UNIVERSITY OF LJUBLJANA
FACULTY OF ECONOMICS

MASTER'S THESIS

AN ANALYSIS OF VALUE CREATION WITH THE BLOCKCHAIN TECHNOLOGY

Ljubljana, September 28th, 2018 JURE ŠIKONJA

AUTHORSHIP STATEMENT

The undersigned Jure Šikonja, a student at the University of Ljubljana, Faculty of Economics, (hereafter: FELU), author of this written final work of studies with the title An analysis of value creation with the blockchain technology, prepared under supervision of Igor Lončarski, PhD,

DECLARE

1. this written final work of studies to be based on the results of my own research;
2. the printed form of this written final work of studies to be identical to its electronic form;
3. the text of this written final work of studies to be language-edited and technically in adherence with the FELU's Technical Guidelines for Written Works, which means that I cited and / or quoted works and opinions of other authors in this written final work of studies in accordance with the FELU's Technical Guidelines for Written Works;
4. to be aware of the fact that plagiarism (in written or graphical form) is a criminal offence and can be prosecuted in accordance with the Criminal Code of the Republic of Slovenia;
5. to be aware of the consequences a proven plagiarism charge based on this written final work could have for my status at the FELU in accordance with the relevant FELU Rules;
6. to have obtained all the necessary permits to use the data and works of other authors which are (in written or graphical form) referred to in this written final work of studies and to have clearly marked them;
7. to have acted in accordance with ethical principles during the preparation of this written final work of studies and to have, where necessary, obtained permission of the Ethics Committee;
8. my consent to use the electronic form of this written final work of studies for the detection of content similarity with other written works, using similarity detection software that is connected with the FELU Study Information System;
9. to transfer to the University of Ljubljana free of charge, non-exclusively, geographically and time-wise unlimited the right of saving this written final work of studies in the electronic form, the right of its reproduction, as well as the right of making this written final work of studies available to the public on the World Wide Web via the Repository of the University of Ljubljana;
10. my consent to publication of my personal data that are included in this written final work of studies and in this declaration, when this written final work of studies is published.

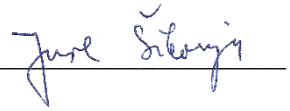
Ljubljana, September 28th, 2018 Authors signature: 

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APENDIXES

LIST OF ABBREVATIONS

sl. – Slovene

GDP – Gross domestic product

DLT – Distributed ledger technologies

HTTP –Hypertext transfer protocol

PoW – Proof of work

PoS – Proof of stake

DPoS – Distributed proof of stake

CBCCs – Central bank cryptocurrencies

CPI – Consumer price index

QTM – Quantity theory of money

CSDs – Central securities depositories

ICSDs – International central securities depositories

CCPs – Central counterparty clearing houses

EMIR – European market infrastructure regulation

RTGS – Real time gross settlement

ACH – Automated clearing house

RSPs – Remittance service providers

AML – Anti-money laundering

CFT – Counter terrorism financing

ICOs – Initial coin offerings

USA – United States of America

FOMO – Fear of missing out

IM – Investment management

AuM – Assets under management

C2C – Consumer to consumer

B2B – Business to business

FDI – Foreign direct investment

APAC – Asia Pacific

INTRODUCTION

Finance industry is being transformed as a part of new digital or technology revolution with a pace not seen before. New technologies such as electronic payments, big data analytics, artificial intelligence and virtual currencies are leading to greater speed, transparency and lower transaction costs. The concept of blockchain is most recognized as the underlying technology upon which cryptocurrency Bitcoin is built. Although there has been much excitement about the disruptive potential of the technology, there is also much confusion as some people still think blockchain is used only to enable criminal and anonymous transfers of money. The reality is far from that. In fact, blockchain's main promise is to deliver a new approach to data and value management. Until now the most important issues of privacy, security and trust regarding data and value transfer between different counterparties were solved by use of trusted third-party intermediaries (Kursh & Gold, 2016). Fundamental trust issues were mitigated by transacting through neutral central authorities in which both transacting parties have confidence. Independent third party's mission was to serve as the central mediator, to ensure that transaction parties own what they have agreed to exchange, to ensure the transaction occurs and finally, to ensure that the respective value transfer occurs.

We can see blockchain as an ultimate trust machine. Computer resources and cryptography are used in order to maintain a distributed, time-stamped and immutable consensus ledger of all previous transactions. Distributed nature removes a single point of failure and can disintermediate the process of traditional information and value exchange. Shared public database offers a new architecture where all capital market participants work from common and shared datasets, in near real-time, and where supporting operations are either streamlined or made redundant (Credit Suisse, 2016).

Blockchain in essence can support a variety of different applications, from smart contracts, asset registries to borderless and near instant value transfers. While its current capabilities are still limited, it offers fascinating future prospects. The main purpose of this master thesis is to describe this technology and analyse ways in which it adds value to an economy. I describe how it works, its different versions and possible applications in finance and its different sectors. Next to that the purpose is to calculate potential reductions in fees that will affect main players along the value chain of capital markets. To explore possible use cases of blockchain, I start the thesis with the aim to describe major shortcomings of current transaction systems. Modern finance infrastructure relies on use of third party intermediaries where data is redundantly updated and reconciled. The first goal of the thesis is to introduce the concept of blockchain: what it is, how it works and what types of blockchain exist. I aim to describe benefits that different implementations of blockchain can bring in making of an immutable source of truth that is uniformly shared across network participants and has embedded self-executing commitments. The second goal of the thesis is to investigate where and for what purpose can the blockchain be put to use in the modern financial infrastructure.

I explore different applications of the technology in the traditional infrastructure of capital markets. With its design blockchain could render obsolete current services of legacy players, encourage vertical integration and disintermediate incumbents and their business models. I try to describe ways to re-engineer, rationalize and increase the efficiency of legacy systems and technology through cost removal, increase of efficiency and explore potential ways to deliver new revenue streams in different segments of finance: **blockchain based currencies, clearing and settlement, payments, fundraising, smart contracts and investment management**. Next comes the empirical part where my goal is to estimate blockchain's added value via potential reduction in fees and revenue sources for three major segments of finance: **transactions, clearing and fundraising**. My goal in the fourth chapter is to investigate main projects and firms which are deploying new solutions built with the help of the technology. I describe their business models, provide overview of the infrastructure they are building and explore where they can help rationalize and increase the efficiency of the current system. Last chapter concludes the master thesis and is followed by the reference list used throughout my work.

I used data and literature provided by academics, leading banking/consulting players and up-to-date internet resources. However, I did face several limitations in terms of data and research available as this is a very nascent technology that lacks demonstrable historical use case records. This was especially evident when I tried to evaluate and quantify blockchain's added value. Therefore, calculations presented at the end should be used for information purposes only.

1 OVERVIEW OF BLOCKCHAIN AND BLOCKCHAIN BASED SOLUTIONS

1.1 Blockchain beginnings and how it all started

Cryptographically secured chain of blocks was first described in 1991 by Stuart Haber and Scott Stornetta. A year later they implemented Merkle trees to the blockchain and were able to collect several files into one block (Haber & Stornetta, 1991). However, it was only in 2008 that the Blockchain became more recognized when a person or a group known under the alias "Satoshi Nakamoto" published the Bitcoin whitepaper. The concept of a digital currency or a "purely peer-to peer version of electronic cash" named Bitcoin had been built on a public ledger of all transactions – later named blockchain – and has used peer-to-peer network and a distributed timestamping server, where network manages the database automatically and solves one of the main trust issues - the double spending problem. For the Bitcoin to work as cash, it had to be able to change hands without being capable of being spent twice by the same person. Usually, in conventional payment systems, there is a bank that acts as a trusted third party and serves as a database that contains the amount of money in circulation at any given time (Economist Staff, 2015). Now, in this digital era, we came

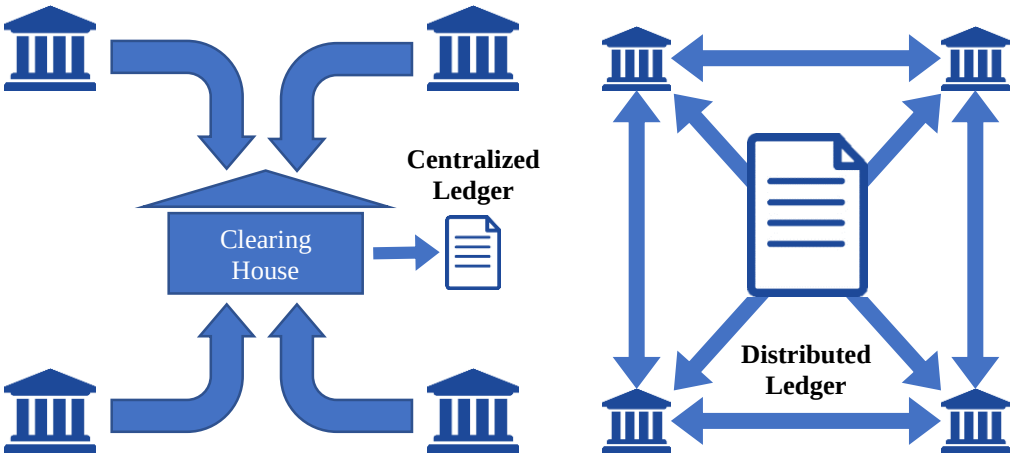
up with the concept of blockchain which solves those issues through a public record of ownership and transactions. I will go more in detail below, where I will start by describing the double spend problem and how it is avoided with the use of blockchain. Extending far beyond popular cryptocurrencies or cryptoassets such as Bitcoin or Ethereum, blockchain technology is bringing disintermediation to almost all industries. A survey performed by the World Economic Forum (2015, p. 24) highlights that financial services will be among most disrupted industries and that at least 10 % of global gross domestic product (GDP) will be stored on blockchain infrastructure by 2027.

Private institutions (i.e. banks) realized that they could use the core idea and underlying principles of blockchain and create a permissioned blockchain, where the transactions' validation is performed by a preselected entity or members of consortium. Due to decentralized nature of the technology, the term blockchain in the context of a permissioned private ledger is highly controversial and often disputed. This is the reason why distributed ledger technologies (DLTs) emerged as another term. However, to avoid confusion, blockchain idiom will be used throughout the thesis.

1.2 Double spend problem

While there are many electronic payment schemes and some of those are coin based, where a certain part of code stored locally by a user represents a fixed amount of value, coin based systems run the risk that many copies of this same code are spent by two different users. In order to make efficient electronic transfer of value, we need to have detection and double spending problem prevention. Usually, in the "real" economy, there is a central entity (i.e. a central bank) assumed in between two transacting parties and it handles or oversees all of the transactions. However, in the off-line scenarios (where a connection to the central bank is not available), double spending detection techniques are used. They are used to find the wrongdoer of this act at some later time. This presents a huge risk as a user can spend a unit of currency several times in a short period of time before being noticed. Such double spending issues, being this on-line or off-line, can lead to inflation of money as with counterfeit money where new currency is added into circulation. With more money in the circulation, each unit of currency is therefore worth less. Furthermore, such issues diminish trust in the same. As stated above, till now the prevention of double spending has taken two forms: centralized and decentralized. Former is usually done by an on-line central trusted third party (a central bank) that verifies whether a unit of currency has already been spent. This approach then represents a single point of failure from both availability and trust viewpoints. On the other hand, a distributed or decentralized system has firstly been proposed and implemented by the Bitcoin digital currency. It uses a scheme where transactions are seen by and exchanged among network participants via resource intensive work, ensuring that no unit of currency is spent twice and thus avoids the need for a centralized third party verification. As seen on Figure 1 transactions are therefore rather recorded on a public and distributed ledger (Hoepman, 2008).

Figure 1: A distributed ledger and the underlying infrastructure



Source: Santander InnoVentures, Oliver Wyman & Anthemis Group (2015).

1.3 The shortcomings of current transaction systems and issues finance industry is facing

Historically, exchange of value was done with the use of trusted generally accepted instruments such as minted coins, paper money or letters of credit. Modern banking systems have emerged just recently if we look at the whole history of human kind.

With every important technological innovation such as the Telephone, the Internet, credit card systems or mobile technologies, we have achieved greater speed, convenience and efficiency of transactions. The distance between buyers and sellers has been virtually totally eliminated - no matter if exchanging parties lived several kilometres or thousands of miles apart.

However, the transactions are still inefficient, expensive and exposed to various threats and suffer from following constraints:

- **Cash limitations.** Cash is useful only in smaller transactions happening locally. Also, it can be replicated relatively easy due to its non-complex construction.
- **Double spend problem.** Digital value faces threat of being duplicated and spent several times.
- **Time consuming.** The time between transaction execution and settlement is very long, especially if we perform overseas transactions - settlement time can take as much as 3 days.
- **Trust issues.** Modern transactions systems often have blurred trust, requiring exchanging parties to use a verified third party intermediary to perform a transaction.
- **Intermediation.** Mostly all (financial) transactions currently go through a trusted third party intermediary, making them costly and time consuming.

Low net interest margins, high levels of non-performing loans, high cost to income ratios, and effects of tightened regulations are among the key drivers affecting low profitability of European, American or Eastern financial institutions. This has put severe pressure on severely affected banks and their business models from the start of the Global Financial Crisis in 2008.

In recent years the technological penetration has led to flourishing of Internet finance. Non-stop innovation and emergence of new Internet financial products and services have led to departure of significant amounts of household saving deposits and increased bank's cost of capital. Additionally, trust in the financial sector being on the all-time low levels, with rising pressure from non-traditional and tech players all trying to eat into revenue pie, current banking and financial industry players are being transformed by powerful forces. Their ability to cope with innovation and cost efficiency is being severely tested, putting them under enormous pressure to survive. There are only two ways for financial industry players if they want to last – either embrace change and transform or they will die (PricewaterhouseCoopers, 2014a).

1.4 The blockchain promise – what is it and how it functions

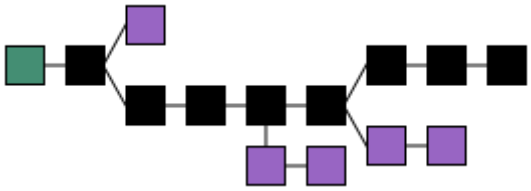
As stated above, the first blockchain made public was the one conceptualized by Satoshi Nakamoto in 2008. Originally called block chain and a year later implemented as a core infrastructure of the cryptocurrency Bitcoin where it serves as the public ledger on which all transactions are written. It was the first successful application of electronic cash that solved both the double spending problem as well as avoidance of the trusted third party authority. A blockchain is a decentralized and distributed digital ledger. Transactions are recorded chronologically, linked and secured using cryptography. Blocks are linked together and assigned with a timestamp and transaction data. By design, a blockchain or distributed ledger records transactions between two parties efficiently, permanently and makes it possible to verify entries easily. It is typically managed by a peer-to-peer network, which is ruled by a certain protocol or set of rules. Once data is recorded onto the ledger, blocks cannot be amended retroactively without alteration of all subsequent blocks. If one would aim to do so, network majority consensus would be required. It is therefore very hard, if not impossible, to alter the transactions that have been written onto blockchain and are then shared across a network of computers (Economist staff, 2015).

Main Audit and verification of transactions are therefore performed easily and inexpensively as all data is uniformly shared across all computers in the network. Computers are authenticating transactions via mass collaboration and are incentivized by collective self-interests to do so. The use of blockchain removes the possibility of infinite reproducibility of a digital asset and makes participants' uncertainty regarding data security marginal. Blockchain's have been described as a value-exchange protocol, solving the long-standing double spend problem. Use of blockchain to transfer value has indicated that it can be

completed more quickly, more safely and cheaply than with traditional transaction systems (Bheemaiah, 2015).

Figure 2 shows blockchain built out of series of blocks. Main chain (black) consists of the longest series of blocks from the start (green) to the current one. Orphan blocks in purple can be found outside of the main chain.

Figure 2: A series of blocks known as a blockchain



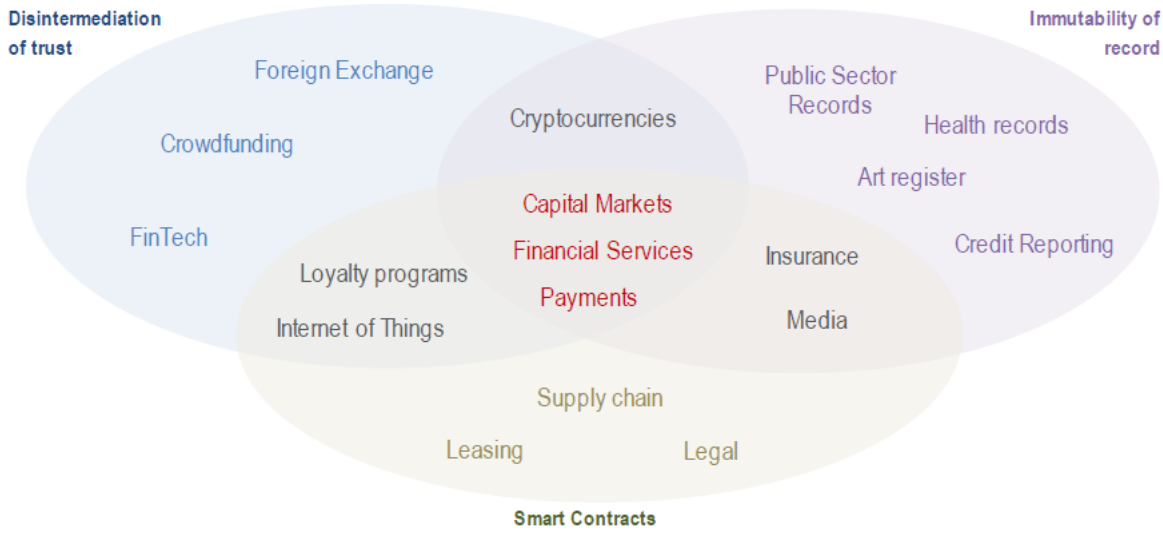
Source: Own work.

Blockchain technology presents disruptive benefits in three ways:

- **Immutability of record.** There is an audit trail.
- **Disintermediation of trust.** Less reliance on trusted third parties.
- **Smart contracts.** Self-executing commitments, fulfilment of which can be trusted.

The Figure 3 below shows where those three potential disruptive benefits could be implemented.

Figure 3: Blockchain's potential use cases

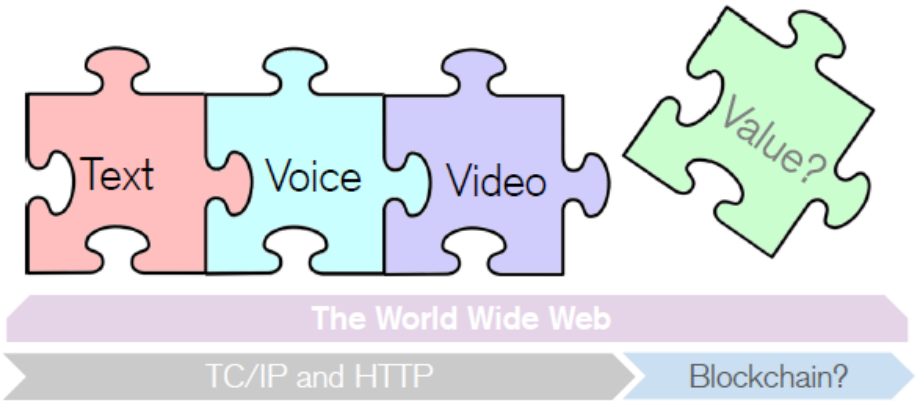


Source: Credit Suisse (2016).

