification of account holders, as in an account-based system, costly processes could be avoided, such as costs associated with infrastructure, intermediaries, and regulation.

The transmission mechanism of a hub-and-spoke payments network, such as a cryptocurrency, is illustrated in Figure 5. Fiat money is changed into tokens through any of the spokes, be it an online interface, physical ATM, or some agent, and deposited and stored in a digital wallet. When the network, here referred to as the hub, confirms the transaction, the tokens become available in the recipient digital wallet. The tokens could then be stored for saving purposes, transacted for services available in the same currency, or changed back to fiat currency via the same spokes. The same scheme would apply for domestic as well as cross-border transactions, and eliminating the need for messaging and settlement in correspondent banks or central bank money (He et al., 2017).

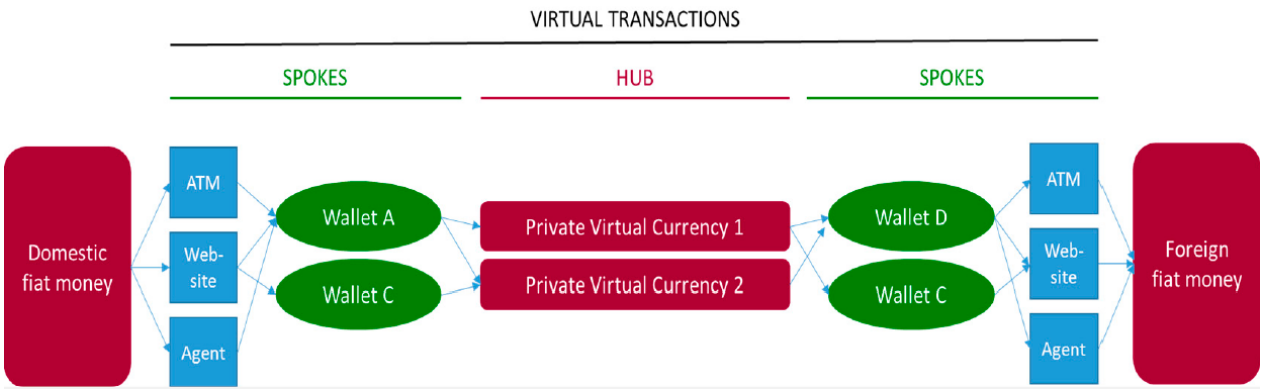

Figure 5: Hub-and-Spoke Networks. From "Fintech and Financial Services: Initial Considerations", by He et al., p.25, 2017. Copyright 2017 by IMF. Reprinted with permission.

A clear challenge to the adoption of cryptocurrencies is the volatility in their exchange rate to fiat money. First, as argued by He et al. (2016) among others, this volatility may limit the ability of cryptocurrencies to serve as a reliable store of value. Further, Yermack (2013) found that, in the case of Bitcoin, the cryptocurrency's exchange rate exhibits little correlation with both other widely used currencies and macroeconomic events, making hedging and forecasting difficult for its owners. The decentralized nature of cryptocurrencies does, however, offer an alternative means of saving when trust in financial institutions and intermediaries is low. Allen, Demirgüç−Kunt, Klapper, and Peria (2016) did indeed find that trust is a barrier to financial inclusion, and that trust is more likely to be reported as such in countries with lower branch penetration. In countries with political uncertainty and rampant inflation, a volatile currency could still be favorable to the national currency. One of our informants also emphasized this argument:

> *If we look at Africa as a continent, it's not a country that has not had economic problems and economic challenges.... And together with South America, along with most of Asia, this crypto market as a whole, although we in Norway experience it as incredibly volatile and dangerous, this is peanuts compared to what many countries have as their central economy and what they have to deal with.*
>
> – Bjørn Bjercke, *Associate Partner at EY*

Zimbabwe would be an example of this, having experienced 58 verified instances of hyperin-

flation in recorded history (S. Hanke, 2017). BitFinance,[21] a Bitcoin exchange in Zimbabwe, has reported that 37% of its customers use the platform as a saving mechanism (Fioramenti, 2018). Second, the relatively high volatility could make it difficult for the average consumer to consider cryptocurrencies as a viable medium of exchange. Particularly for those living near a subsistence level, changes in cost due to volatility in the exchange rate to fiat money could have dire consequences. In the case of cross-border payments, where an exchange rate conversion is needed for both the acquiring and liquidation of the token, foreign exchange rate risk introduces an additional element of uncertainty. Traditional means of hedging for foreign exchange risk could potentially detract from the cost advantage cryptocurrencies have over traditional banking, as well as complicating the transaction for the user.

In the case of cryptocurrencies as a medium of exchange, innovations might provide ways to circumvent the issues related to a relatively high exchange rate volatility. Abra, a global currency wallet in the form a mobile app with an integrated exchange platform, uses smart contracts to reduce volatility associated with currency trades (Biggs, 2018). The investment platform uses multi-signature smart contracts on the Bitcoin and Litecoin blockchains to simulate investment contracts. In a similar way to how a gold exchange traded fund is based on USD, Bitcoin and litecoin are used in place of USD. The smart contracts commit the user's account to making automatic payments to a third party if the price of the underlying cryptocurrency increases and correspondingly to receive payments if the value of the underlying depreciates. This contract of difference allows users to lock in the value of the underlying cryptocurrency. The platform also utilizes multi-signature smart contracts to create what the providers call synthetic digital assets, an example of which is commonly referred to as *stablecoins*. Stablecoins are price-stabilized crypto tokens pegged in some way to another more stable asset. This technology has been extended to also create synthetic digital assets that include other cryptocurrencies, enabling the platform to offer exposure to 70 different cryptocurrencies and fiat currencies without actually holding the physical currency. Consequently, the blockchain and smart contracts enable a peer-to-peer payment rail with no intermediaries and inexpensive hedging of exchange rate risk. In the current fee structure in Abra's model, there is no fee for depositing, hedging, or exchanging between currencies. Fees

[21] Later renamed Golix.

occur at withdrawal and through spreads in the exchange rate.

> *It's much easier now to hedge your holdings, the market is more mature, there is more liquidity, and there are more options. Four years ago we didn't really have a lot of options or a lot of exchanges to work with, so as the space matures, as liquidity increases, as exchange-related frictions decrease, its going to be easier, its going to be faster and I think it's even going to be cheaper to use cryptocurrencies as a payment rail for remittances.*
>
> – Miguel Cuneta, *SCI Ventures Inc.*

In principle, with access to only a smartphone and a mobile data plan, payments could then be made across the globe with no intermediaries. Although, as expressed by one of our informants, there are many challenges:

> *And then it will be that cryptocurrencies will come in because it's free to use, given that you have a smartphone, given that you know what cryptocurrencies are, given that you understand how it works enough to trust it, given that you actually get to spend it somewhere and given that you actually get hold of it, too. How do you earn Bitcoin today? You cannot mine it yourself, you have to buy it somewhere, you buy it at some exchange. To buy it, you need fiat currency, so it's just so complicated to get into that.*
>
> – Peter Frøystad, *Fintech Innovation*

Solutions such as Abra's present an easy and intuitive way of processing transactions on the blockchain; both the sender and recipient may only see the deposit value and transaction value denominated in their choice of fiat currency, and both storage of value and transactions will be independent of fluctuations in the price of cryptocurrencies. However, this depends on the availability of smartphones. According to GSMA Intelligence (2018), the current share of smartphone connections is around 34% in sub-Saharan Africa, constituting the countries lagging the most behind the rest of the world. However, lower smartphone prices and increasing coverage of 3G and 4G networks are contributing to rapid adoption, and current estimations

project smartphone adoption to reach 68% in sub-Saharan Africa in 2025, a doubling of the region's current share (GSMA Intelligence, 2018). Thus, smartphone availability is an issue, but one that will diminish rapidly with time. Other places, such as the Philippines, are expected to reach a smartphone adoption of 71% in 2020 (GSMA Intelligence, 2017). Thus, adoption of blockchain-enabled mobile solutions could potentially be a reality sooner. Further, with as much as 86% of the country's population being unbanked (Chipongian, 2017), the potential benefits could be significant.

Analogous to how trust is critical for fiat money in traditional token-based systems, trust in a blockchain-enabled system would also be essential. Trust must be shifted from financial institutions to the underlying protocol itself, or to other third-party application providers. This should not necessarily require the users to actually understand the technology. Users will need to trust the cryptocurrency exchanges and wallet providers as well, which facilitate both the starting and ending points of the transaction. However, the trend towards open-source code could make this easier, allowing for the community and independent third parties to judge the security of the different providers. Most wallet services grant users the control over the private keys proving ownership of the assets. This puts the user in control, regardless of trust to the wallet provider, but it could easily result in loss of assets without a proper understanding of the technology and necessary security precautions.

5.4.2 Blockchain and Financial Inclusion

Despite the possible implications of adoption, the widespread of blockchain and cryptocurrences is currently present, as pointed out by one of our informants:

> *I think that's already happening. If you look at places like South America, Costa Rica, and Africa. These are some of the places that have the widest adoption of cryptocurrencies. They trust that more than they trust their national currency. So I mean, that's already happening.*
>
> – Collin Thompson, *Intrepid Ventures*

One crucial issue that has been present and an impediment to financial services is the lack

of identity among these populations. KYC obligations embedded in the highly regulated landscape of banking restrict the provision of financial services to the unbanked. With the emergence of blockchain technology, these populations may receive digital identities that are verified and stored on the blockchain, distributed nationally and internationally, as pointed out by Perlman (2017). BanQu[22] and Bitnation[23] are examples of blockchain platforms involved in the provision of digital identities to undeveloped nations and refugees.
The properties of blockchain technology has unlocked more possibilities to increase and lead the way for new initiatives towards global financial inclusion which current legacy systems have neglected.

> *Innovation at that level doesn't happen that simply, because there's already entrenched factors that prevent that from happening, whereas these lower-scaled economies, they have the ability to leapfrog. They're not going take on our legacy systems. They're just going to go to things that are really advanced and is useful now, and that's what blockchain technology and cryptocurrencies provide.*
>
> – Collin Thompson, *Intrepid Ventures*

An interesting observation, made by De Soto (2000), is that property registry formalization has been important to advance financial inclusion among undeveloped countries; registered property then serves as collateral to obtain credit. Various equipment, vehicles, and similar assets owned by individuals may not be sufficient as collateral because these assets may be missing formal legal titles, which may be a cause of lacking resources or corruption (Perlman, 2017). For instance, Kerekes and Williamson (2010) identified a trust issue within the banking industry in Peru, where land titles fail to hold any advantage over untitled land. They argued that enforcement of property rights may be the reason for the failure. As such, blockchain technology may serve as a viable enforcer by embedding a land registry distributed across banks and governments. Both Georgia[24] and Sweden[25] have developed pilots for national land registries, using permissioned and permissionless solutions, respectively. This point was

[22] http://www.banquapp.com/our-solutions/how-it-works
[23] https://tse.bitnation.co
[24] https://exonum.com/napr
[25] https://www.lantmateriet.se/en/

also emphasized by Leeor Groen:

> *I think specifically things like land registry, property topics, distribution of wealth and exchanging of information... These are all things where I think blockchain has significant potential and it's even more so accentuated in the countries that don't have the level of trust and infrastructure that we are so fortunate to have here.*
>
> – Leeor Groen, *Valley Ventures*

Notably, among the main issues that have been raised regarding blockchain registered property are the severe consequences in the event of a lost private key (Mizrahi, 2015). This concern was analyzed in Section 5.1.2, in which we presented potential solutions to proper management of private keys.

Nonetheless, legal jurisdictions will likely obstruct any international integration and interconnection to the developed part of the world. As discussed previously, regulatory frameworks associated with blockchain and cryptocurrency is yet an abstract territory. Most of our informants do, however, not see regulation as a barrier.

> *I don't see regulation as a barrier. I see regulation as a barrier in nations where the established way of doing things is in control of how laws are enacted.*
>
> – Collin Thompson, *Intrepid Ventures*

Consequently, less developed parts of the world may potentially lead the way in adopting new and innovative applications of blockchain technology. Contingent on continued growth in smartphone penetration and internet access, the non-discriminatory attributes of cryptocurrency wallets and decentralized ledgers may bring fast and inexpensive payment rails circumventing financial intermediaries. Further, immutable blockchains may offer new ways of recording ownership of both property and identity in populations where trust in the governments and financial institutions are is. Finally, the adoption such solutions hinge on the approach of regulators.

> *Financial inclusion is much, much more important for the world than some anti-*

money laundering schemes. So this is the dilemma. What is worth more? Should we exclude the rest of the world because somebody misuses the system, or should we open up for the whole world and let the malicious users get caught otherwise?

– Bjørn Bjercke, *EY*

6 Conclusion

In this thesis, we have analyzed the disrupting effect of blockchain technology on financial intermediation and the emerging possibilities within the financial system as an interoperable infrastructure. Despite the decentralized nature of blockchain, initially developed to circumvent intermediation, its usage has recently been directed toward centralized systems, thereby giving rise to new opportunities within the financial industry as a whole.
Since the launch of Bitcoin, global payments have steadily experienced a decentralizing effect by allowing direct peer-to-peer transactions without the need for any intermediary authority. Disintermediation, low fees, and instant transactions seemed to be the major buzzwords across the financial industry and have accordingly disrupted certain dimensions of the payment system by substituting conventional transaction methods with cryptocurrencies. Moreover, the function of smart contracts has further provoked the decentralizing and disintermediary effect by moving toward a crypto-economy. Nonetheless, our analysis unfolded current limitations of blockchain that may prevent the technology from having the disintermediary effect proclaimed by its proponents.

First, by its cryptographic mechanisms and immutability attribute, distributed ledgers are often perceived as trustless. Network integrity is preserved through cryptographic algorithms that incentivize users not to act maliciously or collude. In this regard, we showed that these incentives are significant for large networks such as Bitcoin and Ethereum, in particular those that follow the proof-of-work consensus algorithm, but they present vulnerabilities for smaller networks where the costs and convenience of an attack are significantly reduced. Second, while blockchain itself has shown to function as a robust and secure infrastructure, its weakest link is the input of external data which motivates and supports intermediation. As such, we conclude that the payment industry likely will experience some degree of decentralization, whereas assessment and enforcement outside the control of blockchain will prompt the need of a trusted third-party to ensure the integrity of non-native data.