Blockchain is often portrayed as the missing link of the internet (Figure 4). Voice, video, text and others are easily transferable over the internet, while the fourth part - value transfer - has traditionally been absent. Similar to hypertext transfer protocol (HTTP), which hyperlinks text nodes to each other and on top of which the internet – a distributed information exchange system – is built, blockchain is meant to serve as the application for a distributed value exchange system. Traditionally, asset exchange was possible only with a trusted third party overseeing the transactions. With the disintermediation of trust and displacement of third party intermediaries by participant consensus, reliable, auditable and safe asset exchange across internet suddenly becomes possible.

The value transfer was traditionally performed over classic centralized systems, where siloed and duplicated ledgers were required. A distributed database has many advantages over a centralized system, mainly with the possibility to provide greater transparency and with drastically reduced duplication and transaction costs.

Figure 4: The missing piece of the internet



Source: Credit Suisse (2016).

Current databases are complex and centralized systems with high operating costs. They require constant communication and data exchange with other centralized systems that can be either internal or external. Traditionally, a database consists of: 1) legacy database systems hosted on the servers of a single organization (i.e. having a single failure point), and 2) licensed or internally developed systems that respond to queries by communicating the requested information. On the other side, a distributed blockchain system offers an independent, interlocked and immutable record, which is tamper resistant, secure and verified/settled by a consensus. Blockchain systems provide vast options of potentially faster, cheaper and more secure information systems.

A list of benefits of a system built with blockchain is summed below:

– **Asset security.** Immutable and permanent of transaction data imparts confidence among in the promise of value exchange and enhances fraud detection.

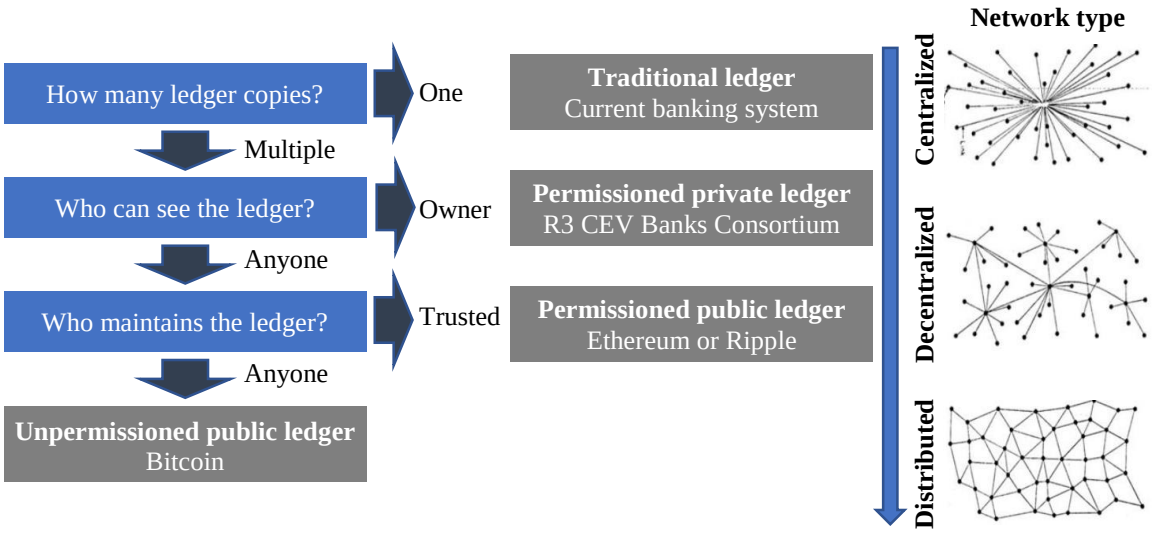
- **Quick to update.** Incentivization of system participants ensures reduction of processing and transaction times.
- **Trusted emissary.** Distribution of trust across the system eliminates or reduces third party risk, opposite to centralized and "single point of failure" systems.
- **Permanent uptime.** Blockchain's distribution features means that permanent irrefutable up-time is achievable.
- **Incorruptible.** Multiple copies of the ledger, which are shared and constantly updated across the network, ensure that there is a constant backup system for the entire ledger.
- **Borderless.** Decentralized, network-based blockchain systems can be virtually borderless (Goldman Sachs, 2016).

Blockchain's permissioning is determined by ledger levels, while different functionality can be achieved depending on the ledger layers covered and the choices made in how the levels are approached. They are explained below.

1.4.1.1 Ledger levels – understanding level permissioning

Figure 5 below depicts various ledger levels and network types. There are three ledger properties that are relevant and need to be outlined: the number of copies, reader access and write access. Traditional legacy systems have one and centralized copy of the ledger – if there is more than one copy, then the ledger is said to be shared. If anyone can view the ledger (ledger not permissioned) and participate in forming the consensus decision (ledger not private), then this is an unpermissioned public ledger.

Figure 5: Ledger levels and network types



Source: Credit Suisse (2016).

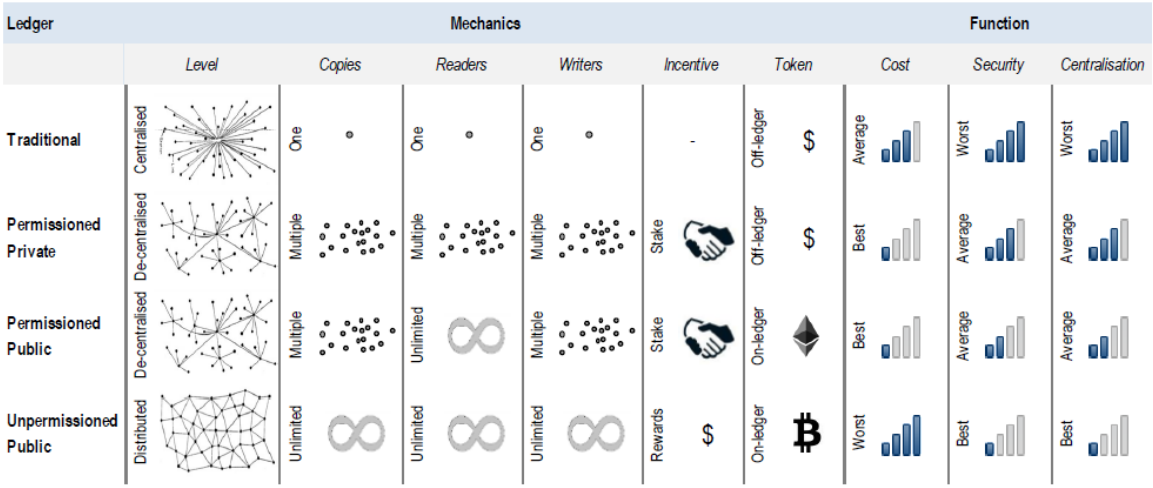
Bitcoin is a distributed network, while the traditional ledgers are of centralized nature. Between these extremes are decentralized permissioned Ledgers. This implies that those who participate in the consensus mechanism are a selected (permissioned) group, which creates multiple points of centralization. Private permissioned ledgers are those in which only the owner and selected system consensus participants can view the ledger. On the other side, a public permissioned ledger is a system, where only a selected group can maintain the ledger although anyone can see what is written on it.

Different types of ledgers have several fundamental differences. Notably, there is a trade-off between cost and security. As explained above, a distributed consensus mechanism can use network participant's computing power to maintain security; the cost of ensuring that is rather high. On the other side, a private ledger participants own a stake in the system and therefore their interest is to maintain safety, reliability and reputation of the network. This version is a cheaper source of the truth, but it lacks a totally distributed structure and purity of a secure "trustless integrity". Another fundamental difference is whether assets are on-chain (tokenized) representations of real-world value, on-chain tokens with intrinsic value or instead any type of data. Four ledger levels and their properties are:

- **Traditional ledger.** The ledger is centralized, has one source of truth, and has to be connected and reconciled with other ledgers to settle transactions. Owner, which has complete editorial power, forms the consensus mechanism and ensures that the record is immutable.
- **Permissioned private ledger.** Here, various entities are given write and read access on the ledger. Inceptives for overseeing the consensus-forming process are usually given off-chain. Usually, the participants tend to have a stake in the integrity of the ledger as well.
- **Permissioned public ledger.** Like above, only pre-selected permissioned entities or stakeholders may participate in the consensus mechanism, but anyone can view and transact upon the ledger. This system ensures that the transparency and accountability are much higher.
- **Unpermissioned public ledger.** On the far end, unpermissioned public ledger (or double permissionless ledger) is a public ledger, where anyone can participate in the consensus forming and can see what is written on the ledger. To ensure fairness, participation is incentivized by tokens, which are native to the ledger. A totally distributed structure ensures that there is a single source of truth and entirely trustless integrity. Bitcoin would serve as the best example here (Credit Suisse, 2016).

Different ledger levels and its functions/benefits are illustrated on the Figure 6.

Figure 6: Ledger levels, mechanics and different functions

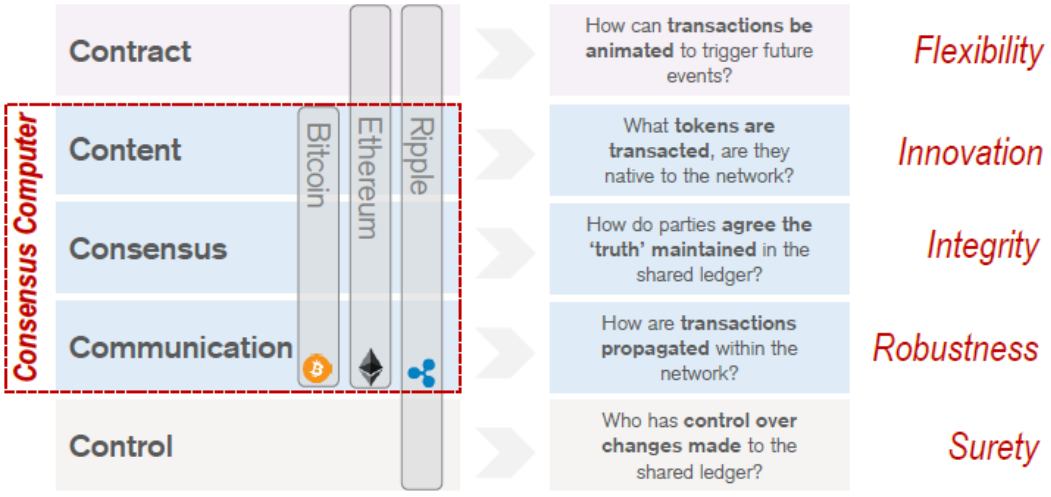


Source: Credit Suisse (2016).

1.4.1.2 Ledger layers – understanding ledger functionality

Depending on which ledger layers are embedded in the specified blockchain, different functionalities can be achieved (Figure 7).

Figure 7: Credit Suisse's adoption of Consult Hyperion's 4x4 SLT model



Source: Credit Suisse (2016).

The control layer determines permissioning of the chain and governs who has write access to it. Besides it, any consensus driven blockchain needs to have at least the following layers: Content, Communication and Consensus. Content and Communication layers denote the token scheme and token value (representative of extrinsic or intrinsic value, or simply representation of information), and the way transactions are propagated within the network. Bitcoin, for example, has only those layers. Any consensus driven blockchain can be

modified to achieve different objectives via different consensus mechanisms (Proof of work, Proof of stake, etc.) (Credit Suisse, 2016). They are explained below.

Furthermore, the contract layer can be used to add additional logic to the transactions. For example, it can be used to embed contractual logic, which automatically executes when certain terms are met. Possible use cases of blockchain in the contract layer:

- **Smart contracts.** Smart contracts enable embedding of contractual logic into blockchain. They operate similarly to the if-then function which executes automatically once certain conditions are satisfied. Once an obligation is put into a smart contract and embedded onto a blockchain, it has the benefits of autonomy, speed, security, verifiability and immutability. Potential use cases include anything from the simple administering of who wins or loses a bet, to settlement of derivative transactions or mortgage transactions, where repayments are denominated in an on-chain token of value (for example Bitcoin) (Capgemini Consulting, 2016b). More about smart contract can be found below.
- **Proof of existence.** Due to immutability and consensus properties of a shared ledger, data, when written on a blockchain, becomes notarized. The content level is therefore neither intrinsic nor extrinsic units of value, but instead information, which, when recorded on a chain, becomes time-stamped and notarized. Potential use cases here are pretty obvious – it can be used as a method of authentication or certification of documents (Capgemini Consulting, 2016b).

1.4.1.3 Difficulties blockchain is facing

Despite the recent buzz surrounding blockchain's disruptive potential, one has to keep foot on the ground and realize that there are several hurdles accompanying the technology and its use. Some of the key challenges to widespread implementation of blockchain-based systems and solutions are:

- **Security versus cost trade-off**

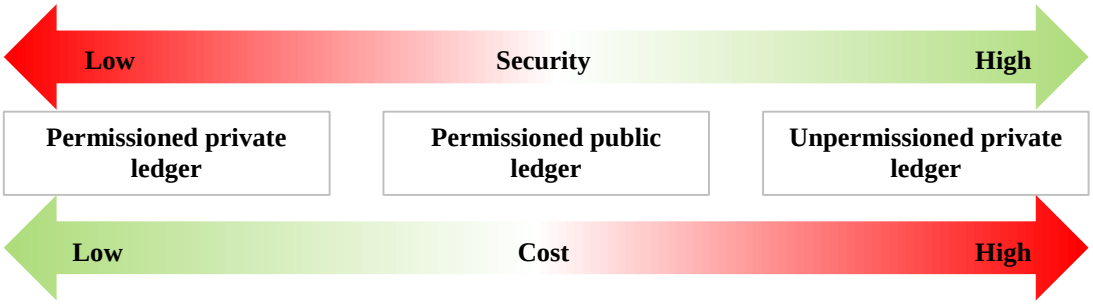
The purest form of a blockchain can be understood as an unpermissioned public blockchain - like the one that underlies the Bitcoin. Full network decentralization and permisionless participation means authority is fully devolved; it is in theory infeasibly costly for one entity to gain even part of control. Such trustless system resembles high security, yet it comes at a price which is not so far away from the transaction costs we see in the traditional systems.

On the other side, consensus mechanism in the permissioned ledgers can be much cheaper as it doesn't require that entities engage in resource intensive systems (i.e. proof of work) to prove their trustworthiness. Instead, only pre-selected participants are permissioned to be involved in the consensus forming mechanism and are granted the right to edit the chain. However, this comes with a caveat. As we give more authority to selected participants, we

lose distribution which ensures high levels of ledger integrity. Therefore, the main question one should ask is – **who determines which participants should be granted access?**

As seen on the Figure 8, high security of a distributed and unpermissioned public ledger leads to the high costs of maintenance. A low cost permissioned private ledger solution on

Figure 8: Cost versus security trade-off of different blockchain types



Source: Credit Suisse (2016).

the other side lacks the benefits of security and distribution. In conclusion, there always exists a cost versus security trade-off of blockchain types - we have to bear this in mind when thinking about a proper and sufficient infrastructure (Credit Suisse, 2016).

– **Is blockchain really needed?**

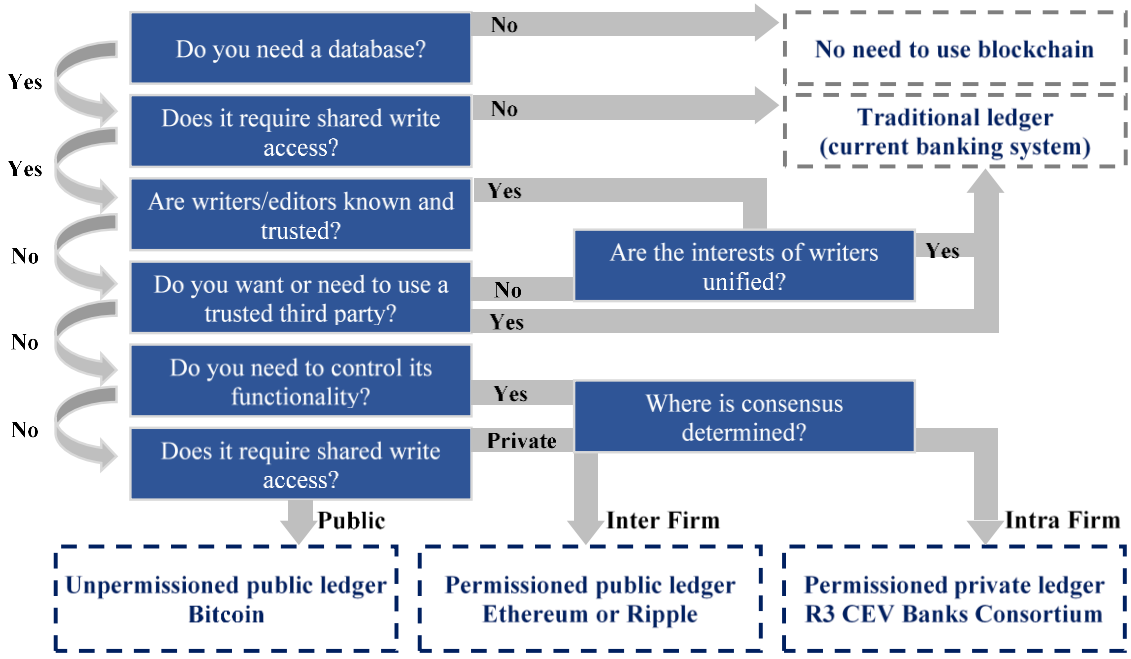
For a blockchain to be relevant and applicable, one has to require a database, need shared write access, have unknown writers who have unified interests, and not trust a third party to maintain the data integrity. This implies that blockchains are not always necessary and that a regular SQL database could be more appropriate in certain use cases (Figure 9) (Credit Suisse, 2016).

– **Critical mass is essential**

As designed, blockchain based systems rely upon multiple users – primarily at the authoring level. Metcalfe's law, which is most often used to portray the value of the network (i.e. the value of the network is proportional to the square of the number of connected users on the system - n^2), can be used to estimate the value of the bitcoin network. Industry leaders believe that this carries to other blockchain systems as well and that the widespread adoption is required to truly harness the network effect of blockchain. A single cell or entity is analogous to a centralized legacy database and only a network of connected entities gives certain value.

Before a critical mass is achieved, certain threats need to be mitigated: i) platforms' fragmentation, ii) institutional and social apathy to transition to and/or agree on a platform.

Figure 9: Do you really need a blockchain?



Source: Credit Suisse (2016).

– **More entry points mean there are more possible points of attack**

Most secure databases in the world are set up in distant and air-gapped locations. The system is usually physical disconnected from the internet and is therefore highly resistant to any kind of cyber-attack. To achieve this in the blockchain system, each entity or node could potentially be air-gapped as well. As the system relies upon connectivity, it is highly unlikely to get that. Even more concerning is the fact that if an individual or a group of individuals would gain restricted access to the blockchain system, the steal of the database would be equivalent to a breach of every connected bank's database in the world simultaneously.

– **Blockchain transactions are often public**

Although identities of participants' transactions on Bitcoin's blockchain are unknown, transactional data is not. The key problem here is that in an unpermissioned ledger transaction data needs to be visible should the nodes be able to validate them.

Opposite, in a permissioned ledger, transaction data doesn't need to be visible. This anonymity and privacy hurdles may be a barrier to adoption of certain public chains.

– **Private key management issues**

To access edit permission for a blockchain, one should possess a private key. Once this is lost, it is impossible to gain access to the on-chain tokens and value that is associated with it.

– **Crap in, crap out**

Information on the blockchain isn't necessarily the "single source of truth". In fact, information stored on ledger is only good as barriers used to i) ensure that the data quality added is sufficient, ii) quality of node permissioning is high.

– **Blockchain forks**

Another feature that blockchain has are so called forks. Blocks can be sometimes created concurrently, which results in a temporary fork – meaning that additional blocks are created outside of the original chain of blocks. To maintain a single source of truth with blockchain, common rules among network participants have to be used. Forks where a certain set of rules governing that particular blockchain are changed, have been used to add new features to a blockchain or to reverse the effects of bugs or hacking (Coindesk, 2017). Bitcoin Cash, one of the cryptocurrencies with the highest market cap, is essentially a fork of the original Bitcoin's code – to improve latency and transaction speed, several features have been added to the code and thus another (and separate) Bitcoin Cash blockchain was made.

1.5 Consensus mechanisms and transactions validation

To ensure successful transaction validations, immutability of record and to prevent constant forking, blockchains utilize special algorithms for scoring different versions of its history and picking the one with the highest value. In this case, the blocks not selected and included into the main blockchain are called "orphan" blocks (Lee Kuo Chuen, 2015).

Like explained above, computers in the network supporting the blockchain are known as nodes or miners. They usually do not possess the same version of the blockchain's history at all times and are programmed to hold the highest scoring version of the database and whenever a peer receives a version scoring higher (an old version of blockchain with a new block added) they refresh their own database and the message changes to the peers in the network. Peers are incentivized to work only on extending the blockchain with new blocks (rather than changing old ones) and the probability of an entry becoming superseded decreases exponentially as more blocks are added on top of it, eventually almost diminishing (Nakamoto, 2008). Public ledger of past transactions, or a blockchain, is updated by a process called "mining", which is done by network nodes. This process is designed to be resource-intensive and allows nodes to reach a secure and tamper-resistant consensus. To ensure immutability and validity of blockchain, various proofing methods are used: proof of work, proof of stake, delegated proof of stake and proof of burn, zero knowledge proof, etc.

When adding a new block to the blockchain, a transaction has to satisfy one of the proofing method of its protocol and thus needs to be verified and confirmed by nodes in the network. Alongside verifying transactions, mining is a mechanism by which new units of currency are added into circulation. To compensate for resource intensive work, which ensures

security of the system, new coins are added to the network and miners get to keep a portion of both transaction fees and newly created coins (Bitcoin Wiki, 2017a).

Nodes act as verifiers for the network. Permissionless blockchains allow everyone to join as a verifier, while preselection or preauthorization from a consortium or a centralized authority is required in a permissioned blockchain. Data integrity, data security and distributed consensus are achieved by the following proofing methods.

1.5.1.1 Proof of work

The main innovation introduced by Satoshi Nakamoto was the so-called proof of work method (PoW), which creates distributed trustless consensus and solves the double-spend problem. A proof of work is a piece of data that is difficult (costly and time consuming) to produce, but easy for others to verify and which satisfies certain requirements. There is a lot of trial and error on average before a valid piece of data or proof of work is made. In other words, PoW can be a random process with low probability.

Or put like this: one party (usually the prover) presents the result of a calculation that is hard to calculate, but easy to verify. Other parties in the network can be sure that the first party (prover) performed a certain amount of computational work to generate the result. In essence, proof of work serves as a defense against attackers overpowering the (Bitcoin) network and introducing alternative blockchains that overwrite previous transactions (Bitcoin Wiki, n.d.)

The main problem of PoW method is that its calculations are mostly useless – they are solving random "calculations" and therefore not contributing a lot to society other than wasting huge amounts of electrical energy (Buterin, 2013).

1.5.1.2 Proof of stake

This is an alternative to the PoW method mentioned above. Instead of requiring the prover to perform a certain amount of computing, a proof of stake (PoS) system requires that the prover shows ownership of a certain amount of a currency – meaning the more currency you own, higher is your mining power when mining it. This method then forces miners to have a stake in the network and will defer people from using their mining power (Buterin, 2013).

Opposite to PoW, no coin creation (or mining) exists in this protocol. Instead, all coins exist from the day one and validators (i.e. stakeholders) are paid solely in transaction fees. PoS mechanism is more energy efficient than a proof of work based system. Debates over successful distributed consensus were wild and gained lots of media attention as some authors argue that this is not an ideal method, yet only slightly better than PoW.

1.5.1.3 Delegated proof of stake

Some argue that the delegated proof-of-stake (DPoS) is the fastest, most efficient, most flexible and most decentralized consensus model currently available. Unlike in PoS, where the ability to earn rewards when processing transactions rests with coinholders (i.e. those with the actual stake of coins), the DPOS offers the feature where coinholders vote and decide on delegates who are responsible for validating transactions and with that earn transaction fees. To allow for fast transaction confirmation, DPOS leverages the power of stakeholder approval voting and can resolve consensus issues in a fair and democratic way (BitShares, n.d./a).

Other proofing methods include proof-of-burn and zero-knowledge proof. I will not try to describe them here as they have lots of different characteristics from the ones mentioned above. Cryptography, technology and industry experts are constantly working on and trying to develop a method that would provide us with the most efficient and secure consensus mechanism.

2 PUTTING BLOCKCHAIN TO WORK

Here I show where blockchain can be used in the modern financial infrastructure. I explore different applications of the technology in the traditional infrastructure of capital markets and describe ways to re-engineer, rationalize and increase efficiency of legacy systems in different segments of finance: blockchain based currencies, clearing and settlement, payments, fundraising, smart contracts and investment management.

2.1 How and where will blockchain impact?

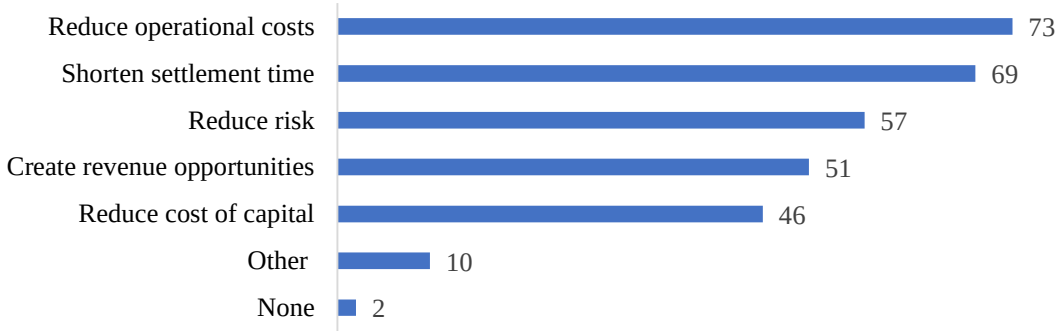
From a “missing piece of the internet” to “the worst speculative bubble of modern history”, blockchain is fueling imagination of technology evangelists and various experts, both seeing significant opportunities for implementation across a range of industries.

As an innovative technology, there are three ways to consider the potential impact of blockchain:

- **Growth:** Where unimagined potential arises in the fields of various applications, implications and revenue opportunities – all from applications built with the help of blockchain and its different implementations.
- **Opportunities:** Discover areas where blockchain offers the opportunity to re-engineer, rationalize and increase the efficiency of legacy systems and technology through cost removal, increase of efficiency and potential new revenue streams.
- **Traps:** Blockchain could render obsolete current services of legacy players or encourage vertical integration, thus disintermediating incumbents (Goldman Sachs, 2016).

Several surveys that give us an indication of where industry experts expect the biggest change were made recently. A survey by Greenwich Associates in 2016 (Figure 10) indicates that industries involved in the business of selling trust and industries currently experiencing great complexity and costs will be impacted the most.

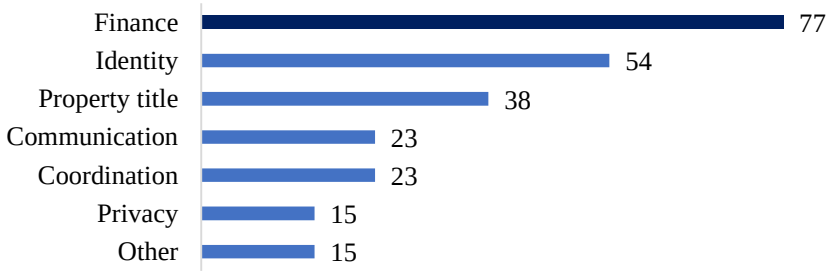
Figure 10: Blockchain technology's main benefits – (%) of survey respondents



Source: Greenwich Associates (2016).

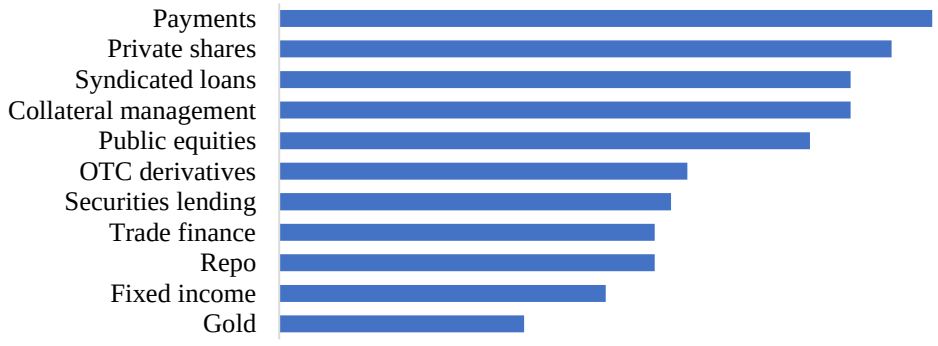
A consensus belief is that Financial Services and within them Payments and Capital markets will bear most change (Figure 11 and Figure 12).

Figure 11: Which areas do you think blockchain will have the greatest impact in? (%)



Source: Greenwich Associates (2016).

Figure 12: Most promising use cases to deliver change in Financial Services



Source: Greenwich Associates (2016).

Following sections contain analysis of legacy infrastructure and give us an overview of possible solutions where friction could be mitigated. Additionally, sections provide us with an overview of innovative solutions that bring new ways of sharing trust, ownership of assets and possible ways of raising capital.

2.2 Currency – is blockchain money going to replace fiat money in the future?

Let's first start with asking ourselves how old money is. In fact, we don't know the exact answer to it. But we know that when we look at the archaeological discoveries of writings, we find some of the first writings about money in the forms of ledgers. The majority of the ancient writing was about money and ledgers – in whatever "currency" existed then. We also know that people have used stones, shells, wheels, feathers or livestock for the means of exchange. People have traded three chickens for one pig or sold a precious stone to get a nice horse. Exchange of goods and services has been done throughout human history, using wide variety of mediums of exchange – implying that the money is as old as civilization.

We should look at the nature of money as a form of communication. At its core, money is not something of value. Rather it represents an abstraction of value - it is a way of communicating value. We use money every day to communicate value to each other and it shows us how much we value a certain product or service. The concept of money is deeply ingrained in our society and is an important social construct, yet it is one of the technologies that is least studied, both from historical and technology perspective. When Satoshi published his Bitcoin whitepaper, he wanted to create a totally new form of money - totally digital and borderless.

Our society first started with the abstract forms of money - such as livestock. As time progressed, we started to use precious metals as they possessed some of the most important characteristics of money: scarcity, divisibility and transportability. Although revolutionary, this was still not the best means of exchange.

Long time after came the first piece of paper that represented a certain amount of value. Gold was deposited at a trustworthy person or institution and a piece of paper representing the value of gold was issued. This piece of paper was much more convenient and was easier to transport. However, this means of exchange invention was controversial for lots of people, prolonging widespread use as masses needed several centuries to adapt their beliefs. Plastic cards, mobile money and different internet payment mechanisms represent another big transformation in the means of exchange and were similarly heavily criticized at the beginning.

Among rich literature in definitions of money, Kiyotaki and Wright developed a widely cited economic model where money endogenously emerged as a medium exchange. The definition describes money as a medium which exists to facilitate trade and to make barter

exchange more efficient. Further on they described money and the difference between a commodity and fiat money as:

"When a commodity is accepted in trade not to be consumed or used in production but to be used to facilitate further trade, it becomes a medium of exchange and is called commodity money. If an object with no intrinsic value becomes a medium of exchange, it is called fiat money." (Kiyotaki & Wright, 1989)

Definitions mostly portray money on what it does and not what it is, which implies that anything can be money and used as a medium of exchange, as long as it is used and exchanged in a certain way. Money can be any item or a verifiable record that is accepted as payment for goods and services in a particular socio-economic context or in a particular country. Money's main functions are the following: **a medium of exchange**, **a unit of account**, **a store of value** and occasionally, **a standard of deferred payment**.

Medium of exchange is something that is accepted in exchange only for the purpose that it can be later traded for other services and goods. A medium of exchange is something that is transportable, durable, divisible, easily recognizable and is inevitably a store of value, yet vice versa is not always true (Ostroy & Starr, 1988).

Means of payment, which is different from a medium of exchange, is a widely used and accepted method for the delivery of money. Main difference here is that a medium of exchange is an asset of value, while a means of payment is not. Yang (2007) defines cash or banknotes as the only asset which can be both a medium of exchange and a means of payment, while cheques are only the latter.

Unit of account is defined as a metric for value and is used in bookkeeping. Doepke and Schneider (201) interpret it as the good in which the value of future payments is specified. Money as a unit of account implies a certain ratio at which goods can be exchanged. Prices can be quoted in various units, yet only one of them is the unit of account for a producer which has to pay for inputs such as salaries or material and pay out dividends and taxes.

Standard of deferred payment function is distinguished by Greco (2001), while Abel and Bernanke (2005) list this under other functions of money. It is a generally accepted way to settle debt in a unit in which debts are denominated. The real value of debts may change when denominated in money due to inflation and deflation.

Store of value function implies that the money must be able to be reliably saved, stored, and retrieved. Value of the money must remain stable over time and must be predictably usable as a medium of exchange when retrieved. Mankiw (2007) argues that inflation diminishes the ability of the money to function as a store of value.

Using money as a medium of exchange insures efficiency and reduces the number of transactions needed to ensure optimal allocation of resources between participants. It reduces

the information and transaction costs in exchange, thereby making transactions of goods and services cost-effective.

In contrast to historical systems where commodity money was used, most modern monetary systems are based on fiat money. The main purpose of central banks around the world is to maintain a sustainable rate of economic activity, where a policy is set to target a certain rate of inflation or deflation per year. Price stability intends to avoid both prolonged inflation and deflation, thus improving the transparency of price mechanism. Under successful price stability policy people can recognise changes in relative prices (i.e. prices between different goods and services), without fear of changes in the overall price level. This allows them to make educated consumption and investment decisions, thereby allocating resources efficiently (Bank of Finland, 2018).

Nowadays very few people actually use cryptocurrencies for day-to-day transactions. Volatile nature, slow transactions, and technological barriers toughen use of cryptocurrencies for daily purchase of general goods and services. A 10% or more daily change in value of a cryptocurrency is not uncommon at all. Should cryptocurrencies become a widely used medium of exchange that is not subject to extreme price risk, volatility and price stability issues need to be answered. Different solutions have already been proposed and can be seen below.

Liquidity is the degree to which an asset or any good can be easily and at a low cost exchanged into other goods or services. Keynes (1936) uses liquidity as an equivalent for money, while Ostroy and Starr use this definition:

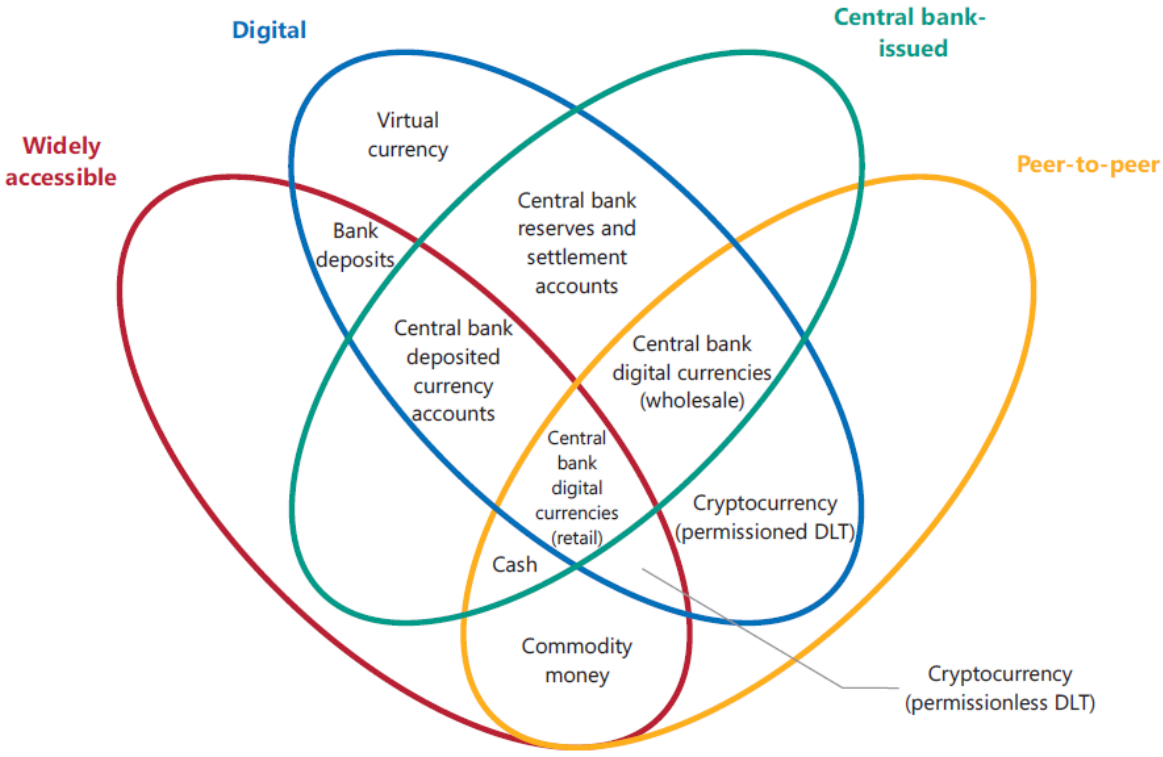
"What distinguishes money from other stores of value is its liquidity, and what underlies the liquidity of money is the fact that it is the common medium through which other commodities are exchanged." (Ostroy & Starr, 1988)

Among a world of assets, money is the most liquid as it gives consumers or market participants the freedom to easily trade goods and services. Likewise, spread between the prices to buy and sell should be minimal (or zero) when buying items with money.

Cryptocurrencies have been widely studied recently. They allow for trustless peer-to-peer transfer of electronic value between contracting parties. Historically, only cash and commodity money allowed for peer-to-peer exchange, while different electronic representations of money (i.e. bank deposits) are exchanged using a trusted third party centralized intermediary. Bech and Garratt (2017) developed following diagram which puts cryptocurrencies into universe of different forms of money which is further separated per different properties: *issuer* (central bank or other); *form* (electronic or physical); *accessibility* (universal or limited); and *transfer mechanism* (centralized or decentralized, i.e. peer-to-peer).