We have further discussed the disrupting effect introduced by blockchain technology in raising capital. ICOs represent a novel form of financing through the sale of tokens. Thus far mostly unregulated, the space has offered participants both wildly profitable projects as well as

scams. By circumventing both the traditional venture capital industry and crowdfunding platforms, due diligence is left to the general populace. Rating agencies and the community of participants themselves are striving to provide verifiable information and transparency to the token offerings. We argue that initial coin offerings are disrupting the established venture capitalists, but that the disruption predominantly brings new opportunities. Furthermore, the initial coin offering space is characterized by regulatory uncertainty, and its future role in funding will hinge on the approach of regulators.

Furthermore, we found significant support for blockchain applications within post-trade clearing and settlement, but with little disintermediary effect. Increased efficiency in reconciliation and verification was among the paramount benefits that we identified in terms of cost reduction and efficiency in settlement processes and audit trails due to the distributed and transparent nature of blockchain. This will further streamline compliance processes such as KYC and legal obligations, and potentially reduce counterparty risk through effective liquidity management facilitated by smart contracts. However, we did not find support for near-instantaneous settlement for securities trades due to liquidity implications.

Blockchain technology could expand the global financial services industry and thereby provide financial inclusion to unbanked parts of the world. The developing regions stand to gain in particular if blockchain-enabled payment rails were to be more decentralized due to the lack of identity among its populations. In contrast, blockchain can supply these identities and accordingly unlock new possibilities without.

There are many unknowns with respect to how blockchain technology will impact financial services and intermediaries, as well as the speed with which it will do so. It is the purpose of this thesis to reflect upon and highlight the potential implications this distributed technology may constitute for the financial industry.

References

Adham, M. (2017). *Brave ICO review: 600% in 6 days.* Retrieved April 29, 2018, from https://medium.com/faast/brave-ico-review-600-in-6-days-b51d8cbb70a8

Agrawal, A., Catalini, C., & Goldfarb, A. (2011). *Friends, family, and the flat world: The geography of crowdfunding.* University of Toronto. Retrieved from https://kunnskapsverket.org/litteraturdatabase/publikasjon/friends-family-and-flat-world-geography-crowdfunding

Aitken, R. (2017). *Accord project's consortium launching first legal 'smart contracts' with hyperledger.* Retrieved June 14, 2018, from https://www.forbes.com/sites/rogeraitken/2017/07/26/accord-projects-consortium-launching-first-legal-smart-contracts-with-hyperledger/#73c15438472c

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

Allen, F., Demirgüç−Kunt, A., Klapper, L., & Peria, M. S. M. (2016). The foundations of financial inclusion: Understanding ownership and use of formal accounts. *Journal of Financial Intermediation*, *27*(5). Retrieved from https://www.sciencedirect.com/science/article/pii/S1042957315000534

Althauser, J. (2017). China's cryptocurrency market after ICO ban: Kiss the rod or die. Retrieved April 25, 2018, from https://cointelegraph.com/news/chinas-cryptocurrency-market-after-ico-ban-kiss-the-rod-or-die

Antonopoulos, A. M. (2014). *Mastering bitcoin: Programming the open blockchain.* O'Reilly Media.

Antonopoulos, A. M. (May 31, 2016). *"understanding the blockchain" - Andreas Akarintonopoulos [video file].* Retrieved May 7, 2018, from https://www.youtube.com/watch?v=mRQs9Y6CUSU

Australian National Audit Office. (2012). *Developing and managing contracts: Getting the right outcome, achieving value for money.* Retrieved 02.06.2018, from https://www.anao.gov.au/work/better-practice-guide/developing-and-managing-contracts-getting-right-outcome-achieving-value

Australian Securities Exchange Ltd. (2018). *Chess replacement.* Retrieved June 7, 2018, from https://www.asx.com.au/services/chess-replacement.htm

Badi, M., Paoli, P., Roongta, P., Snant, Y., Dab, S., Peeters, M., & Sampieri, O. (2017). *Global payments 2017: Deepening the customer relationship.* The Bostong Consulting Group. Retrieved from https://www.bcg.com/publications/2017/transaction-banking-financial-institutions-global-payments-2017-deepening-customer-relationship.aspx

Bank for International Settlements. (2017). *Basel iii: Finalising post-crisis reforms.* Retrieved from https://www.bis.org/bcbs/publ/d424.htm

Bansal, A. (2012). *Trends in retail banking channels: Meeting changing client preferences.* Capgemini Consulting. Retrieved from https://www.capgemini.com/wp-content/uploads/2017/07/trends_in_retail_banking_channels_meeting_changing_client_preferences.pdf

Barnett, C. (2016). *Why title iii of the jobs act will disappoint entrepreneurs.* Retrieved May 28, 2018, from https://www.forbes.com/sites/chancebarnett/2016/05/13/why-title-iii-of-the-jobs-act-will-disappoint-entrepreneurs/3/#5ce4e7791afc

Batiz-Benet, J., Santori, M., & Clayburgh, J. (2017). *The SAFT project: Toward a compliant token sale framework.* Retrieved from https://saftproject.com/static/SAFT-Project-Whitepaper.pdf

Batlin, A., Jaffrey, H., Murphy, C., Przewloka, A., & Williams, S. (2016). *Building the trust engine: How the blockchain could transform finance (and the world).* UBS Group Technology. Retrieved from https://www.ubs.com/microsites/blockchain-report/en/home.html

Bennington, A. (2017). *The simplest way to understand why The Dao was a security.* Retrieved April 25, 2018, from https://www.coindesk.com/simplest-way-understand-dao-security/

Benos, E., Garratt, R., & Gurrola-Perez, P. (2017). *The economics of distributed ledger technology for securities settlement.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3023779

Berger, S. C., & Gleisner, F. (2009). Emergence of financial intermediaries in electronic markets: The case of online P2P lending. *"BuR - Business Research"*, *2*(1), 39–65. doi: 10.1007/BF03343528

Bible, W., Raphael, J., Riviello, M., Taylor, P., & Valiente, I. O. (2017). *Blockchain technology and its potential impact on the audit and assurance profession.* Retrieved from https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf

Biggs, J. (2018). *Abra adds 20 cryptocurrencies to its wallet app.* Retrieved May 21, 2018, from https://techcrunch.com/2018/03/15/abra-adds-twenty-cryptocurrencies-to-its-wallet-app/

Boardman, R. (2017). *Will ICOs replace vcs? one vc isnt worried.* Retrieved June 5, 2018, from https://techvibes.com/2017/11/02/will-icos-replace-vcs-one-vc-isnt-worried

Boston Consulting Group. (2012). *Cost benefit analysis of shortening the settlement cycle.* The Boston Consulting Group. Retrieved from https://www.bcg.com/documents/file119009.pdf

Boyce, C., & Neale, P. (2006). *Conducting in-depth interviews: A guide for designing and conducting in-depth interviews for evaluation input* (Vol. Volume 2 of Pathfinder International tool series: Monitoring and evaluation). Pathfinder International.