As seen in the Figure 13, electronic blockchain based money is transferable in a decentralized peer-to-peer manner. It can be issued privately (Bitcoin for example) or by a central bank. Accessibility further distinguishes between two forms of central bank cryptocurrencies (CBCCs) - a generally available retail CBCC and a wholesale CBCC, which is available only to financial institutions. Several possible implementations of both privately and central bank issued cryptocurrencies exist. Developing technology, different supply mechanisms and volatile nature of cryptocurrencies have led to emergence of innovative solutions which aim to provide with a widely used medium of exchange that can allow for successful monetary policy targeting and can ensure price stability. Two versions of a stable blockchain based currency have therefore been proposed. One is a fixed supply currency such as Bitcoin and the other are so called stablecoins. Both of them are privately issued. For the currencies issued by the central bank, there are three possible implementations of blockchain technology into a central bank controlled crypto money: a central bank cryptocurrency peg, a retail facing generally available (i.e. Fedcoin) and wholesale (i.e. CADcoin) central bank issued cryptocurrency. Different versions have distinct characteristics and are explained below.

Figure 13: The money flower and different types of blockchain money



Source: Bank for International Settlements (2018).

2.2.1 Privately issued cryptocurrencies

Privately issued cryptocurrencies offer a truly disruptive way of value exchange. While nations currently have a monopoly on the issuance of money, privately issued cryptocurrencies that are governed by a distributed consensus could pose significant market competition to the ones issued by governments. Different versions exist and are explained below.

2.2.1.1 Bitcoin, a highly volatile medium of exchange

From its birth in 2008, Bitcoin has gone from a "nerds-money" to one of the assets that gained most of the media attention. Forward looking technology evangelists see Bitcoin as a radical transformation of money and value exchange, where transactions are borderless, immutable and only need to obey the rule of the network that is not controlled by any centralized entity. The integrity and validity of transactions or data is exchanged in a peer-to-peer manner among billions of participants **without going through a trusted third party** and thus delivers a unique value proposition to addressing a long-standing problem digital cash was facing: how to ensure that users cannot costlessly duplicate tokens and spend them countless times – **a double-spending problem**. For example, such problem could be mitigated by a third-party intermediary, say Visa or MasterCard, which would monitor and confirm transactions. Instead, Nakamoto came up with a disruptive approach which uses cryptography to ensure validity of transactions and where the storage and maintenance of the historical record of transactions – blockchain – is outsourced to a distributed network of competing nodes. In order to protect this record from tampering, nodes facilitate in a costly process of mining. Resource intensive work ensures that the record is updated with new transactions, providing winning miners with newly minted tokens.

Bitcoin's unpermissioned public ledger system allows for:

- **Transparent and neutral system with total payment freedom.** All information concerning Bitcoin's supply characteristics is written online and is publicly known. No individual, organization or central bank can manipulate the protocol since it is cryptographically secured and highly censorship resistant.
- **Great security and control.** Bitcoin users are in full control of their transactions - no merchant can force unwanted or unnoticed charges. Bitcoin's payments contain no personal information and therefore offers strong protection against identity theft.
- **Choosing your own fee.** There is no fee when receiving Bitcoin. When sending it, one can control how large fee to pay (Bitcoin Wiki, 2017b).

A small segment of world's population has adopted Bitcoin over the last years as a medium of exchange and potentially a store of value. Bitcoin, having 21 million outstanding units, has seen its price rise from as little as few cents (in 2010) to its high of $19,329 in December 2017, and plummeting to $5,895 on 29 June 2018. Current outstanding supply of 17,147,325

units gives it a market capitalization of $107 billion as of 13 July 2018 (CoinMarketCap, n.d.). A typical bitcoin user in Europe is a male aged 25–44 and might be more comfortable with that volatility level, while most people need assurance that the purchasing power of a financial instrument will stay relatively stable before they start adopting it as money (ING, 2018). Bitcoin's volatility continues to surpass that of major financial assets such as gold, the US dollar index and the S&P 500 (BuyBitcoinWorldwide, n.d.).

Competing with various forms of digital cash, especially widely used mobile money (i.e. a digital currency denominated and backed by a given country's unit of account that is issued by telecoms and/or banks and is transferrable by a mobile phone), and volatility complicating its ability to replicate the properties of banknotes in digital form is lessening cryptocurrency's probability of ever gaining widespread acceptance. Network effect enjoyed by legacy exchange media such as US dollar are further challenging Bitcoin's use. An effect known as lock-in effect, sometimes referred as hysteresis, has been widely studied. Once a standard unit of account and medium of exchange are adopted in a certain socio-economic context, any single participant willing to divert from that standard faces risk of having its transaction costs rise as no one in that community uses that unit of account nor states prices with it. Incumbent currencies worldwide are therefore retaining strong foothold against various challengers. Studies show that once a country has been dollarized or partially dollarized, it is very unlikely to de-dollarize even if the domestic currency has long since stabilized (Oomes, 2003).

With the evolution of the infrastructure and ecosystem, Bitcoin's (or that of any other similar cryptocurrency) extreme volatility should iron out. Common thought in the industry is that as new financial infrastructure and financial instruments (i.e. derivatives) evolve, and with increased Bitcoin's usage as a medium of exchange (i.e. making Bitcoin's order book thicker, increasing market liquidity which should therefore lead to decrease in asset's volatility), the speculative investments should decrease and flatten out volatility, hence making Bitcoin more competitive.

Since 2008 Bitcoin's volatility has been falling down, with some exceptions of few periods where the hype around blockchain shot into the sky. Often as volatile as a penny stock and low trading volume continue to dampen Bitcoin's prospects for wide spread consumer adoption. Bolt and van Oordt (2016) predict that Bitcoin's fixed supply means (i.e. 21 million coins) that its volatility must get in the same range of fixed supply commodities like oil or gold.[1] Fixed supply further limits a supply-side feedback loop, which is a critical component when reducing volatility of an asset. All other things being equal, inelasticity of Bitcoin makes it more volatile than gold and silver.

[1] Bolt and van Oordt (2016) among others see Bitcoin's volatility as a sign of early development. With further technology development and widespread acceptance volatility should drop, although fixed supply implies that its volatility will be similar to that of other commodities rather than traditional currencies. Also, the exchange rate will become less sensitive to speculative positions.

Bitcoin's network currently has a highly limited number of transaction that it can process per second. Unlike Visa, which can process up to 24,000, Bitcoin can handle only up to 7 transactions per second. To address this problem, various proposed and already functioning solutions like Lightning Network were issued (Poon & Dryja, 2016).

All in all, should Bitcoin gain wide spread acceptance as a medium of exchange and see its use as a pseudonymous cross-border payment rail, its transaction output has to scale significantly and its price must become less volatile.

2.2.1.2 Stablecoins

To get closer to stable blockchain money, "price stable cryptocurrencies" have been proposed. Typically, most stablecoins tend to be pegged against the US dollar, while some implementations are linked to a basket of currencies or an index such as the Consumer Price Index (CPI), similar to how central banks hit inflation targets today. Furthermore, a stablecoin can be backed by a collateral that corresponds with the market cap of outstanding coins. The collateral can be fiat currency, a cryptocurrency, gold or any other arbitrary asset. As it is backed by corresponding reserve, price of a stablecoin should remain constant – at least in theory.

A common thought in the industry is that stablecoins' main utility is to cost efficiently solve transfer of value between assets moving from traditional financial markets into the crypto market – thus distorting the lines between the blockchain and traditional value systems, of which the latter is based on physical assets such as fiat money or the US dollar.

As per the type of collateral, there are three models of stablecoins so far:

- **Fiat backed stablecoin.** Tether, for example, is one of the several stablecoin projects. Maintaining a reserve of US dollars in a bank account and issuing fully backed cryptocurrency units (i.e. Tethers, or USDT), Tether has demonstrated that it is possible to succeed as a stable and fully pegged cryptocurrency (i.e. 1 USDT = $1). However, in order to maintain the peg, collateralized stablecoin users need to trust a centralized issuing body to hold sufficient reserves (Tether, 2016).
- **Crypto collateralized stablecoins.** An alternative to a centrally (fiat backed) orientated cryptocurrency is a protocol, which keeps reserves on a distributed blockchain. An example of that is BitUSD, whose network of users ensures that a sufficient quantity of bitShares (i.e. a cryptocurrency type of collateral) is held on-chain for each bitUSD outstanding. If bitUSD's value falls below $1, say 97 cents, then bitShares are used to repurchase bitUSD until the price of the latter has returned to par. Peg of bitUSD to dollar has remained in place since 2014 (BitShares, n.d./b).
- **Non collateralized algorithmically controlled stablecoins.** Non collateralized stablecoins are price stable cryptocurrencies not backed by any collateral. In fact, most current applications make use of an algorithm or a system that automatically expands

and contracts supply based on the price of the coin. Supply-demand function is most often following the Quantity Theory of Money (QTM)[2], which states that there is a direct relationship between the quantity of money in an economy and the level of prices of goods and services sold. QTM states that should the amount of money in an economy double, the inflation levels also double. An example of such decollateralized stablecoin is Basecoin, whose value is again pegged to $1. If required, underlying protocol automatically adjusts the outstanding supply of Basecoin tokens (i.e. increasing supply when price of the token is above $1 or decreasing supply when price is below $1), keeping price of the token constant. This stablecoin operates as a fully decentralized, protocol-enforced algorithm that implements so called algorithmic central bank monetary policy. Price-stable cryptocurrencies offer broad specter of possible use cases. People in developed countries take stable currency for granted, while for others living in third world countries that have weak institutions, unstable currencies and where high inflation and currency devaluations are not uncommon, a price-stable cryptocurrency offers to solve high arching issues of that nation. Historically, in case of a rapidly devaluing local currency, such countries have adopted US dollar. Nowadays instead, Blockchain based money and stable cryptocurrencies in particular could see growing demand in those regions - The Managing Director of the IMF, Christine LaGarde, called this as a "Dollarization 2.0" (Al-Naji, Chen & Diao, 2017).

2.2.2 Central bank cryptocurrencies

Technology enables different versions of blockchain based money that is transferable in a decentralized peer-to-peer manner. Central banks have the opportunity to create different versions of blockchain based mediums of exchange that can bring more transparency and efficiency in the current system.

2.2.2.1 A central bank cryptocurrency peg

A solution where a central bank pegs the price of an existing cryptocurrency, say Bitcoin, to the value of its local currency. Venezuela has similarly pegged its currency to cryptocurrency "Petrodollar" (Bloomberg, 2018). The European Central Bank would for example peg the value of Euro to Bitcoin and offer to buy and sell unlimited amounts of Bitcoin at a pegged rate – 1,000 EUR per 1 Bitcoin.

However, one caveat exists here. As described in the Nobel Laureate Robert Mundell's (1999) work, a central bank would face the impossible trinity problem – both an inflation target and the price of Bitcoin cannot be targeted at the same time. Should the economy miss

[2] Originally formulated by Irving Fisher and Milton Friedman.

its inflation target (i.e. 1-3 % a year), then the ECB would have to give up on its Bitcoin peg. If the ECB decides to keep the Bitcoin peg, then it will have to give up on its inflation targets.

A Bitcoin standard economy would behave similarly as a gold standard economy, where its price levels would become hostage to the supply and demand for Bitcoin. A central bank peg can also be attacked as seen in the case of Soros' attack on the British pound.[3] Should the market doubt the exchange rate, speculative pressure will build, thus forcing central bank to give up on the peg (Koning, 2016).

2.2.2.2 Retail central bank cryptocurrency (Fedcoin example)

A retail central bank issued cryptocurrency (Fedcoin for example) would, opposite to Bitcoin, rather have a dynamic supply of coins. Fedcoin type of cryptocurrency is intended as a substitute for cash and should build its value offering on privacy attributes of cash. Bitcoin has its supply ceiling at 21 million units. New tokens can be created only in a predetermined algorithmic fashion – as a reward to miners for verifying Bitcoin network transactions. Finite supply where the quantity of Bitcoins outstanding is progressing towards a cap of 21 million units is limiting the flexibility of modern monetary policy. In order to insure central bank's successful target following, a monetary policy-friendly cryptocurrency has to be created. Koning proposed Fedcoin, a cryptocurrency which has flexible supply characteristics where there is no floor or ceiling to the quantity of coins issued.

A Fedcoin would function as follows. The central bank of the reference country would determine the exchange rate between Fedcoin and banknotes of the existing currency in circulation. For example, in the United States, it could be converted in both ways and at par with the US dollar (i.e. $1 could buy 1 Fedcoin). Outstanding supply of coins would be managed by the FED. Opposite to Bitcoin's predetermined supply rule, Fedcoin's supply would increase or decrease depending on the customers' desire to hold it – similar to today's supply of cash. Should the public desire to hold more of Fedcoin, they must turn over US dollar banknotes for new Fedcoin of the same nominally quantity (i.e. 100 dollar bill for 100 Fedcoins). To protect from duplication, returned banknotes would be cancelled by the central bank.

A central bank would therefore act as a permissioned entity which has total control over issuance of its cryptocurrency. This function would work similarly to how central banks currently provide cash – should commercial banks and customers demand higher amount of coins in circulation, the central bank could proceed and print this cash on demand. Opposite, a central bank would redeem unwanted tokens (and destroy surplus tokens) and replace them with ordinary banknotes – similar to how it destroys old currency today. Unlike Bitcoin, Fedcoin wouldn't represent competing private money, but would be considered as a new

[3] George Soros, a famous speculator, bet heavily against the British pound in 1992, forcing the Bank of England to devalue the currency.

form of sovereign currency. This would make a stable cryptocurrency like Fedcoin a third component of the monetary base, alongside existing cash and reserves. Central bank's ability to follow price stability via processes of monetary policy would therefore be uncompromised.

Another thing worth mentioning here is that since FED would act as a gateway in and out of Fedcoin, it would have to know the public address of Fedcoin recipents. While exchange of cash can be done anonymously, conversion of bank deposits to obtain Fedcoin would provide central bank with the public address of the recipient. Although this can be mitigated by a third-party intermediary (which would accept and sell Fedcoin on behalf of the respective owner), AML and CTF requirements could limit Fed's willingness to allow for uncontrolled exchange (Koning, 2016).

2.2.2.3 Wholesale central bank cryptocurrency (CAD example)

CADcoin's concept has been part of the research initiative performed by Payments Canada, the Bank of Canada, R3 blockchain innovation consortium and a number of Canadian financial institutions. The main aim of the project was to better understand how blockchain technology could transform the future of payments in Canada. Launched in March 2016, it provides the platform for wholesale[4] payments settlement. Unlike Fedcoin, which is intended as a retail payment solution, CADcoin is not a consumer facing medium of exchange and does not trade on a public network.

To perform transactions amongst platform members, a participant bank has to pledge cash collateral into a special pooled account held by the central bank, which then converts that value into CADcoin equivalents and delivers it to the participant's account. The members of the network, who have to be preapproved, exchange the CADcoin, and when one wants to convert to another currency, it simply redeems the CADcoins for cash collateral. Converted CADcoins are then destroyed by the central bank.

As such, this is a proposal of a permissioned blockchain network infrastructure, where all network participants are trusted and authorized to perform transactions. Before the exchange each of the network participants (i.e. financial institutions) has to set up a digital currency account as part of a CADcoin asset registry, which is owned by the central banks, while the digital funds belong to the member bank. Opposite to the Fedcoin, the central bank issues depository receipts and not tokens of value. While still not fully functional, CADcoin is an interesting proposal whose shared ledger reflects accurate real-time account balances for each digital currency account of network members (Garrat, 2016).

Whatever the future developments bring, blockchain has already proved that it can provide our society with innovative forms of money. Central banks around the world are

[4] Wholesale term is synonymous with the terms "interbank" and "high-value".

continuously researching this area and might come up with a solution that makes blockchain based mediums of exchange widely used and thus bring more transparency and efficiency in the system. Opposite to centralized central bank issued money, privately issued cryptocurrencies offer a truly disruptive way of value exchange. Their borderless, trustless, consensus driven and immutability properties are giving our society, especially the unbanked world, an innovative solution to securely and cost efficiently transfer value all around the world – requiring almost no other infrastructure than a mobile phone and internet access.

2.3 Clearing and settlement

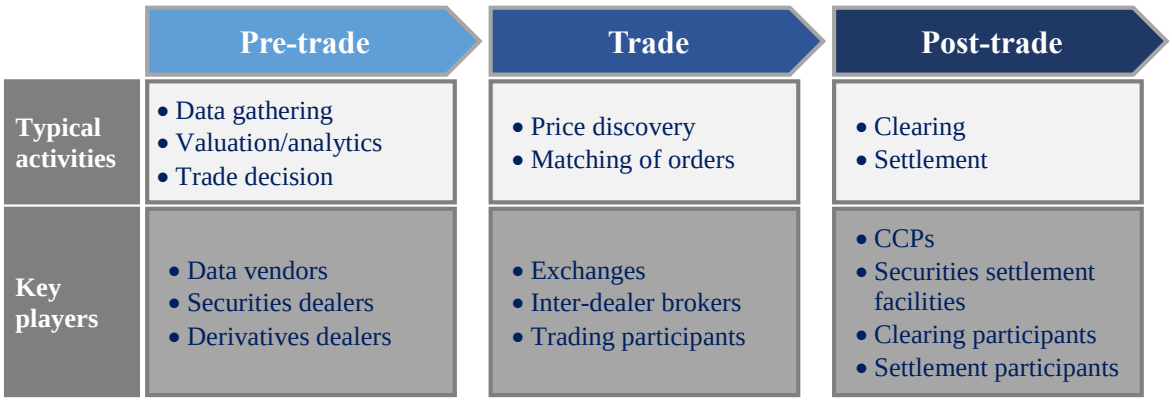
Clearing and settlement services enable smooth functioning of capital markets by lowering transaction costs of an investor when completing a trade (Giddy, Saunders & Walter, 1996). In finance, clearing represents all activities from the time a trade or a commitment for transaction is made until it is settled. Settlement represents the process whereby securities are delivered from the seller to the buyer, and simultaneous money transfer from the buyer to the seller. Clearing and settlement institutions are making sure that transactions are facilitated safely and efficient.

There are currently four types of institutions that provide clearing and settlement services:

- **Domestic central securities depositories (CSDs).** CSD's perform domestic securities settling. Countries mainly have one domestic CSD that is heavily regulated by the government. A CSD is traditionally associated with the national stock exchange. The institution holds the securities in electronic form, which is also known as a book-entry form (i.e. shares or stock certificates are digitized and ownership tracking is enabled by book entry whereby no physical certificate is given to investors), or in dematerialized or paper format such as a physical stock certificate. CSDs also provide custodial services as well as play an active role in securities' issues.
- **International central securities depositories (ICSDs).** ICSDs main function historically was to settle Eurobond trades. Now they are active in clearing and settlement across different international markets and currencies. They can also be involved in securities lending, tax services, voluntary corporate actions, collateral management as well as proxy voting.
- **Central counterparty clearing houses (CCPs).** A CCP is an organization that helps facilitate trading of various asset classes and is often operated by the major banks in the country. A CCP is a counterparty to the buyer and the seller and guarantees the terms of a trade even if one party defaults on the agreement. Parties are usually required to deposit a collateral (i.e. margin) with CCPs, safeguarding successful completion of the trade.
- **Custodians.** Large investment banks that hold customers' securities in both electronic and physical form. They ensure safekeeping of the assets and try to limit the risk of theft or loss (Shaofang & Marinč, 2015).

Transaction or trade process is typically split into three stages (Figure 14).

Figure 14: The trade process



Source: FSI (2015).

In the pre-trade process an investor decides whether they want to trade and decide on what asset type they want to trade. Going further into the trade process, an investor willing to buy is connected with an investor willing to sell – usually through a broker or a dealer. Mainly, for most financial products, the broker will use an organized financial market known as exchange where various financial products are traded. If wanted, a broker can execute the trade directly with another broker via so called over-the-counter trading. When both parties agree on the price of the exchanged asset, the financial product and cash are exchanged between them. Finally, clearing and settlement processes in the post-trade phase are used to ensure successful completion of the exchange.