Brannen, J. (2017). *Mixing methods: Qualitative and quantitative research.* Routledge.

Breitman, A. (2017). *How is Tezos different from Ethereum?* Retrieved June 12, 2018, from https://www.quora.com/How-is-Tezos-different-from-Ethereum

Brown, R. G. (2016). *R3 corda: A distributed ledger designed for financial services.* Retrieved 13.06.2018, from https://www.finyear.com/R3-Corda-A-Distributed-Ledger-Designed-for-Financial-Services_a35855.html

Bruno, G., McWaters, J., Galaski, R., & Chatterjee, S. (2016). *The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services.* World Economic Forum. Retrieved from https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services

Buenaventura, L. (2016). *Theres a $500 billion remittance market, and Bitcoin startups want in on it.* Retrieved May 11, 2018, from https://qz.com/775159/theres-a-500-billion-remittance-market-and-bitcoin-startups-want-in-on-it/

Butler, A. W., Cornaggia, J., & Gurun, U. G. (2010). *Do local capital market conditions affect*

consumers borrowing decisions? (Vol. 63). Retrieved from https://doi.org/10.1287/mnsc.2016.2560

Cant, B., Khadikar, A., Ruiter, A., Bronebakk, J. B., Coumaros, J., Buvat, J., & Gupta, A. (2016). *Smart contracts in financial services: Getting from hype to reality.* Retrieved from https://www.capgemini.com/wp-content/uploads/2017/07/smart_contracts_in_fs.pdf

Casey, M. J., & Vigna, P. (2018). *In blockchain we trust.* Retrieved June 18, 2018, from https://www.technologyreview.com/s/610781/in-blockchain-we-trust/

Chipongian, L. C. (2017). *86% of filipino households dont have bank accounts bsp survey.* Retrieved from https://business.mb.com.ph/2017/01/14/86-of-filipino-households-dont-have-bank-accounts-bsp-survey/

Chu, Y., Ream, J., & Schatsky, D. (2016). *Getting smart about smart contracts.* Retrieved June 12, 2018, from https://www2.deloitte.com/us/en/pages/finance/articles/cfo-insights-getting-smart-contracts.html

Coindesk. (2018). *State of blockchain Q1 2018.* Retrieved from https://www.coindesk.com/research/state-blockchain-q1-2018/?slide=39

Consultative Group to Assist the Poor. (2016). *2014 saw $31 billion in international funding for financial inclusion.* Retrieved May 10, 2018, from http://www.cgap.org/news/2014-saw-31-billion-international-funding-financial-inclusion?utm_source=01%2F19%2F2016+newsflash&utm_campaign=newsflash_011916&utm_medium=email

Copeland, T. (2018). *How will bitcoin solve its energy consumption problem?* Retrieved May 18, 2018, from https://www.newsbtc.com/2018/05/21/will-bitcoin-solve-energy-consumption-problem/

Courtois, N. T. (2014). On the longest chain rule and programmed self-destruction of crypto currencies. *Cornell University Library*. Retrieved June 14, 2018, from https://arxiv.org/abs/1405.0534

Cowley, S. (2016). *New crowdfunding rules let the small fry swim with sharks.* Retrieved May 27, 2018, from https://mobile.nytimes.com/2016/05/15/business/dealbook/new-crowdfunding-rules-let-the-small-fry-swim-with-sharks.html

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., ... Wattenhofer, R. (2016). On scaling decentralized blockchains. *Financial Cryptography and Data*

Security, 106–125. Retrieved from http://www.comp.nus.edu.sg/~prateeks/papers/Bitcoin-scaling.pdf

CrowdExpert. (2015). *Crowdfunding industry statistics 2015 2016.* Retrieved from http://crowdexpert.com/crowdfunding-industry-statistics/

Davenport, B. (2015). *What is multi-sig, and what can it do?* Retrieved June 12, 2018, from https://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do

Deloitte. (2016). Retrieved June 8, 2018, from https://www2.deloitte.com/nl/nl/pages/financial-services/articles/3-blockchain-the-benefits-of-smart-contracts.html

Demirgüç−Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2017). *The global findex database 2017.* Retrieved from https://globalfindex.worldbank.org/globalfindex/sites/globalfindex/files/overview/211259ov.pdf

De Soto, H. (2000). *Hernando de soto, the mystery of capital: Why capitalism triumphs in the west and fails everywhere else.* Bantam Press.

de Velde, J. V., Scott, A., Sartorius, K., Dalton, I., Shepherd, B., Allchin, C., ... Rennick, E. (2016). *Blockchain in capital markets: The prize and the journey.* Retrieved from https://www.euroclear.com/newsandinsights/en/Format/Whitepapers-Reports/BlockchainInCapitalMarkets.html

Diamond, D. W. (1991). Monitoring and reputation: The choice between bank loans and directly placed debt. *Journal of Political Economy*, *99*(4), 689-721. Retrieved from https://www.journals.uchicago.edu/doi/abs/10.1086/261775

Digiconomist. (2018). *Bitcoin energy consumption index.* Retrieved May 18, 2018, from https://digiconomist.net/bitcoin-energy-consumption

Dobrauz, G., Hofmann, S., Khiar, I. L., & Sahin, O. (2018). *Blockchain: key challenges to get your solution GDPR compliant.* Retrieved from https://news.pwc.ch/40735/blockchain-key-challenges-get-solution-gdpr-compliant/

Driscoll, S. (2013). *How bitcoin works under the hood.* Retrieved June 18, 2018, from http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Electronic Code of Federal Regulations. (2018). *Title 17: Commodity and securities exchanges.* Retrieved April 24, 2018, from https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=8edfd12967d69c024485029d968ee737&r=SECTION&n=17y3.0.1.1.12.0.46.176

Euler, T. (2018). *The token classification framework: A multi-dimensional tool for understanding and classifying crypto tokens.* Retrieved June 12, 2018, from http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/

EY. (2018). *Regulatory complexity is the greatest barrier to widespread blockchain adoption, while regulatory changes are the primary driver of broader integration, according to ey poll.* Retrieved June 8, 2018, from https://www.ey.com/gl/en/newsroom/news-releases/news-regulatory-complexity-is-the-greatest-barrier-to-widespread-blockchain-adoption-while-regulatory-changes-are-the-primary-driver-of-broader-integration-according-to-ey-poll

Falato, P., Coumaros, J., Buvat, J., & KVJ, S. (2013). *Backing up the digital front: Digitizing the banking back office.* Capgemini Consulting. Retrieved from https://www.capgemini.com/consulting/wp-content/uploads/sites/30/2017/07/backing_up_the_digital_front26_11_0.pdf

Falkon, S. (2017). *The story of the DAO - its history and consequences.* Retrieved May 8, 2018, from https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee

Fioramenti, L. (2018). *The cryptocurrencies disrupting international finance could stabilize african economies.* Retrieved May 20, 2018, from https://qz.com/1172730/bitcoin-litecoin-eretheum/

Fletcher, B. (2017). *Disrupting the VC industry will benefit retail investors.* Retrieved May 27, 2018, from https://observer.com/2017/11/disrupting-the-vc-industry-will-benefit-retail-investors-google-amazon-apple/

Garbade, K. D., Brown, M., Crump, R., Negro, M. D., Groen, J., Haughwout, A., ... Urry, J. (2012). Economic policy review - special issue: The evolution of banks and financial intermediation. *Federal Reserve Bank of New York*, *18*(2). Retrieved from https://www.newyorkfed.org/medialibrary/media/research/epr/2012/EPRvol18n2.pdf

Garg, N. (2018). *Who will change first banks or their customers?* Retrieved April 15, 2018, from http://www.bobsguide.com/guide/news/2018/Mar/29/who-will-change-first-banks-or-their-customers/

Gokey, T. C. (2015). *The path to a post-trade utility.* Retrieved from https://www.broadridge

.com/_assets/pdf/broadridge-the-path-to-a-post-trade-utility.pdf

Gräslund, K. (2016). *Potential of blockchain technology for financial auditing.* Retrieved from https://www.financierworldwide.com/potential-of-blockchain-technology-for-financial-auditing/#.WyatXaczZPY

Greenbaum, S., & Thakor, A. (2007). *Contemporary financial intermediation* (2nd ed.). Elsevier Inc.

Griffin, P., & Zagone, R. (2015). *Assessing the Ripple protocol: Implications of distributed networks and digital currencies for retail payments.* Ripple. Retrieved from https://ripple.com/files/ripple_submission_ecb.pdf

Grossman, S. J., & Hart, O. D. (1986). *The costs and benefits of ownership: A theory of vertical and lateral integration* (Vol. 94) (No. 4). Journal of Political Economy. doi: 10.1086/261404

GSMA Intelligence. (2017). *The mobile economy, Asia Pacific 2017.* Retrieved from https://www.gsma.com/mobileeconomy/asiapacific/

GSMA Intelligence. (2018). *The mobile economy 2018.* Retrieved from https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/05/The-Mobile-Economy-2018.pdf

Haldane, A. (2013). *Andy haldane: "banking may be on the cusp of an industrial revolution".* Retrieved June 13, 2018, from http://www.wired.co.uk/article/a-financial-forecast-from-the-bank-of-england

Hanke, S. (2017). *Zimbabwe hyperinflates again, entering the record books for a second time in less than a decade.* Retrieved May 20, 2018, from https://www.forbes.com/sites/stevehanke/2017/10/28/zimbabwe-hyperinflates-again-entering-the-record-books-for-a-second-time-in-less-than-a-decade/#1e6529253eed

Hanke, S. N. (2014). *Friedman and hanke on bitcoin.* Retrieved May 18, 2018, from https://www.cato.org/blog/friedman-hanke-bitcoin

He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., ... Verdugo-Yepes, C. (2016). Virtual currencies and beyond: Initial considerations. *IMF staff discussion note*, *16*(3). Retrieved from https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

He, D., Leckow, R., Vikram Haksar, T. M.-G., Jenkinson, N., Kashima, M., Khiaonarong, T., ... Tourpe, H. (2017). Fintech and financial services:

Initial considerations. *IMF staff discussion note*, *15*(5). Retrieved from https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985

Hellmann, T., & Puri, M. (2002). Venture capital and the professionalization of startup firms: Empirical evidence. *Journal of the American Finance Association*, *57*(1), 169-197. Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1111/1540-6261.00419

Hernández, G. O. (2018). *Accord project takes first steps toward 'blockchain agnostic' smart contract.* Retrieved June 14, 2018, from https://www.law.com/legaltechnews/2018/06/07/accord-project-takes-first-steps-toward-blockchain-agnostic-smart-contract/?slreturn=20180514173936

Hileman, G., & Rauchs, M. (2017a). Global blockchain benchmarking study. *Cambridge, Centre for Alternative Finance*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224

Hileman, G., & Rauchs, M. (2017b). Global cryptocurrency benchmarking study. *Cambridge, Centre for Alternative Finance*. Retrieved from https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf

ICOdata. (n.d.-a). *Funds raised in 2016.* Retrieved April 25, 2018, from https://www.icodata.io/stats/2016

ICOdata. (n.d.-b). *Funds raised in 2017.* Retrieved April 25, 2018, from https://www.icodata.io/stats/2017

Ijiri, Y. (1986). *A framework for triple-entry bookkeeping.*

Ivancic, P. (2018). *Bitcoin scalability update: Segwit, transaction efficiency, and Lightning Network implementation.* Retrieved June 4, 2018, from https://cryptoslate.com/bitcoin-scalability-update-segwit-transaction-efficiency-and-lightning-network-implementation/

Kahn, C. M., & Roberds, W. (2009). Why pay? an introduction to payments economics. *Journal of Financial Intermediation*, *18*(1). Retrieved from https://www.sciencedirect.com/science/article/pii/S1042957308000533?via%3Dihub

Kasireddy, P. (2017). *Fundamental challenges with public blockchains.* Retrieved June 3, 2018, from https://medium.com/@preethikasireddy/fundamental-challenges-with

-public-blockchains-253c800e9428

Kean, B. (2018). *Don't believe the hype. five largest ICO "exit scams": Expert take.* Retrieved May 1, 2018, from https://cointelegraph.com/news/dont-believe-the-hype-the-five-largest-ico-exit-scams-expert-take

Kelso, C. E. (2018). *Switzerland shows the way: Bank first to offer crypto business accounts.* Retrieved June 12, 2018, from https://news.bitcoin.com/switzerland-shows-the-way-bank-first-to-offer-crypto-business-accounts/

Kerekes, C. B., & Williamson, C. R. (2010). Propertyless in peru, even with a government land title. *The American Journal of Economics and Sociology,*, *69*, 1011-1033. Retrieved from https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1536-7150.2010.00734.x

Kharif, O. (2017). *Only one in 10 tokens is in use following initial coin offerings.* Retrieved May 9, 2018, from https://www.bloomberg.com/news/articles/2017-10-23/only-one-in-10-tokens-is-in-use-following-initial-coin-offerings

Kharpal, A. (2017). *Initial coin offerings have raised $1.2 billion and now surpass early stage VC funding.* Retrieved May 7, 2018, from https://www.cnbc.com/2017/08/09/initial-coin-offerings-surpass-early-stage-venture-capital-funding.html

Kharpal, A. (2018). *Founders of a cryptocurrency backed by floyd mayweather charged with fraud by sec.* Retrieved May 9, 2018, from https://www.cnbc.com/2018/04/03/floyd-mayweather-backed-cryptocurrency-ico-fraud-sec-says.html

Lazanis, R. (2015). *How technology behind Bitcoin could transform accounting as we know it.* Retrieved May 30, 2018, from https://techvibes.com/2015/01/22/how-technology-behind-bitcoin-could-transform-accounting-as-we-know-it-2015-01-22