Transaction and information flows in clearing, settlement and payments are very opaque, time consuming, require significant amount of reconciliations and typically involve multiple intermediaries. Below I explain how shared ledgers can bring unprecedented cost-efficiency and transparency in the system should blockchain's broad-scale adoption occur.

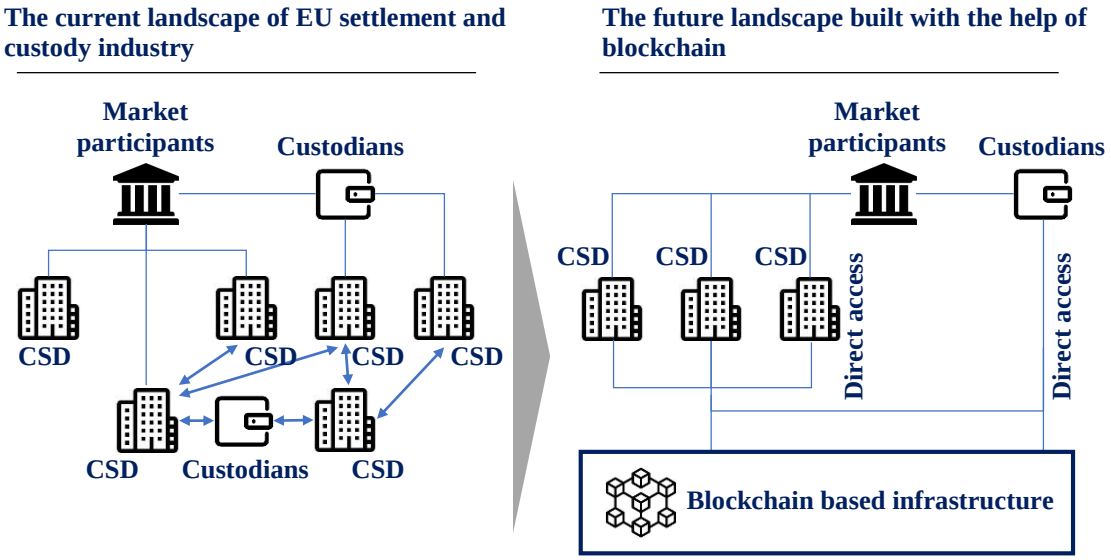
2.3.1.1 Settlement and custody

Across the whole trade chain a blockchain solution would be potentially most suitable to ensure safer, faster and more efficient post-trade process. A consistent and single "source of truth" of assets' ownership could be provided to different market infrastructure providers such as CSDs, CCPs, custodians and beneficial owners. Current typical two days securities settlement (T+2 basis) can be mitigated via a shorter settlement cycles which could help reduce risk and settlement failures, especially exposure to counterparty risk of various dealers.

A register of asset owners could be made available on a real-time basis to permissioned entities such as clearing houses, agent banks and custodians (Figure 15). Existing process flow where beneficial asset owners interact with CSDs via agent banks and custodians could

be made more efficient and cost efficient by allowing custodians to interact directly with asset owners and CSDs via a permissioned blockchain. While the distributed ledger could potentially change existing processes of custodians, industry leaders do not believe that their core functions and therefore their revenue flows could be fully removed as regulators and market participants show greater need for secure and regulated safekeeping of assets.

Figure 15: Current versus future settlement and custody industry setting



Source: Standard Chartered (2016).

2.3.1.2 Clearing

CCPs' importance has been severely elevated via passage of the Dodd-Frank Act and European Market Infrastructure Regulation (EMIR) recently, which have directed that a large number of OTC derivatives transactions be centrally cleared through such infrastructure. While blockchain could deliver instant and finalized settlement, and since there is total transparency into whether trading counterparties can meet their obligations, industry experts and leaders have questioned whether CCPs would become redundant. Standard Chartered and Credit Suisse, among others, believe that this is not likely to happen and that CCPs will have its role in a blockchain era and will continue to perform a key role in novation and risk mitigation for both buyers and sellers. It is possible to replace CCPs' novation function, yet this would require the market to transact bilaterally (where margin payments would be triggered by smart contracts) which would interact with cash accounts at commercial or central banks held off or on-ledger. While this is technically feasible, it is questionable whether an improvement on the existing market structure would result in significant cost savings and additional level of transparency. Therefore, it is expected that CCPs would continue to perform clearing and netting functions, thus reducing settlement volumes and demand for settlement liquidity. Additionally, they would retain the transaction collateral management role – ranging from period transactions in derivatives markets to

administrative demand for settlement in cash markets (Standard Chartered, 2016; Credit Suisse, 2018).

In theory, most markets could migrate to T+0. While the existing legacy market infrastructure is capable of faster operating, different laws, regulation and market convention show little appetite for change, as fast and instantaneous settlement would increase liquidity requirements and capital efficiency since every transaction would need to be settled, opposite to current end-of-day net settling. DTCC estimates that over 97 % of daily equity trades in the US are settled through netting and only 3 % of trades go through the full settlement mechanism (Credit Suisse, 2018).

2.4 Payments

Payments are the lifeblood of any economy and business – without the ability to pay and receive money there can be no business. Payments' industry worldwide is enormous and helps to transfer value in any form of money. To perform a payment, originators of payments and their processers use a range of different channels and each of them has different operating characteristics, rules and settlement mechanisms. The value being transferred is usually stored in depository accounts at banks or other financial institutions. To enable payments and value exchange, banks need to be connected to a set of payments systems and need to use them to process payments on behalf of their customers. Banks are, in current infrastructure setting, connected to a wide array of payments systems, often to more than 50 at once. Examples of such systems are Fedwire (US Federal Reserve Bank network), SEPA (Single European Payments Area), CHIPS (Clearing House Interbank Payment Systems) or SWIFT. Banks that operate in different countries connect to payments systems in each of the countries where they operate either directly or through a correspondent bank. For more efficient settlement process and for successful use of less conventional payment systems, banks worldwide typically maintain accounts with a country's central bank and participate in that central bank's payment systems (Treasury Alliance Group, 2018).

Looking broadly, all payment systems can be placed into one of the following five payment channels:

- **Paper based systems** such as checks or drafts. These are one of the oldest forms of non-cash payments and are still widely used in the United States. To perform a payment, one party needs to write an instruction on paper to pay another.
- **High-value payments** such as Real Time Gross Settlement (RTGS) mechanism or others - also called wire transfers.
- **Low-value batch systems** or **Automated Clearing House (ACH) batch payments**. Unlike wire transfers, those payments are processed in batches and were originally intended for small payments under $100,000.

- **Cards.** A payment channel including credit, debit and stored value cards. Use of this channel is growing tremendously worldwide for both making and receiving payments. The card channel also provides the "rails" or settlement systems that support some of the newest ecommerce payments systems (i.e. mobile wallets).
- **New payment systems** such as mobile applications, cryptocurrencies and other payment mechanisms: Examples of these include Bitcoin, Alipay, Ripple etc. (Treasury Alliance Group, 2018).

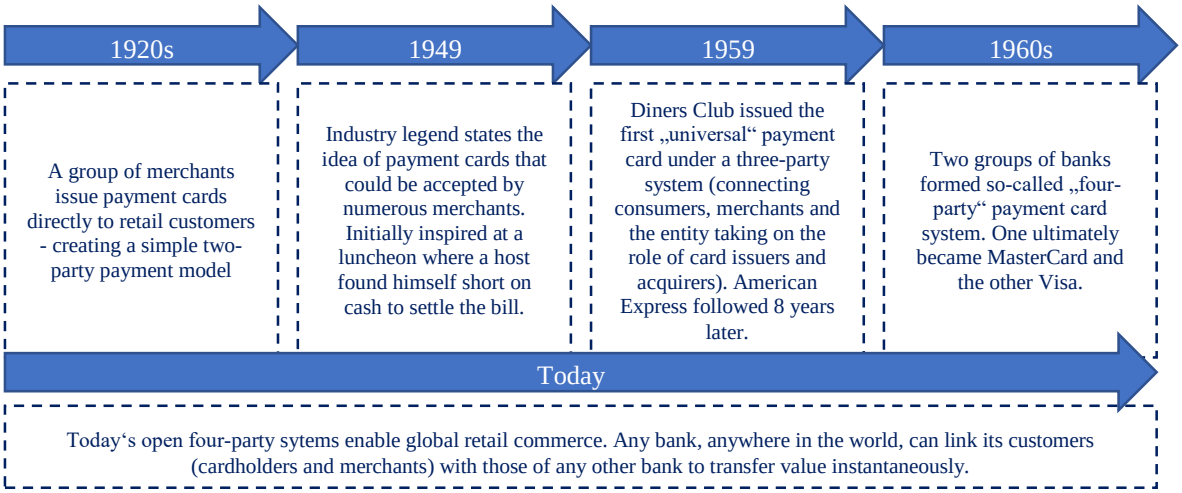
We further distinguish payments depending on where two transacting accounts are held. If two accounts are held with the same bank, we talk about **intra-bank** transfers. If the money transfer happens between two different banks and is often international, then we talk about **inter-bank** transfers. The latter transactions are usually more complex and are using the principle of correspondent banking – making transaction fees magnitudes greater (Visa, 2006).

The payments business is a major source of revenue and data for both retail and wholesale banking institutions. Nowadays, banks still remain most trusted financial partners for both customer groups as they bring broad expertise to the payments ground. Highly regulated business has historically offered continuous protection of customers' assets, data and needs. Those strengths and reputation made sure that banks remained the go to place for both retail and corporate clients. Still, bank's leadership in the payments sphere is under attack recently. Digital entrants, new digital tools, technologies and capabilities are all trying to eat into banks' integrated value chain. New players don't need to have same sizes of balance sheets and geographical footprint as incumbent banks, nor do they need to offer the same product portfolio. Instead, they can now pick off a certain part of the traditional payments value chain – from interface, product portfolio, or the underlying infrastructure – and utilize modern technology to disrupt the market. This shook the market and changed stakes considerably, threatening to displace the long term customer ties that banks had.

2.4.1 Card payments

Credit and debit card payments market is highly frictional and outdated. It is based on the so called "four-party" system, which has its origins in the 1960's (Figure 16). Such system adds three extra participants between the consumer and the merchant and is often under scrutiny as transaction costs are too high.

Figure 16: Four-party system



Source: Credit Suisse (2016).

The system is composed of four parties:

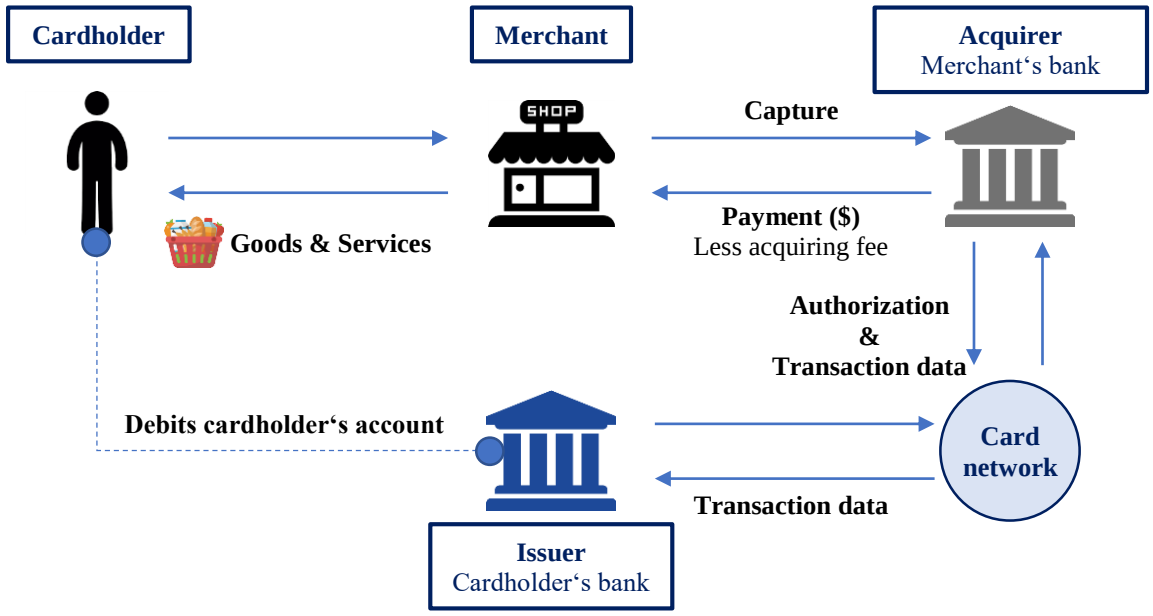
- **Merchants.** The ones selling the goods to the end customer.
- **Acquirers.** Banks or specialist acquirer processing firms such as Elavon, WorldPay, First Data, Global Payments, etc.).
- **Issuers.** Banks and other card issuing firms (i.e. HSBC, Bank of America, UniCredit, Deutsche Bank, etc.), which usually use services of specialist issuer processors such as TYSY.
- **Card schemes or card networks.** Visa, MasterCard, China Union Pay, American Express, JCB, Diners/Discover (Treasury Alliance Group, 2018).

An example of a non-cash transaction in a four-party system is shown in Figure 17. As seen here, a four-party system employs three additional players between the customer and the merchant. Logically, such system has been under much scrutiny and criticism recently as it is believed that the fees are too high and can be brought down with the use of blockchain.

So, how does a transaction happen (Figure 18 depicts the usual fee breakdown for an end-consumer payment worth $100)? Let’s imagine a cardholder (customer) uses his Visa debit card, issued by a bank with which he has a retail account. For example, let’s suppose he has an account with the HSBC bank, which is in this case the “issuer”. The customer will then use his Visa card to buy $100 of goods from the merchant. The latter again has a contract with a so called acquirer, which can be either a bank or a specialist acquirer firm. Hence, the acquirer, card network/card scheme and card issuer all charge fees so that the typical cost to the merchant in the US is around 2 %[5].

[5] Credit Suisse (2016, p. 56) estimate.

Figure 17: Four-party system based transaction



Source: Adapted from Treasury Alliance Group (2018, p. 12).

Figure 18: Four-party system fee breakdown

Source: Credit Suisse (2016).

Blockchain, due to its decentralized nature, can cut out many middlemen in the card payments industry. Removing these middlemen out of the picture effectively slices the transaction overhead and can even facilitate what is known as "micro-transactions"—small transactions conducted with near-zero charges and instant verification. Similar would be with chargeback fees. Since customers have the ability to decide on the transaction fees, merchant don't have the ability to take more than what is needed to process a payment (Credit Suisse, 2016).

2.4.2 Cross border payments

Cross-border payment would be, per a broad definition, a transaction that involves individuals, corporations, settlement institutions, central banks or a combination thereof, in at least two different countries. Transactions are usually classified as:

- **Large value transactions** that are usually related to financial market transactions, particularly foreign exchange – Forex.
- **Non large value** generally related to international trade of goods/services and remittances

2.4.2.1 How cross-border payments work today

As the world gets more interconnected, cross-border trade grows rapidly as companies increasingly ship goods and services worldwide. Vast majority, approximately 80 % of cross-border trade payments are nowadays handled through the so called "correspondent banking" relationships, where a series of banks and domestic payment systems are linked together to move funds. Banks maintain correspondent banking relationships with local banks across cities worldwide and the correspondent, either itself or through its partnerships, provides the liquidity for international payments in local currency accounts abroad. To service international payments, a bank has to establish a line of credit with the correspondent bank or pre-fund a nostro account internationally. A nostro account is a bank's account held in a foreign country, denominated in the foreign country's currency and used to facilitate cross-currency exchange and settlement. In such system the bank providing the services is called the **correspondent bank**, while the one buying the services is called the **respondent bank**.

Correspondent banking has been used as a model for cross-border payments for centuries. Since money has to move across different systems with low coordination and double bookkeeping, settlement is slow (often 3-5 days) and traps liquidity, error prone (error rates run upwards of 12.7 %[6]) and very costly. Little changes of fundamentals have been made, helping banks generate substantial value in the meantime. McKinsey estimates that cross-border transactions represent 20 % of total transaction volumes in the payments industry, yet they generate 50 % of its transaction-related revenues[7]. Opposite to domestic transactions which got hit by competition and regulation in recent decades, margins in cross-border payments remained healthy over time. Only now, with rising pressures from regulators, digital innovators and customer expectations for seamless, real-time and digitally enabled systems, banks have started to rethink their old and outdated international payment systems – especially for low-value payments.

[6] See Ripple (2016).
[7] 2015 Data. See McKinsey & Company (2016, p. 3).

Current setting of corresponding banking system inherently has four issues:

- **Access.** Funding positions across the world is needed to perform cross-border transactions and some global corridors might require additional corresponding bank partners, which in effect translates to non-competitive FX, fees and liquidity.
- **Finality and certainty.** Long chains of intermediaries exchanging information presents error prone and non-efficiently connected siloed systems, leading to unpredictable processing times, low transactions and liquidity visibility, and uncertainty in funds delivery.
- **Speed.** Payments often take more than 3-5 working days to process. Different corridors with different time zones are a huge issue here.
- **Cost.** To perform a transaction, banks absorb massive costs related to payment processing, treasury operations, liquidity, FX and compliance.

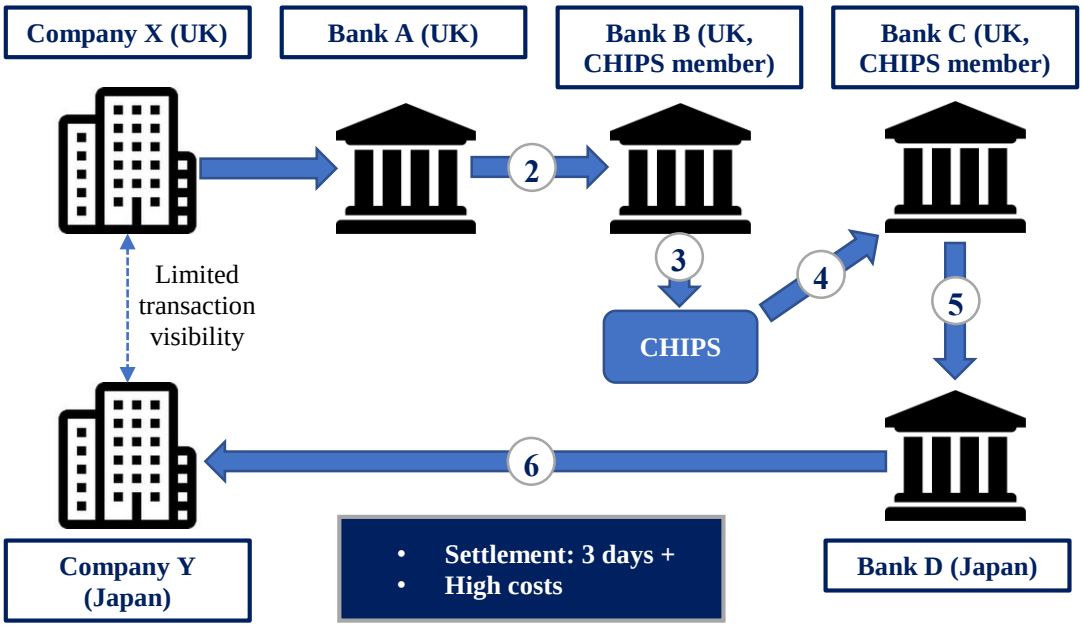
Cross-border payments are often settled in a specific country's domestic settlement system. For example, a German company which wants to make an US dollar payment to a Japanese company sends the required dollar amount from its US correspondent bank to the Japanese company's US bank account in the United States. Usually, the payment is made through an ACH or RTGS transfer. Should the Japanese bank not have an account at a bank in the United States, then the funds are transferred to the Japanese company bank's correspondent in the US.

An example of a cross-border transaction is explained in Figure 19: Company X, located in the UK, wants to make a payment to the Company Y in China. Therefore, Company X asks its bank (bank A) in the UK to make a GBP payment to Company Y. As Bank A does not belong to the certain payments system (for example CHIPS[8]), it asks its correspondent bank (Bank B), which is a CHIPS member, to make the payment. Therefore, Bank B sends the funds via CHIPS to Bank C, which is also a member. Bank C is the correspondent bank for the Japanese Bank D, which is where the Company Y has an account to receive funds (Visa, 2006).

Rising profitability pressures and rising liquidity and compliance costs have forced banks to exit selected currency corridors. As the world becomes more and more connected and as the Internet of Things surfaces, we shall see increasing demand for international payments, especially in the low-value segment, serving new remittance corridors and device-to-device micropayments.

[8] CHIPS or Clearing House Interbank Payments System is a United States clearing house for high-value transactions.

Figure 19: Example of a cross-border transaction



Source: Visa (2006).

2.4.2.2 Retail low-value payments – remittance services

Migration is on the huge rise worldwide. Millions of people live and work far away from home, following opportunities globally and sending huge parts of their earnings home, where the rest of their family lives. The transfer of money by a foreign worker to an individual in their home country is called a remittance. Remittances are not a new phenomenon and have been normally associated to migration which has always been a part of human history. They are a huge part of international capital flows, especially to labour exporting countries.

Spain, Italy and Ireland were historically heavily dependent on remittance income received from their emigrants during the 19th and 20th centuries. Industry of remittances worldwide has massively increased, from less than $100 billion in 2000 to more than $613 billion in 2017[9]. More than two thirds of those capital flows were to low and middle income countries, especially to the people in the APAC region. World remittance flows are expected to increase by more than 4 % in the next years. Not only banks, high margins and low efficiency of cross-border payments have attracted the attention of so called Remittance Service Providers (RSPs) such as Western Union and MoneyGram which are targeting mainly unbanked or under-banked consumers and are differentiating their offerings by speed, convenience and clarity rather than price (World Bank Group, 2018).

Key risk factors of remittances are shown in Figure 20. Remittance money flows are mainly cash transactions which include high-risk locations as destinations (where there is often

[9] See World Bank Group (2018).

violence, terrorism and a lack of government oversight). Operations are mainly conducted through agents or RSPs, which makes it difficult to perform any Know Your Customer requirements. As such, they are difficult to track and are therefore highly sensitive to money laundering and terror financing fears. Banks worldwide still consider it as high risk and have been massively de-risking over the last years (i.e. closing the bank accounts of customers in countries or sectors believed to pose high risk of terrorist financing and money laundering). Also, banks consider RSPs as entities not having sufficient controls, lacking customer due diligence and the capacity to comply with the AML/CTF regulations. Banks make generalizations here and apply the same risk-factors to the entire remittance sector, not differentiating between "bad" and RSPs having sufficient controls. As a result, even if a RSP has good control system, it might not get access to correspondent banking. Those key risk factors are limiting innovation in the space and constraining introduction of cheaper modern technologies – among which we find Internet, smartphone, apps and blockchain – keeping the average cost of remittances above 7 %.

Figure 20: Key risk factors of remittances

- Remittances difficult to track and potentially sensitive to money laundering (AML) and terror financing (CTF) concerns
- De-risking measures taken by commercial banks
- Remittance sector perceived as high risk
- Exclusive partnerships between national post office systems and a single money transfer operator
- Lack of supervision and compliance requirements for RSPs
- Some RSPs may not have access to correspondent banking

Source: Own work.

The main force making cross-border payments inefficient is the lack of a single universal global payment system. Inefficiencies in the transactions are put down to corporates, which results in higher direct and indirect costs. A recent survey of corporate leaders indicated that more than 40 % of respondents want reduced time needed to detect and resolve unauthorized debits, reduce the time required to identify insufficiently funded debit transactions, and receiving credit for overseas payments. In order to improve the challenges cross-border transactions are facing, three main challenges need to be improved:

– **Most payment systems are designed and based on local laws and practices within domestic banking and financial structures**

Domestic infrastructures, which have been established by various countries for both high and low value payment systems, are mostly based on proprietary communication and security standards. There is therefore a huge lack of standardization and automation in both inter-bank and intra-bank networks, often resulting in manual intervention to collect and

amend data. The United States, for example, has many siloed payment infrastructures, which are competing among themselves for user volume. Out of more than 60 major clearing and settlement entities (number down from several hundred in the last years), an US bank needs to operate several redundant payment platforms and operations. Specific and dedicated applications, trained staff and various business processes only add to massive banks' operating costs.

- **Lack of a single universal global standard and deviations between different systems are reducing the ability of both bank and corporate treasury/enterprise systems to efficiently exchange data**

Manual processes, especially paper handling, are being removed by virtually all business types in the world. Financial institutions' data and payment instructions have to be generated and sent securely and cost-efficiently to the recipient. Order matching and reconciliation needs to happen automatically. Yet only 15 % of respondents in a recent wire transfer survey indicated that their wires always come with sufficient information of a remittance payment and that more than 17 % of the received wires need to be further researched by a receiving firm – at the average cost of $35 per wire and 30 minutes of time. Large costs associated with enhancing internal systems and processes relative to the small volume of international payments are the reasons why institutions are lacking the drive to adopt common standards. And before institutions adopt a standard that can be used across various market, it needs to comply with multiple domestic rules and regulations. Not only that, standard's value is recognized only when the specification is widely accepted, making banks reluctant to invest if they are uncertain should other banks make similar investments to upgrade their systems.

- **Government regulations and incentives are changing the payments landscape. Domestic regulations are shaping payments, which only compounds the challenges cross-border payments face since rules often vary between a sending and receiving location**

The complex structures of different payment systems (which can be public, private or operated as industry consortiums) only adds to the challenge. Cross-border payments' route often goes between systems with totally different rules and regulations, thus lifting complexity and fees.

Cross-border transactions costs are mainly related to different factors. In order to make an international payment firms often have to pay fees and commissions as well as other explicit or implicit fees (i.e. foreign exchange conversions). Years old worldwide use of correspondent banking model only adds to the complexity and makes the execution time and cost of a cross-border payment substantially higher than that of domestic transactions (Visa, 2006).

2.4.2.3 Trends in payments and impact on cross-border payments

Legacy transaction services provided by banks are becoming increasingly commoditized. The treasury, liquidity management and risk management functions are integrated more closely in order to deliver greater efficiency in an increasingly global environment.

Key trends impacting cross-border payments are:

- **Transnational payment systems are growing.** Before there was only one domestic payment system in a certain country and now we are witnessing the emergence of different transnational systems such as TARGET, CLS (Continuous Linked Settlement) or FedACH (Federal Reserve's International ACH Project). On the other side, card payment systems such as those run by VISA or MasterCard are already global in nature and have expanded to commercial payments from retail payments only. Further growth and interconnectedness of transnational systems can reduce clearing and settlement times and can ensure better visibility of funds flows. More importantly, standardized and non-siloed formats will greatly reduce the amounts of errors, duplicates and repairs.
- **Increasing initiatives and mandates of governments.** Recent anti-money laundering (AML) and counter terrorism financing (CFT) initiatives require that cross-border transactions satisfy additional stringent requirements. To satisfy ongoing list of requirements banks' compliance costs are significantly rising while offsetting new revenue opportunities are only minor.
- **Closely managed risk and liquidity usage.** Among many risks payment systems are facing, credit and settlement risks[10] are two of the most significant. Payment systems that process payments in real-time or in batches during the day, in both gross and net settlement systems, have a clear relationship between liquidity usage and settlement delay. Sender's liquidity costs are reduced by a delay in settlement, while both delay and liquidity costs of the receiver are increased. Hence, it is important that payment systems strike a balance between minimizing the liquidity costs and keep settlement risk under control. Improvements in both risk and liquidity management help drive down overall costs by reducing losses and free up excess capital that is used during settlement.
- **Expansion of multinational corporations and banks.** Large conglomerates or international players such as Goldman Sachs, HSBC, Bank of America, UniCredit, and Deutsche Bank operate their own internal global payments networks, which send payments to different countries across the globe. Such internal networks usually don't differentiate between domestic and cross-border payments as these funds flows are all within the corporation. Internationalization and consolidation of main banks ensures global economies of scale, which can help drive down transaction costs further and can increase payment revenues that happen under their umbrella.

[10] Credit risk – the possibility that a party within the system won't be able to fully meet its financial obligations. Settlement risk – the possibility that a party will have insufficient funds to meet a financial obligation as and when expected, although it may be able to do so at some time in the future.

- **Increasing usage of outsourcing in order to drive further operational efficiencies.** Banks are increasingly expected to focus on sales and marketing (maintaining direct relations with clients) functions only, while the "back office" functions such as processing of payments and securities is being outsourced to other niche players. Outsourcing of non-core activities can help banks reduce operational costs as well as offer additional products that previously could not be provided (Visa, 2006).

2.5 Fundraising

Current applications used to support the issuance of securities (i.e. stock and bonds) are often still based on issuances of physical certificates or notes representing ownership. Redundant and siloed record keeping is leading to large reconciliations across market participants. There are several ways a company can get new capital infusions. Capital can be raised by selling registered securities publically or privately through the issuance of unregistered securities. Securities could be equity or debt-related and are offered to potential investors in both public and private markets. The process remains manual and paper intensive, leading to higher cost of issuance. Average fees paid are 3.45 % for Regulation D private security issuance, 0.9 %-1.5 % for a bond issuance and 7 % for an IPO issuance (Capgemini Consulting, 2016a).

The issuance and trading of securities is a heavily regulated process. In the United States, The Securities and Exchange Commission is responsible for oversight of the capital markets industry. Currently, issuance processes are based on the creation, distribution and management of physical documents (i.e. stock certificates, bond notes, etc.) and are administrated using a traditional book entry system. Once securities are issued, the purchase/acquisition and subsequent trading of these securities documents is conducted via legacy securities exchanges such as NASDAQ, NYSE or AMEX, and cleared and processed through the established clearing system (i.e. such as that of DTCC).

A legacy system of siloed intermediaries in charge of securities issuances faces several challenges:

- **Multiple versions of truth.** Issuers, syndicate members and investors maintain their version of record, requiring a time consuming reconciliation process between participating systems.
- **Long clearing and settlement cycle.** T+3 days is a market norm when settling a trade. Private security settlement in some instances can take up to 10 days to settle.
- **Manual handling of processes.** Labour intensive work is prone to error and makes security issuance process inefficient.
- **Potential counterparty risk.** Long settlement cycle keeps the counterparty risk open on both ends.
- **A long chain of intermediaries makes process less transparent and costly.** To complete or change a transaction, information has to be cascaded across a layer of

intermediaries (i.e. stockbroker, exchange, bank, local custodian, global custodian CSD, etc.), adding additional cost and time.

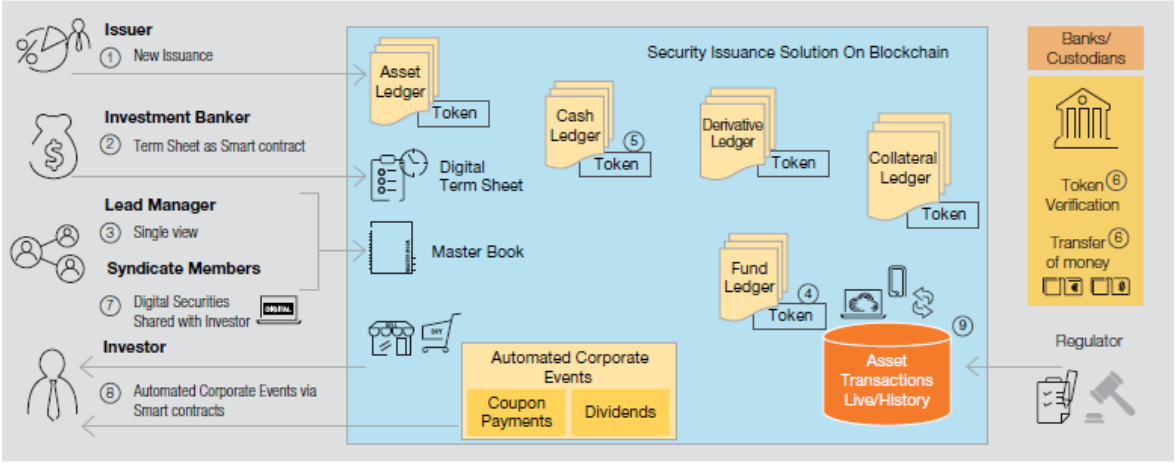
– **Limited audit trail.** Manual security issuance processes give no electronic audit trail of the activity performed with the transaction.
– **No 24/7 availability.** Many intermediaries working on different systems make it nearly impossible to maintain 24/7 system availability (Goldman Sachs, 2016).

2.5.1 Blockchain's use case in the legacy industry of securities issuance

Smart contracts that execute on blockchain can be used in both public and private security issuance processes. Removal of physical documentation and a fully digitized solution can reduce the use of intermediaries, making process lean and much more efficient.

A permissioned blockchain system with programmed smart contracts that automatically execute terms and conditions associated with a contract would fully replace physical certificates and notes of the traditional issuance process. A set of decentralized and geographically distributed permissioned nodes would process transactions and make them immutable and transparent, creating a unique and shared version of truth (i.e. record of ownership) viewable by multiple participants as well as market regulators. Current system of siloed and separate records would be enhanced by blockchain and would not need reconciliation by different parties. Blockchain further allows for direct issuance of digital securities by issuing them on the distributed ledger through standardized and secure transactions. Such open and digitized structure allows for direct dealings between issuers, syndicate members and investment banks and helps to track real-time ownership of the securities. Multiple intermediaries of issuing agents and custodians are not needed, resulting in reduced costs. Figure 21 shows a blockchain based securities issuance model and its functions with reference to various market participants.

Figure 21: A blockchain based solution for a fully digitized security issuance process



Source: Capgemini Consulting (2016a).

The steps below articulate the roles and responsibilities performed by specific participants:

1. **Issuer issues new securities into the asset ledger.** Issuer gets a limited time slot right to create the new asset on the asset ledger.
2. **Investment bank.** To help with the securities issuance process and preparation of the digital term sheet, an investment bank is mandated by the issuer.
3. **Lead manager and syndicate members** have a single view of the Master Book on a blockchain platform. The Master Book contains prospective investors' bids or orders as well the quantity and price of shares requested.
4. **The fund manager** uses tokens to manage investor's holdings that are recorded on fund's ledger. Tokens that represent cash or security are used to determine value of the investor's portfolio and represent investor's holdings on the blockchain platform. These tokens are then used in case of a trade settlement happening within or outside the platform.
5. **Cash transfers** are represented via tokens.
6. **Custodians and banks.** When settlement occurs outside the blockchain platform, custodians and banks act as keepers of tokens and transfer securities/money to the beneficiary accounts.
7. **Digital securities** are credited to investor's account.
8. **Mandatory corporate events and disbursements** are executed when smart contracts are triggered. Ownership of the asset determines potential dividend payments, coupon payments, interest, stock splits, return of capital or mergers.
9. **Regulatory reporting** becomes easier as the data is now publicly accessible and has complete audit trail, thus providing full transparency. Better monitoring of money flows and transactions is enabled by live data auditing, providing regulators with greater ability to detect financial instability, fraud or money laundering (Capgemini Consulting, 2016a).

2.5.2 Initial coin offerings and information asymmetry

Startups, especially blockchain startups, have most recently embraced so called Initial Coin Offerings (ICOs) as a vehicle to raise early money. ICOs propel the liquidity enhancement of the early stage start-up finance needs for capital and offer an alternative to bypass both banking and non-banking entities (i.e. Venture Capitalists) and their services. ICOs offer the opportunity to raise funds for an early stage development project and unlike IPOs, where companies issue and sell stocks via regulated and centralized exchange platforms, issue digital coupons or so-called "tokens" that are then traded on various exchanges.[11] Often cited as a crowd sale, ICOs are made by a company that issues its own cryptocurrency or token and sells it to wide audience. In this way the company gets the funding needed for product

[11] Token issuance occurs on the blockchain (usually on Ethereum's) and in the form of an organization's cryptocurrency. These tokens then represent the capital inflow required to finance the project and can be sold on an exchange (such as Bitstamp, Kraken, etc.) a few weeks later.

development, while investors participating in the sale receive ownership of a token, which can serve as a way to access the company's platform. When investing in an ICO, investors' risks and rewards when buying a token differ from those of equity. In contrast to IPOs, successful ICOs do not require the underwriting support of a reputable banking institution and therefore remove almost all costs associated with the issuance. Also, current absence of regulatory constraints, procedures with simpler reporting requirements makes ICO fundraising significantly less expensive than a typical IPO. ICOs are further distinguished from crowdfunding as they usually involve a financial stake in the company and its assets. The token ownership in certain cases represent the right to vote on future decisions. The typical way for a company, usually a start-up, to raise money through ICO is to publish a whitepaper that describes their business model, outlies the technology of the firm and plan for the future. The white paper also describes token's functions when issued. Company describes how and when it is going to use raised money and distributes tokens providing access or representing ownership of the company to its founders and outside investors after the sale is done (Conley, 2017).

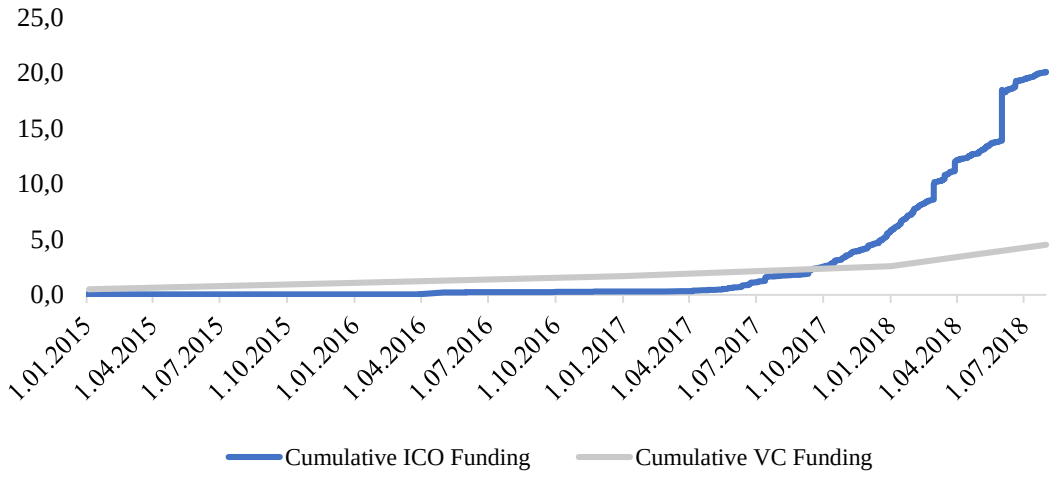
Currently almost every person, with some exceptions of USA's and China's citizens, can participate in such crowd sale and invest in different blockchain projects or start-ups around the world. Having democratized Venture capitalists, this new environment presents both new opportunities as huge risks to investors, especially to the normal financially uneducated public. Various governmental agencies across the globe such as SEC, Chinese Central Bank and Singaporean Central Bank MAS have already issued warnings on ICOs, some of them even banning them due to various malpractices, massive speculation, money laundering and terrorist financing risks.