Lee, T. B. (2018a). *Bitcoin has a huge scaling problem - Lightning could be the solution.* Retrieved June 14, 2018, from https://arstechnica.com/tech-policy/2018/02/bitcoins-lightning-network-a-deep-dive/

Lee, T. B. (2018b). *Bitcoin's transaction fee crisis is over for now.* Retrieved June 4, 2018, from https://arstechnica.com/tech-policy/2018/02/bitcoins-transaction-fee-crisis-is-over-for-now/

Lin, Q., Yan, H., Huang, Z., Chen, W., Shen, J., & Tang, Y. (2018). An ID-Based linearly homomorphic signature scheme and its application in blockchain. *IEEE Access*, *6*,

20632-20640. Retrieved from https://ieeexplore.ieee.org/document/8302552/

Liptak, A. (2018). *Telegram has raised a total of $1.7 billion from its two pre-ICO sales.* Retrieved May 4, 2018, from https://www.theverge.com/2018/4/1/17186004/telegram-presale-open-network-app-ico-cryptocurrency-ton

Mainelli, M., & Milne, A. (2016). *The impact and potential of blockchain on the securities transaction lifecycle.* European Institute of Financial Regulation. Retrieved from http://eifr.eu/news/4405/swift-institute-working-paper-no-2015-007-the-impact-and-potential-of-blockchain-on-the-securities-transaction-lifecycle

Martin, W. (2017). *Cryptocurrencies are continuing to fall after China's shock ICO ban.* Retrieved April 25, 2018, from http://nordic.businessinsider.com/bitcoin-ethereum-price-fall-china-ico-crackdown-2017-9?r=UK&IR=T

Masinde, J. (2016). *Kenya's M-Pesa platform is so successful regulators worry it could disrupt the economy.* Retrieved May 17, 2018, from https://qz.com/873525/safaricoms-m-pesa-has-kenyas-government-worried-what-happens-in-the-event-of-a-crash/

Meguerditchian, V. (2017). *Roadmap for blockchain standards.* Retrieved from https://www.standards.org.au/getmedia/ad5d74db-8da9-4685-b171-90142ee0a2e1/Roadmap_for_Blockchain_Standards_report.pdf.aspx

Merced, M. J. d. l. (2017). *Lehman brothers profit climbs 27%.* Retrieved June 18, 2018, from https://www.nytimes.com/2007/06/13/business/13wall.html

Meyer, D. (2018). *Blockchain technology is on a collision course with EU privacy law.* Retrieved May 21, 2018, from https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/

Minahan, T. (2005). *The contract management solution selection report: Handbook for clm strategy & solution selection.* Aberdeen Group Inc. Retrieved from ftp://public.dhe.ibm.com/software/emea/dk/frontlines/Aberdeen_2005_Contract_Mgmt.pdf

Mizrahi, A. (2015). *A blockchain-based property ownership recording system.* Retrieved May 29, 2018, from https://chromaway.com/papers/A-blockchain-based-property-registry.pdf

Monks, K. (2017). *M-Pesa: Kenya's mobile money success story turns 10.* Retrieved May 16, 2018, from https://edition.cnn.com/2017/02/21/africa/mpesa-10th-anniversary/index.html

Mougayar, W. (2017). *Tokenomics - a business guide to token usage, utility and value.* Retrieved March 19, 2018, from https://medium.com/@wmougayar/tokenomics-a-business-guide-to-token-usage-utility-and-value-b19242053416

Nachamkin, M. (2017). *How to create your own ethereum token in an hour (ERC20 + Verified).* Retrieved May 9, 2018, from https://steemit.com/ethereum/@maxnachamkin/how-to-create-your-own-ethereum-token-in-an-hour-erc20-verified

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* Retrieved from https://bitcoin.org/bitcoin.pdf

Nielsen, J. (2018). *What are atomic swaps?* Retrieved June 16, 2018, from https://coincodex.com/article/1264/what-are-atomic-swaps/

Norton Rose Fulbright. (2016). *Can smart contracts be legally binding contracts?* Retrieved from http://www.nortonrosefulbright.com/files/r3-and-norton-rose-fulbright-white-paper-full-report-144581.pdf

Payton, O. (1979). *Research: The validation of clinical practice.* F. A. Davis Company.

Peaster, W. M. (2018). *What are atomic swaps? our guide to a revolution in decentralization.* Retrieved June 16, 2018, from https://blockonomi.com/atomic-swaps/

Perlman, L. (2017). *Distributed ledger technologies and financial inclusion.* Retrieved from https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201703/ITU_FGDFS_Report-on-DLT-and-Financial-Inclusion.pdf

Peterhoff, D., Miller, A., Romeo, J., Patel, H., & Holroyd, B. (2014). *The capital markets industry.* Retrieved February 13, 2018, from http://www.oliverwyman.com/our-expertise/insights/2014/sep/the-capital-markets-industry.html

Posnak, E. (2017). *On the origin of Tezos.* Retrieved June 12, 2018, from https://medium.com/on-the-origin-of-smart-contract-platforms/on-the-origin-of-smart-contract-platforms-tezos-5eee6255c791

Psaila, S. (2017). *Blockchain: A game changer for audit processes?* Deloitte Consulting. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/mt/Documents/audit/dt_mt_article_blockchain_gamechanger-for-audit-sandro-psaila.pdf

Redman, J. (2017). *Bitcoin's quirky genesis block turns eight years old today.* Retrieved from https://news.bitcoin.com/bitcoins-quirky-genesis-block-turns-eight-years-old-today/

Ripple. (2016a). *The cost-cutting case for banks - the ROI of using Ripple and XRP for*

global interbank settlements. Retrieved from https://ripple.com/files/xrp_cost_model_paper.pdf

Ripple. (2016b). *Ripple solutions guide.* Retrieved from https://bravenewcoin.com/assets/Whitepapers/ripple-solutions-guide.pdf

Ronen, J. (2010). *Corporate audits and how to fix them.* Retrieved from http://people.stern.nyu.edu/jronen/articles/Corporate_Audits.pdf

Rowley, J. (2018). *ICOs delivered at least 3.5x more capital to blockchain startups than vc since 2017.* Retrieved May 5, 2018, from https://techcrunch.com/2018/03/04/icos-delivered-at-least-3-5x-more-capital-to-blockchain-startups-than-vc-since-2017/

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students.* Pearson Professional Limited, Pearson Education Limited.