Nevertheless, the total amount of funds raised via ICOs has reached $20 billion as of Q2 2018 and has greatly surpassed VC funding (Figure 22). Democratization of VCs has led to the global start-up funding by the retail investors, allowing biggest ICOs such as that of EOS and Telegram raising $4.2 billion and $1.7 billion in a matter of few days.[12]

The aggregate numbers aren't so impressive at all. In fact, the speed at which capital can be raised through this funding channel is remarkable. For example, Brendan Eich, Mozilla's former CEO, raised $35 million in 30 seconds for his start-up Brave. The majority of capital raises are performed by companies not having even a working product, which only adds to the confusion of ICO financing. ICOs have the potential to disrupt the business model and asset classes of private equity and real estate funds. The traditional closed nature of venture capital industry has already been shaken, enabling start-up investing for non-accredited retail investors. Borderless nature of tokens has enabled capital injections by a global pool of investors and has diminished typical legal, jurisdictional and business hurdles of traditional venture capital financing. Opposite to traditional non-liquid private placements where VCs

[12] There are 4141 ICOs published as of 17 August 2018. Average ICO size was $16 million in 2017 while start of 2018 saw even bigger deals with the average size of $31 million (Coindesk Research, 2018).

Figure 22: Cumulative ICO and VC funding ($ billion)



Source: CoinDesk (n.d.).

need to wait for an IPO or an acquisition to exit the investment, ICOs and token issuances offer venture capital funds substantial liquidity from the day one (see Figure 23 that compares ICOs to other types of financing) (Kaal & Dell'Erba, 2017).

While there are obvious benefits of the ICOs, certain emphasis has to be put on assessment of the risks that come with its execution. Current loose regulations enable risky issuances to be openly marketed to a wide audience with minimal controls and are subject to pure speculation, both from general public as well as sophisticated investors. The typical ICO has no customers, no revenue and no working product. Prices are mostly driven by the fear of missing out (FOMO) and valuations built mostly on promises written in whitepapers. To spread information about the money raising worldwide, ICO founders utilize various social media channels and reach of reputable industry experts. However, as research has shown, not all social networks enable efficient markets and proper risk assessment on collective level (Zuckerman, 2003).

How do ICOs fit into this? One could not miss the mass crowd excitement and obsessive investments into new token issuances of promising companies recently. Search for yield has led investors to provide capital for ICOs, making underlying investments into companies synonymous with hype and excessive risk taking. Worldwide pool of (mostly) retail investors have flooded the market and did not asses risk properly. How did this happen? When executing an ICO, the team behind it calls for the help of high profile and reputable ICO advisors who are often incentivized inappropriately to market the products and services - irrespective of quality. This effect of social influence diminishes the diversity and independence of the crowd, often biasing collective wisdom of the crowd and leads to wrong assessment of both possible risks and rewards. This effect is often seen together with the information asymmetry as the flow of information is often one sided – going from sellers to

Figure 23: ICOs versus other types of financing

	Public offering	Private offering	Crowdfunding	Tokens
Global investor base	✓ ✓	✓	✓ ✓ ✓	✓ ✓ ✓
Transaction size	✓ ✓ ✓	✓ ✓ ✓	✓	✓ ✓
Access for retail investors	✓	✗	✓ ✓ ✓	✓ ✓ ✓
Fast execution	✗	✗	✓ ✓ ✓	✓ ✓ ✓
Low capital raising fees	✗	✗	✓ ✓ ✓	✓ ✓ ✓
Low regulatory burden	✗	✗	✓ ✓	✓ ✓ ✓
Transparency of ownership	✓ ✓	✗	✗	✓ ✓ ✓
Secondary liquidity/ transferability	✓ ✓ ✓	✓	✗	✓ ✓ ✓
Low trading/ transaction fees	✓ ✓	✓	✗	✓ ✓ ✓
Dividends	✓ ✓ ✓	✓	✗	✓ ✓ ✓

Source: Adapted from Mango Startups (2017).

buyers. Given limited information about the issuing organization and technical aspects behind the idea, buyers cannot accurately assess the value of a token and can only rely on the numbers provided by the sellers. Unlike to IPOs these effects stand out even more here as the new asset class of tokens doesn't fit into established frameworks for comparison and valuation and the only tangible basis to determine any form of future utility of those assets is based on the information provided by the issuer, either through the whitepaper or via other forms of communications. Therefore, the token buying public, which is often financially unsophisticated and has limited and selected information about the issuing organization and technical concepts behind the offering, can only trust that the issuers and its spokespersons are trustworthy and are competent to deliver what is promised. To raise interest in the ICO even further, the issuers state whatever is needed and still hold no fiduciary duty to fulfil it. (Sehra, Smith & Gomes, 2017).

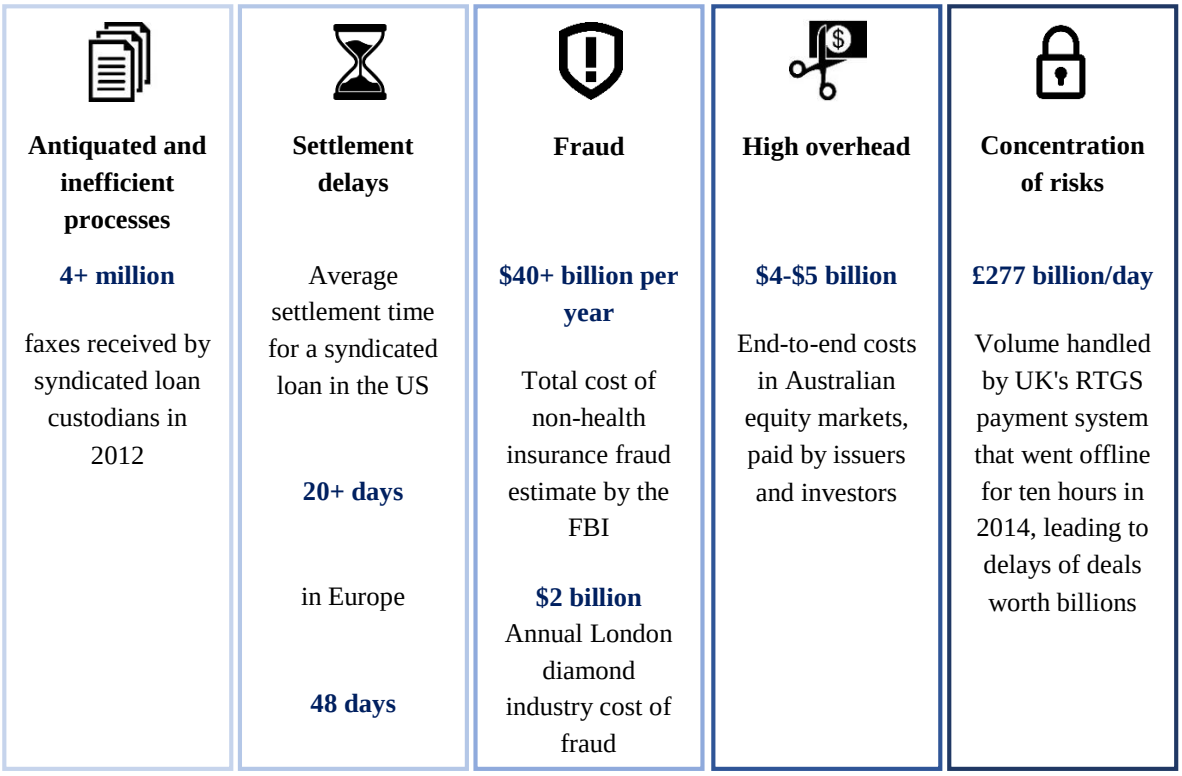
2.6 Smart contracts

It was in 1994 when Nick Szabo, a computer scientist and cryptographer, proposed the outline of so called "smart contracts". Smart contracts, enabled by distributed ledgers or blockchain, are supposed to act as a cure for outdated traditional financial contracts. It is hard to imagine that the amount of reliance on physical documentation, when the disruption by cutting edge technologies is booming daily, is still pretty high among capital markets participants. For example, it is not uncommon that market participants communicate via fax machine in the multi trillion-dollar syndicated loan market as there were more than four million faxes received by loan custodians in 2012. Physical documentation leads to massive delays, increases exposure to fraud, errors and inefficiencies. And high overhead costs and compliance requirements only add additional pressure on profitability of financial intermediaries. Smart contracts that were firstly described as a computerized transaction protocol that executes the terms of an underlying contract became very interesting with the development of blockchain. A universally accepted definition of a "smart contract" still needs to be defined, yet the core functionality is clear: **decentralized consensus driven contracting on contingencies, with low-cost and automatic execution**. And when we embed those smart contracts on a distributed ledger or a blockchain, we automatically get a strong element of immutability and permanence. Underlying assets and contract terms in a smart contract are firstly coded and put into the blockchain, a copy of which is then shared across multiple (confirming or verifying) nodes in the network. As the data on a blockchain is spread across the network, participating entities are aware of the contract terms and associated value transfers, meaning that the transactions are easily trackable and certified. Only with a decentralized consensus can we limit huge market power (or data monopoly) of the third party consensus provider. All traditional resolutions by third parties (i.e. arbitrators, courts) require high human intervention input, leading to greater uncertainty and cost. Smart contracts can therefore facilitate increased exchange of value, money, property, services or products, both automated and in a conflict-free way (William & He, 2018).

Several industries, especially the financial services industry, became very interested in the potential of smart contracts. Recently, banks and industry consortia have introduced working prototypes, a Smart Contract Alliance has formed, and technology has been bolstered by cooperation of technology firms. Bank seniors and executives have started to take it seriously as well. As Roberto Mancone, Deutsche Bank's Managing Director and Global Head of Disruptive Technologies and Solutions put it: "Smart contracts technology has great potential and could transform the business model of many segments of the banks, solving many of the problems banks and regulators are facing". But there are various risks and potential drawbacks on the other site, saying: "The industry still has to test and ensure that these are as robust, autonomous and secure as they are promised to be and the adoption will vary according to geography, regulatory frameworks and complexity of assets managed". Fabian Vandenreydt, Global Head of Securities Market at Innotribe and The SWIFT Institute, sees major inefficiencies and limitations of existing commercial contracts: "There

are still large parts of the securities industry, such as syndicated loans and others, that haven't transformed to digital and operate mainly via faxes and physical documents. I think it is time for industry players to break out of this inefficiency and consider new technologies (like smart contracts) as an opportunity to first digitize in the short term and also leverage reduced operational costs and new business models in the long run". Market participants and capital get locked up due to huge inefficiencies and opaque processes. For example, Bloomberg reported that investors committed $1.2 billion in October 2013 to fund a loan for a junk-rated firm and didn't get any interest for more than 10 months. This example nicely portrays some of the examples the industry is facing (Capgemini Consulting, 2016b). Additionally, we can see common issues of traditional financial contracts in the Figure 24.

Figure 24: Problems of traditional financial contracts



Source: Capgemini Consulting (2016b).

As mentioned above, smart contracts can be implemented on a blockchain or on a non-distributed ledger system. When using a properly secured blockchain, we can make it impossible for a single group or party to reverse transactions once recorded in the database. This feature eliminates the need for trusted intermediaries which are usually needed to authenticate and settle transactions. Key features of smart contracts are: programmability, multisig authentication escrow capability, oracle inputs and automatic contract execution:

- **Automatic execution** of a smart contract based on programmed logic.
- **Multisig** – independently allowing two or more parties the approval of the execution of a transaction (this is a common feature for multi-party contracts).

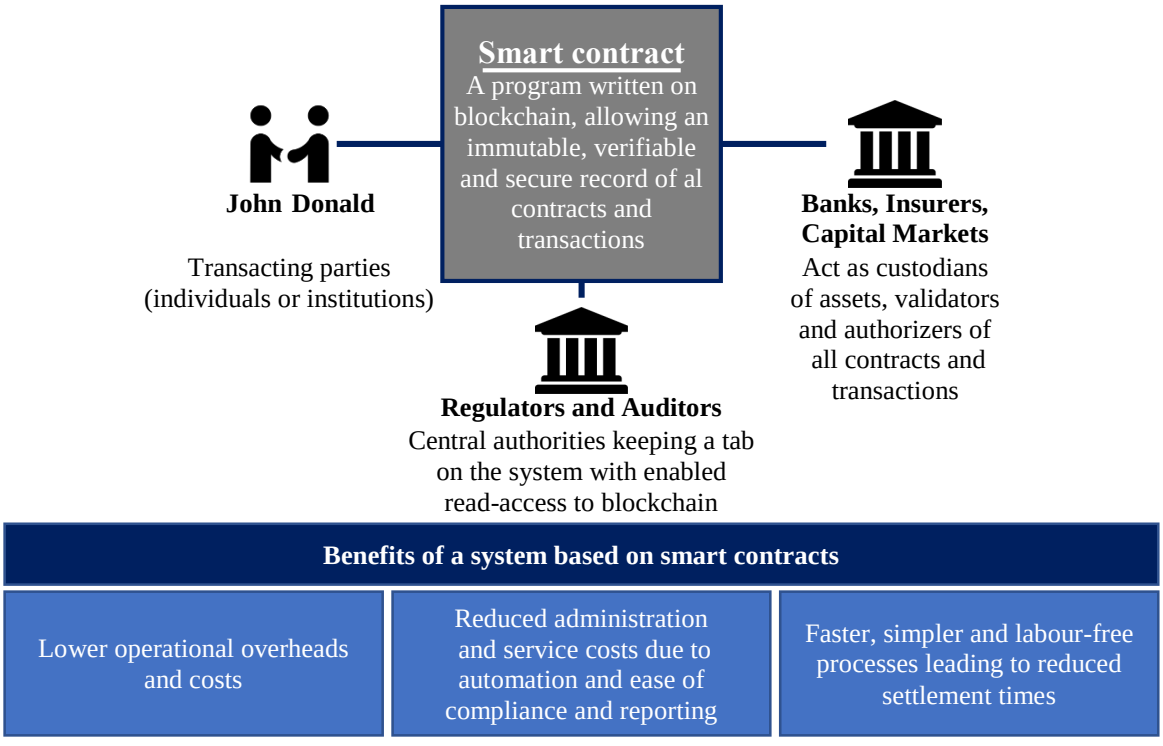
– **Escrow capability** – enabling the locking of funds by a mediator (e.g. a bank or an online market). Funds can be unlocked under conditions acceptable to contracting parties. Due to real-time processing of a smart contract, inputs such as prices, performance or any other outside real-world data can be used to process and verify a transaction. Additionally, one can use oracle services to get additional input for a smart contract.

Capgemini Consulting (2016b) believes that the financial services industry would benefit the most from smart contracts built on permissioned distributed ledgers, where the rules and permissions are granted to certain participants in the system in advance. For example, pre-approved banks can be granted rights to validate transactions, while the audit role could be given to regulators. A permissioned system assures a secure, private and scalable platform where all market participants (stakeholders) are connected:

– **The transacting parties.** Institutions or individuals intending to perform a transaction or enter into a contract.
– **Banks, capital markets players and insurers.** Their role could be tailored for a specified use case, and could act as a custodian or validator of assets for example.
– **Regulators.** They could be granted access to view or audit records of all transactions in the system.

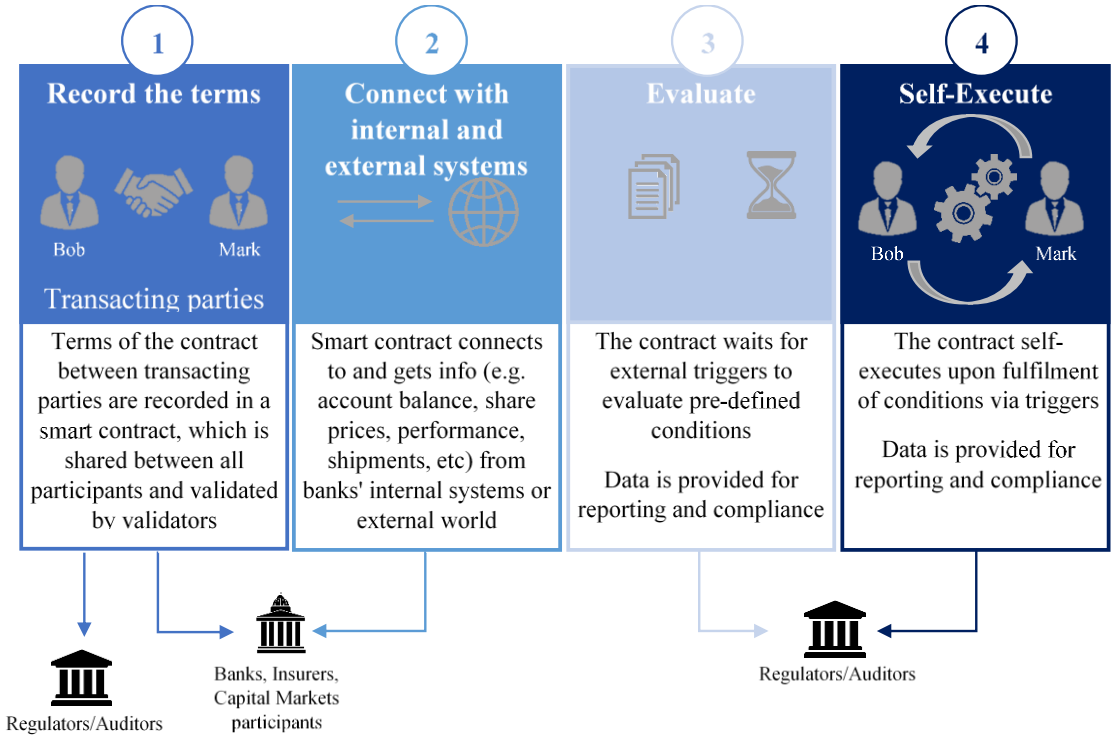
Smart contracts in practice (Figure 25) and smart contract lifecycle examples (Figure 26) can be found below.

Figure 25: Smart contract in practice



Source: Capgemini Consulting (2016b).

Figure 26: Lifecycle of a smart contract



Source: Capgemini Consulting (2016b).