SaveOnSend. (2018). *Western Union: permanent leader of international money transfer?* Retrieved May 11, 2018, from https://www.saveonsend.com/blog/western-union-money-transfer/

Schleifer, T. (2018). *Telegram is scuttling its public ICO. here's why.* Retrieved June 4, 2018, from https://www.recode.net/2018/5/2/17311988/telegram-ico-public-sale

Schneider, J., Blostein, A., Lee, B., Kent, S., Groer, I., & Beardsley, E. (2016). *Profiles of innovation: Blockchain - putting theory into practice.* Retrieved from https://msenterprise.global.ssl.fastly.net/wordpress/2017/07/Goldman-Sachs-Blockchain-putting-theory-to-practice.pdf

SEC. (n.d.). *Jumpstart our business startups act.* Retrieved May 28, 2018, from https://www.sec.gov/info/smallbus/secg/rccomplianceguide-051316.htm

Seel, G. (2016). *Is blockchain really the answer to global payments?* FinExtra. Retrieved June 2, 2018, from https://www.finextra.com/blogposting/13134/is-blockchain-really-the-answer-to-global-payments

Sehra, A., Smith, P., & Gomes, P. (2017). *Economics of initial coin offerings.* Retrieved from http://www.allenovery.com/SiteCollectionDocuments/ICO-Article-Nivaura-20170822-0951%20%20-%20Final%20Draft.pdf

Shamir, A. (1979). How to share a secret. *Massachusetts Institute of Technology*, *22*(11). Retrieved from https://cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf

Sharma, T. K. (2018). *How does blockchain use public key cryptography?* Retrieved June

18, 2018, from https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/

Shin, L. (2017). *Crypto boom: 15 new hedge funds want in on 84.000% returns.* Retrieved May 7, 2018, from https://www.forbes.com/sites/laurashin/2017/07/12/crypto-boom-15-new-hedge-funds-want-in-on-84000-returns/#4752de31416a

Simonite, T. (2017). *Bitcoin is soaring. here's why it's not ready for the big time.* Retrieved June 3, 2018, from https://www.wired.com/story/bitcoin-is-soaring-heres-why-its-not-ready-for-the-big-time/

Smart Contracts Alliance, & Deloitte. (2016). *Smart contracts: 12 use cases for business & beyond.* Retrieved from https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-12-Use-Cases-for-Business-and-Beyond_Chamber-of-Digital-Commerce.pdf

Stark, E. (2016). *What is the Lightning Network and how can it help Bitcoin scale?* Retrieved June 14, 2018, from https://coincenter.org/entry/what-is-the-lightning-network

State of Startups. (2017). *State of startups 2017.* Retrieved May 5, 2018, from http://stateofstartups.firstround.com/2017/

Statista. (2018). *Ic3: total damage caused by reported cyber crime 2001-2016.* Retrieved May 4, 2018, from https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/

Steenis, H. V., Graseck, B. L., Simpson, F., & Faucette, J. E. (2016). *Global insight: Blockchain in banking: Disruptive threat or tool?* Retrieved from https://www.febelfin.be/en/global-insight-blockchain-bankingdisruptive-threat-or-tool

Suberg, W. (2018). *Vietnam: Pincoin, ifan ICOs exposed as scams that allegedly stole $660 million.* Retrieved April 28, 2018, from https://cointelegraph.com/news/vietnam-pincoin-ifan-icos-exposed-as-scams-that-allegedly-stole-660-million

Szabo, N. (1996). Smart contracts: Building blocks for digital markets. *Extropy Nr.16*. Retrieved from http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Tapscott, D., & Tapscott, A. (2017). *Blockchain revolution: How the technology behind bitcoin and other cryptocurrencies is changing the world.* Portfolio Penguin.

Tasca, P., Aste, T., Pelizzon, L., & Perony, N. (2016). *Banking beyond banks and money: A guide to banking services in the twenty-first century.* Springer International Publishing Switzerland 2016.

The Economist. (2015). *Why does Kenya lead the world in mobile money?* Retrieved May 16, 2018, from https://www.economist.com/the-economist-explains/2015/03/02/why-does-kenya-lead-the-world-in-mobile-money

The World Bank. (n.d.-a). *Commercial bank branches (per 100.000 adults).* Retrieved May 16, 2018, from https://data.worldbank.org/indicator/FB.CBK.BRCH.P5?order=wbapi_data_value_2013+wbapi_data_value+wbapi_data_value-last&sort=asc&year_high_desc=false

The World Bank. (n.d.-b). *Remittance prices worldwide.* Retrieved May 16, 2018, from http://remittanceprices.worldbank.org/en

The World Bank. (2018). *Remittance prices worldwide.* Retrieved from https://remittanceprices.worldbank.org/sites/default/files/rpw_report_march2018.pdf

Toit, G. d., & Burns, M. (2017). *Evolving the customer experience in banking: 'alexa, move my bank accounts to ...'.* Retrieved April 15, 2018, from http://www.bain.com/publications/articles/evolving-the-customer-experience-in-banking.aspx

Trocmé, J. (2018). Cybercrime: A potential existential threat for corporates. *LinkedIn Pulse*. Retrieved May 4, 2018, from https://www.linkedin.com/pulse/cybercrime-potential-existential-threat-corporates-johan-trocm%C3%A9/

Tyra, J. M. (2014). *Triple entry bookkeeping with bitcoin.* Retrieved February 18, 2018, from https://bitcoinmagazine.com/articles/triple-entry-bookkeeping-bitcoin-1392069656/

United Nations. (n.d.). *#envision2030 goal 8: Decent work and economic growth.* Retrieved June 18, 2018, from https://www.un.org/development/desa/disabilities/envision2030-goal8.html

Untitled INC. (n.d.). *Token classification framework.* Retrieved May 13, 2018, from http://www.untitled-inc.com/token-classification-framework/

US Securities and Exchange Commission. (2017). *SEC issues investigative report concluding DAO tokens, a digital asset, were securities.* Retrieved from https://www.sec.gov/news/press-release/2017-131

Vigna, P., & Casey, M. J. (2018). *The truth machine: The blockchain and the future of*

everything.

Walle, A. H. (2015). *Qualitative research in business : A practical overview*. Cambridge Scholars Publishing.

Werbach, K. D., & Cornell, N. (2017). Contracts ex machina. *67 Duke Law Journal, Forthcoming*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2936294

Wessel, M. (2013). *Don't build your startup outside of silicon valley.* Retrieved May 4, 2018, from https://hbr.org/2013/10/dont-build-your-startup-outside-of-silicon-valley

Williams-Grut, O. (2016). *'crowdfunding is growing up': Syndicateroom just partnered with the london stock exchange.* Retrieved March 2, 2018, from http://www.businessinsider.com/syndicateroom-get-intermediary-status-with-london-stock-exchange-2016-3?r=UK&IR=T&IR=T

Williamson, O. E. (1993). Transaction cost economics and organization theory. *Industrial and Corporate Change*, *2*(2), 107–156. Retrieved from https://academic.oup.com/icc/article-abstract/2/2/107/888408?redirectedFrom=fulltext

Yermack, D. (2013). Is bitcoin a real currency? an economic appraisal. *NBER Working Paper Series*(19747). Retrieved from https://www.nber.org/papers/w19747.pdf

Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance, Forthcoming*. Retrieved 15.01.18, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2700475

Zheng, Z., Zhao, C., Fan, H., & Wang, X. (2017). A key backup scheme based on bitcoin. *IACR Cryptology ePrint Archive*, 704. Retrieved from https://www.semanticscholar.org/paper/A-Key-Backup-Scheme-Based-on-Bitcoin-Zheng-Zhao/74d2a52930ec741c35cbb4e34d5c5a4c46a12af9

Zyskind, G., Nathan, O., & Pentland, A. S. (2015). *Enigma: Decentralized computation platform with guaranteed privacy.* Retrieved from https://arxiv.org/pdf/1506.03471.pdf

Appendix A: Interview Request

Master Thesis, Norwegian School of Economics
Topic: Blockchain and financial intermediation

We are analyzing the impact of blockchain technology in financial markets and aim to assess two main topics: The impact on banks and other financial intermediaries and opportunities within financial services. We would like to know your and your organization's view of the manner, in particular discussing the following topics:

- Technological innovation
  - Current applications and the value added by blockchain
- The role of banks and other financial intermediaries
  - How have financial services changed after recent technological waves?
- The impact of blockchain on financial intermediaries
  - Can blockchain replace certain financial services?
  - Scalability of smart contracts
  - ICOs and the token economy
- Opportunities and applications of blockchain technology in financial services
  - Infrastructure (e.g. trade settlement and processing, security, privacy, transparency)
  - Accounting and reporting, KYC, AML, lending, autonomous financial instruments, etc.

The interviews may be conducted face-to-face, Skype, phone, or other applications, and should last around 45 minutes. The information will be gathered primarily by notes; however, we may ask for your consent to audio record the interview.

We may also ask for your consent to recognize you in our publication, in which case all quotations will be sent to you for verification. If no consent is given, all personal details will be anonymized, and after completion of the project, 20 July 2018 at the latest, all collected data will be deleted. Also note that you can withdraw at any time during the project in which case all personal data will be instantly made anonymous.

We sincerely hope that you wish to contribute to our study and we will certainly appreciate it. Please do not hesitate to ask any questions regarding the project. Following below are our contact information- we hope to hear from you.

Best regards,

Philip Alexander Stendahl
Phone: ……..
Email: ……..

Jørgen Brekke Brastad
Phone: ……
Email: ……

The study has been notified to the Data Protection Official for Research, NSD – Norwegian Centre for Research Data.

Appendix B: List of Informants

Master Thesis, Norwegian School of Economics
Topic: Blockchain and financial markets

#	Name	Title	Industry/Sector	Company	Country
1	Peter Frøystad	Technical Product Owner	Financial Technology	Fintech Innovation	Norway
2	Torbjørn Bull-Jenssen	Senior Economist	Economic Consulting	Menon Economics	Norway
3	Mariana Bontempo	Project Manager	Technology Consulting	Applied Blockchain	U.K.
4	Marte Kopperstad	Head of Personal Banking Segments and Strategy	Banking	Nordea	Norway
5	Bjørn Bjercke	Associate Partner / Swiss blockchain lead	Financial Services	EY	Switzerland
6	Stylianos Kampakis	Research Fellow	Technology	UCL Centre of Blockchain Technologies	U.K.
7	Collin Thompson	Co-Founder & Managing Director	Financial Services	Intrepid Ventures	Hong Kong
8	Leeor Groen	Manager	Financial Services	Blockchain Valley Ventures	Switzerland
9	Guenther Dobrauz	Partner & Leader of PwC Legal	Legal services	PwC	Switzerland
10	Lukas Wohlgemuth	Associate	Financial Services	Strategy &, part of the PwC network	Switzerland
11	Yusuf Barman	Financial Auditor	Financial Services	KPMG	Switzerland
12	Johan Torås Halseth	Lightning Protocol Engineer	Technology	Lightning Labs	Norway
13	Ketil Qvam Andersen	Senior Advisor, Strategy & Business Analysis	Financial Services	Oslo Børs VPS	Norway
14	Miguel Cuneta	Co-Founder & CCO	Financial Services	SCI Ventures Inc.	Philippines
15	Lasse Meholm	Head of Blockchain & DLT Strategy	Banking	DNB	Norway
16	Finn Kinserdal	Head of Department Accounting, Auditing and Law	Academia	Norwegian School of Economics	Norway
17	Maureen Murat	Of Counsel	Legal services	Cogent Law Group	U.S.

Disclaimer: The views and opinions expressed by our informants in this thesis do not necessarily reflect those of their respective companies.

Appendix C: Interview Guide

Master Thesis, Norwegian School of Economics
Topic: Blockchain and financial markets

Factual questions and introduction
Get an overview of the company and the participant's role in the company and potentially relevant personal interests

- **What are the primary services provided by your company/entity?**
- **What is your role in the company?**

Technological innovation
Get an overview on the company's involvement and view on technological innovation

- **What does your company do in terms of technological innovation?**
  Probe: Innovative solutions, strategy, target areas

- **What are the issues of the core infrastructure and why have companies who are operating on legacy systems avoided its digitalization?**
  Probe: Issues of the current infrastructure, back-office processes, implications of changing the core infrastructure

Blockchain technology
Get an overview on the participant's and company's involvement in blockchain technology, and understand their opinions and views on the potentials of the rising technology

- **How familiar are you with blockchain technology?**
  Probe: Standpoint and general knowledge

- **What is your and your company's opinion on blockchain technology and its recent hype within financial services?**
  Probe: Positively- or negatively biased

- **What are the advantages within settlement processes, both for payments and securities trades (if any)?**
  Probe: Efficiency in clearing processes, infrastructure of current cross-border payments, KYC, netting procedures.

- **How does shorter settlement cycles affect liquidity and counter-party risk?**
  Probe: Scalability of shorter trade settlement cycles; benefits and drawbacks

- **What is your opinion on the observed ICO trend? Can this trend continue or how will it potentially change in the future?**
  Probe: Pros and cons of ICOs, scam vs. reliable projects, regulatory aspects

- **Should venture capitalists feel threatened by ICOs?**
  Probe: Value added by venture capitalists; opportunities, SAFT-framework

- **What are the current implications regarding security of blockchains?**
  Probe: 51% attack, management of private keys, permissioned- vs. permissionless networks

- **Can you tell us about the data privacy properties of blockchains? How do these comply with data protection regulations (e.g. GDPR)**
  Probe: transparency issues, lack of control in decentralized networks, immutability issues ("right to be forgotten"), customer data protection

- **Assuming a permissioned blockchain, compliant to privacy regulations. Will this have any advantages over current systems, in terms of giving customers more control?**
  Probe: Managing customer data on a blockchain; regulatory reporting; KYC

- **What are the advantages regarding accounting and auditing (if any)?**
  Probe: Proof of existence, data integrity, corporate governance and monitoring; supervision, automation of mandatory reporting; continuous auditing

- **Can smart contracts be applied for long-term and complex contracts?**
  Probe: Scalability, benefits and limitations of smart, enforcement, off-chain events, incompleteness of contracts

- **Can blockchain enable and provide financial services to undeveloped countries? Will regulation be a barrier in terms of AML and other criminal activities?**
  Probe: Banking the unbanked; financial inclusion, regulatory implications regarding cryptocurrencies, current initiatives

- **What are the core roles of banks and other financial intermediaries and what are the main threats of blockchain?**
  Probe: Determine important roles and values of intermediation; what benefits of blockchain pose as a threat to banking; cryptocurrency-related financial services

- **Other reflections regarding opportunities within- or impact on financial services?**
  In your opinion, what is the major advantage of blockchain technology within financial services?