As seen in Figure 27, smart contracts will offer significant value to all major segments of the financial services industry and will highly impact the following three key areas: risk reduction, cost savings, and enhanced efficiencies (with freed up capital). By putting the terms of a contract on a distributed ledger, certain business processes can easily be automated

Figure 27: Smart contract use cases in the financial services industry

Capital markets and investment banking	Commercial and retail banking	Insurance
▪ Corporate finance: • Initial public offers (IPOs) • Private equity ▪ Structured finance: syndicated loans, leveraged loans ▪ Stock exchange market infrastructure	▪ Trade finance: ▪ Supply-chain documentation, invoicing and payments ▪ Mortgage lending ▪ Loans and crowdfunding for startups and small and medium enterprises	▪ Automated claims processing (in motor insurance, house insurance, etc. ▪ Luxury goods fraud prevention ▪ New products: insurance for the sharing economy, autonomous vehicles, peer-to-peer insurance

Source: Capgemini Consulting (2016b).

in the short run. Embracement of common standards among market participants will probably lead to automation of entire processes and therefore eliminate huge costs associated with compliance, record keeping, verification, and manual intervention, making banks' process structure much leaner. For example, smart contracts offer its use in various segments of the financial and insurance industry:

- **Reducing syndicated loans settlement time, leading to savings and additional loan growth.** High-yield bond trades are currently settled in T+3 days, while the settlement period for leveraged loans takes up to 20 days. Leveraged loan market is therefore swathed by massive risks and liquidity challenges. Since 2008, the high-yield bond market grew by 11 %, while the leveraged loan market witnessed decline. Capgemini estimates that smart contracts could reduce settlement times for the latter to the range of T+6 to T+10 days. Delays in documentation processing, buyer and seller confirmation, assignment agreement as well as KYC, AML and FATCA checks could be greatly reduced with the help of a permissioned ledger, making liquidity in the market much higher. If the growth of leveraged loans can be at least half that of the high-yield bond market (i.e. between 5 % and 6 %), it would amount to additional $149 billion loan demand in the market. As those loans typically carry 1 % to 5 % underwriting fees, $1.5 billion to $7.4 billion could be added to the income of investment banks. Not only that, shortening of the settlement cycle could greatly reduce operational costs, regulatory capital requirements as well as costs associated with delayed compensation payments during the settlement of leveraged loans.
- **Assets transfer – tokenization of different asset classes.** The blockchain offers many advantages to today's generally less liquid markets of various asset classes such as real estate, land, special commodities or similar. For example, let's imagine buying a piece of commercial real estate. As we all know it, this process is pretty complex and takes time as many different intermediaries are included. Banks, escrows, lawyers, insurers, regulators, tax authorities, inspectors and title companies are all included in the complex transaction, making average closing time nearing 60 days. The commercial real estate industry's market information is tightly controlled by institutional investors, brokerage firms, market data providers and investment brokers, which are playing a crucial role acting as the information intermediary between buyers and sellers. The factors above, administrative and legal hurdles are making transactions of commercial real estate very slow and costly. Blockchain, with its smart contracts features, gives us the opportunity to "tokenize" real estate assets. The purpose of a smart contract on a blockchain is to retain a permanent history of all real estate transactions, which can in retrospect easily be retrieved, verified and audited. Property titles, ownership histories and the value of the property are represented on the blockchain by a token. Commercial building can be assigned a digital address (via a smart contract), containing real-time occupancy information, physical characteristics, legal status, historical performance as well as the financial position. Tokenization can lead to global dissemination of data and can, more importantly, lead to use of new monetization tools with a global audience. As the real

estate data becomes more available, investors will have a much easier time evaluating potential acquisitions. Investment brokers will lose their information asymmetry advantage and could be totally avoided when pricing buildings (Malviya, 2017).

- **Smart contracts can enable leaner and innovative insurance products.** Smart contract can be used to for automatic triggering of reimbursements based on data acquired from the internet or from physical sensors. Premium compensation and risk assessment could be done automatically as blockchain could provide a shared ledger which contains person's history record (previous claims, medical history, etc.). Furthermore, smart contracts enable peer-to-peer and micro-insurance products where policies and covers are automatically activated or deactivated based on data collected by various sensors. This in turn this massively speeds up claims processing and reduces operating costs of insurance companies.

The technology and development capabilities around smart contracts are evolving rapidly. Existing smart contract functionalities as multi-signature payments, escrow services, as well as others are already in place, yet there are still various challenges that need to be overcome before we see smart contracts in the mainstream use. They are:

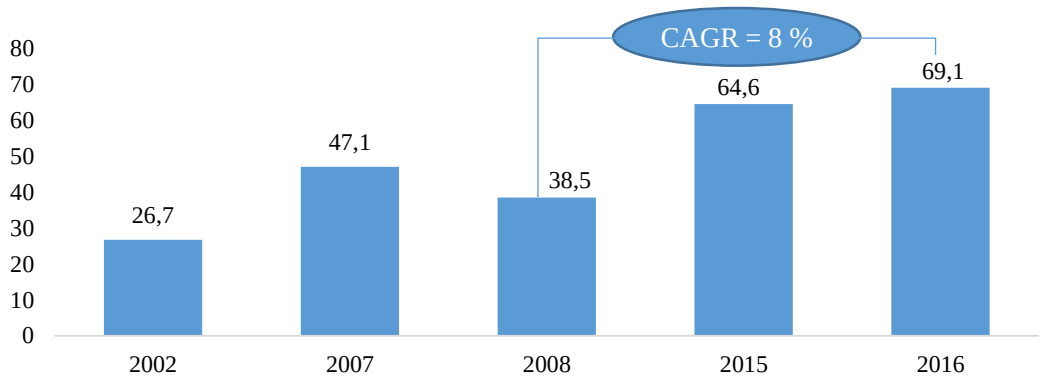
- **Scalability of transactions and speed of execution.** As more and more industry infrastructure relies on distributed ledger technologies and the amount of transaction grows, high throughput will be required in order to keep pace with many of existing today's applications.
- **Interoperability with external data and legacy systems.** Should smart contracts effectively execute required functions, they would need to be fully integrated with the existing industry infrastructure and systems. High complexity and interconnectedness requirements raise significant questions about the effort and investments required.
- **Flexibility of contracts.** Real-world's contract modification features need to be further explored, making smart contracts upgradeable during the term of a contract.
- **Regulatory challenges.** Regulators are beginning to realize the potential of distributed ledgers and are starting to roll out various initiatives which will help in overcoming legal and administrative hurdles of smart contracts.
- **Privacy and security needs.** As the data on a distributed ledger can potentially be seen by all participants, industry participants (i.e. banks, brokers, insurers, etc.) will be reluctant to participate on a common smart contract platform should the privacy issues not be taken into account. Cryptographic key management and view/read permission grants will serve as key roles in solving these issues.
- **Governance.** Distributed ledgers model eliminates the need for a trusted intermediary, as the required authority is provided by the transparency and consensus among the participants. This will require that multiple market participants such as banks, consumers and regulators come together and agree on one common platform, which unambiguously outlies certain working standards, disputes resolution and limitations of liability.

The implications and potential of smart contracts is subject to much debate by key participants along the capital markets value chain. While they are promising to solve many of the problems associated with existing traditional financial contracts, certain development still need to happen before mainstream adoption happens. In order that financial organizations realize benefits of reduced risk, lower operating, administration and service costs, as well as more efficient business processes, careful evaluation and tailoring of strategy need to happen before the benefits of more competitive products and services can be brought down and increase customer experience (Capgemini Consulting, 2016b).

2.7 Investment management

Current environment of investment management (IM) is troubling asset managers as they face various challenges and pressures of their legacy business model. Industry's growth in revenues and total assets under management (AuM) has slowed significantly, while regulatory burdens and concerns over access to liquidity are rapidly rising. The global assets under management have been continuously rising since the crisis, with a CAGR of 8 % to $69.1 trillion in 2016 from $38.5 trillion in 2008 (Figure 28). Although the numbers seem nice on the surface, **the vast majority of the recent global increase in AuM was produced mainly by the increase in value of investments in mature markets**. The industry's lifeblood – net new flows – were standing at modest 1.5 % in 2016 and averaging 1 % in the after crisis period. Comparing to pre-2008 environment where annual inflows were at 4 % - 6 %, it seems unlikely that the growth will return to that levels. Although the global total assets under management grew, the pressure on margins in both institutional and retail segments remains and increases daily (BCG, 2017a).

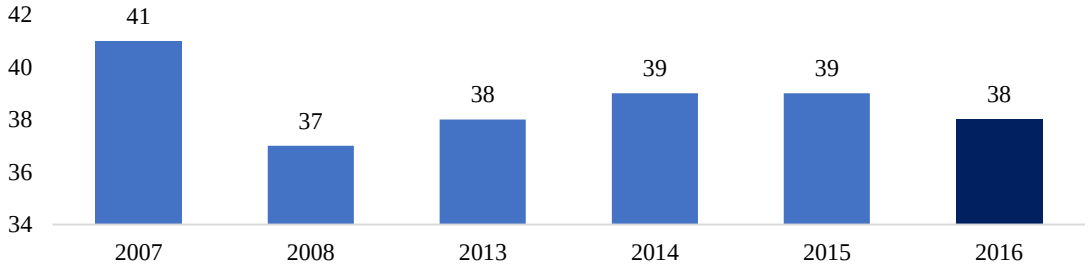
Figure 28: Growth of global AuM ($ trillion)



Source: BCG (2017a).

Although the industry has seen increase of total AuM, asset managers' revenues and especially operating profits margins did not follow suit (Figure 29).

Figure 29: Development of operating profit (% of revenue)



Source: BCG (2017a).

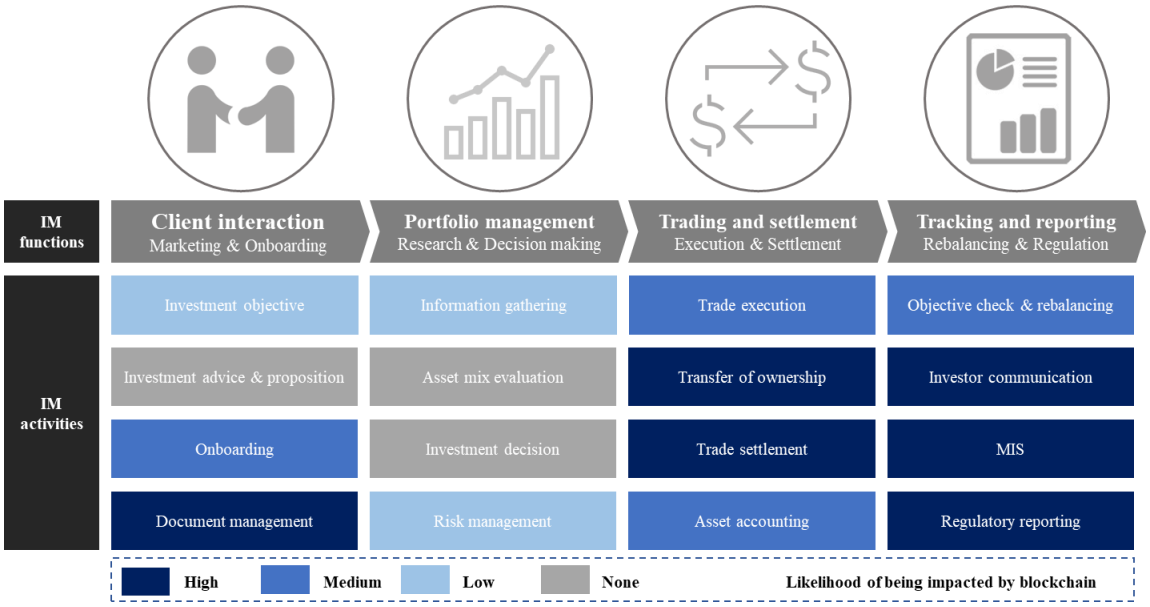
The decade long ongoing shift from active to passive management is causing revenues and margins to melt away. Not only that, fees have been declining for most products in both the retail and institutional segments – in institutional, the decrease is driven by competition among suppliers, while regulatory pressure for fee transparency and ban on distribution fees impacted the retail side (BCG, 2017a).

In an environment of uncertain market growth, weak net inflows and diminishing fees, industry players will have to tackle new challenges. To do so and to improve their bottom lines, asset managers are focusing on improving data management, upgrading their operating models and looking to provide continuing service improvements to their clients' pool (Oliver Wyman & J. P. Morgan, 2016). To be competitive in the future, asset managers will need to transform the way they work, through innovation and use of disruptive technologies such as artificial intelligence, machine learning, big data, analytics, and blockchain.

Figure 30 shows various activities along the value chain of investment management. In order to provide service to customers, every investment manager has to perform certain set of activities, out of which some are more likely than others to migrate to a blockchain infrastructure – processes requiring multiple parties granting approval, strong audit, compliance and regulatory oversight are more suited for adoption of blockchain technology.

Blockchain's ability to store clients' data – profile data, preferences, net worth, account information, risk profile – can greatly affect current IM value chain. Document management, trade settlement, transfer of ownership and investor communication are burdensome, time consuming and costly processes today. Current strict on boarding requirements, when customers separately provide proof of identification, residency, marital status, sources of wealth and occupation can be greatly enhanced with the blockchain technology. Instead of waiting for days or weeks to collect the data, investment management firm will be able to access a blockchain ledger containing public profile of its prospective customer. After successful client onboarding, the system will enable easy audit trail for tracking changes. Burdening Regulatory reporting and current Trade settlement process that can take up to 7 days will also be among most impacted by the blockchain's arrival.

Figure 30: IM value chain impact



Source: Deloitte (2017).

Among before mentioned benefits of the distributed ledger, investment management industry will be able to account transactions and trades easily. Transfer of assets will be done instantly and without the use of a third party. In addition to quick on boarding, investors will be able to receive near-real-time performance of its portfolio and portfolio risk data, giving them better insight to understand their positions and exposure, thus enabling of up to minute value creation updates (Deloitte, 2017). This greater transparency will, as Oliver Wyman and J.P. Morgan (2016) expect, return trust into investment management industry, which was involved in a litany of scandals and appears to be the least trusted of all financial services firms.[13]

Others, more forward looking technology evangelists, say that blockchain offers opportunity to create "super liquidity" events through opening up of capital markets to participants in developed or non-developed countries. Adding up to total value of traditional asset classes, borderless and digital nature will help establish a ledger of connected IoT devices, connecting 30 billion value creating objects with capital markets around the world.[14]

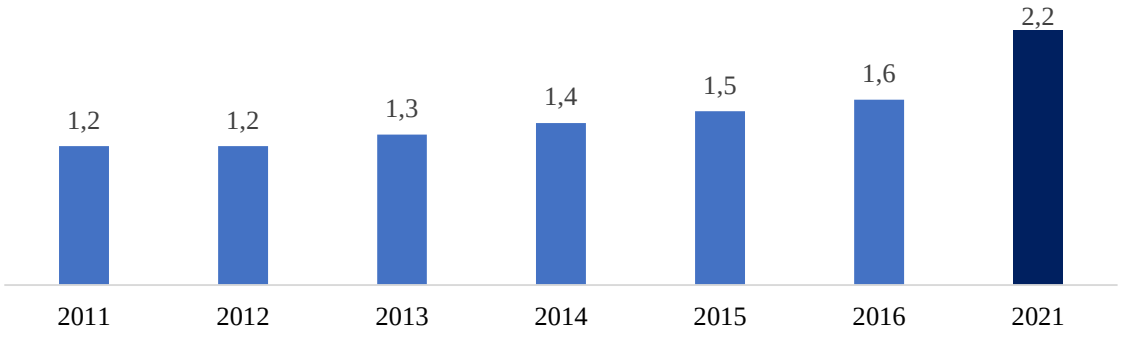
[13] Fund Managers are the least trusted among a group of different organizations, with only 12 % of responding customers trusting this type of organization (PricewaterhouseCoopers, 2014b)
[14] IoT stands for Internet of Things. McKinsey & Company (2014) predicts 30 billion objects will be connected to the IoT by 2020.

3 EMPIRICAL ANALYSIS OF POSSIBLE REDUCTIONS IN FEES AND POTENTIAL REVENUE SOURCES FOR MAJOR SEGMENTS OF FINANCE WITH FOCUS ON TRANSACTION, CLEARING AND FUNDRAISING FEES

3.1 Transactions

The sheer size of global payments industry is enormous and represents more than 34 % of overall banking revenues. BCG (2017b) estimates that the value of global payments transactions in 2016 stood at $420 trillion – or 5.5 times global GDP. With a CAGR of more than 5 %, global payments revenues will reach $2 trillion dollars by 2020 (Figure 31) (McKinsey & Company, 2017).

Figure 31: Global payments revenue ($ trillion)



Source: McKinsey & Company (2017). At fixed 2016 $ exchange rates.

3.1.1 Card payments

Like described above, the majority of the current card payments industry is based on the so called four-party model. By design, this model is overwhelmed with intermediaries, and each of them adds to the total fee of a card payment. Merchant acquirer fee, network fee and interchange fee all add to the high fees that equal to 2 % of the total payment. A four-party system adds three extra intermediaries – layers of friction – between the merchant and the consumer, giving rise to criticism that transaction costs are too high.

I will, for the sake of this paper, focus on merchant acquirers and their revenues. Out of the 2 % total fee to the merchant, merchant's bank or a specialized merchant acquirer takes home on average 0.35-0.4 %, while the rest gets split between network and interchange fees. Merchant acquirers in the United States and Europe combined processed almost $8.7 trillion worth of transactions in 2017 (Table 1). Should merchant acquirers be totally eliminated,

Credit Suisse's estimate of a 0.6 %[15] average net take implies revenue cutting opportunity of almost $52 billion per year.

Table 1: Revenues of merchant acquirers in US and EU in 2017 ($ trillion)

Region	Top acquirers in US and EU (Total value of transactions, 2017)
United States	5.76
Europe	2.81
Total	8.57

Source: The Nilson Report (2018a & 2018b).

Blockchain's technology offers two possible use cases where traditional card payments system is disrupted. Firstly, Bitcoin or a similar unpermissioned public ledger cryptocurrency gains traction as a payment vehicle and disintermediates the traditional four-party system. Secondly, a version of a permissioned (either public or private) ledger is implemented: ability to see transactions can be granted to anyone, yet only permissioned actors can participate in the consensus forming process. To grant for success of the ledger, only companies with vested interest in the network should have the ability to form transactions.

Although card networks currently are very efficient, safe and enable almost seamless customer experience, I believe there is enough space to drive current 2 % fees down. This reduction mainly comes from margin squeeze of especially merchant and cardholder's bank, although total disintermediation of the current four-party system might also happen in the long term.[16] Blockchain does not help reduce settlement speed and fees of domestic payments only, global and instant micropayments enabled with a mobile phone become a possibility as well. But before that happens, several issues will need to be solved. Firstly, the market will have to determine who is going to pay for the consensus mechanism, and secondly, scalability and customer experience needs to match at least that of the current infrastructure.

3.1.2 Cross-border payments

Cryptographically secured tokens of value that can be transferred between parties without the need for a central counterparty hold lots of promise for the world of international payments. They allow for seamless and easier transactions and offer more scalable and cost-efficient provisioning of FX liquidity, where a bank doesn't need to open and maintain many

[15] Credit Suisse (2016) estimate.
[16] Disintermediation is already happening in China where mobile payment apps AliPay and WeChat Pay combined hold more than 90 % of the market share in the payments market that is increasingly becoming mobile only (Business Insider, 2018).

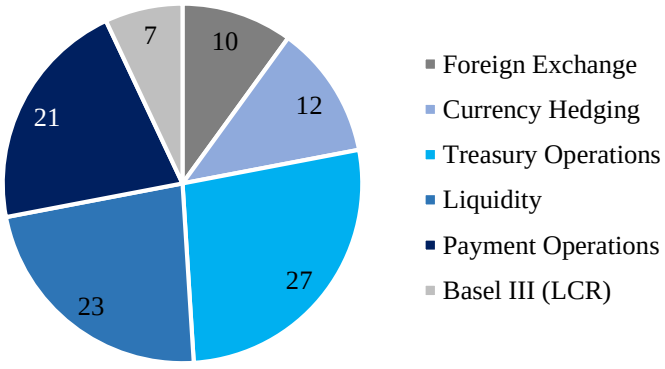
bank accounts across the world. Current infrastructure is structured in a way where respondent banks are charged big marked up spreads and processing fees. They also have to maintain minimum required levels of capital in nostro/vostro accounts around the world – trillions of dollars trapped under such arrangements represent huge opportunity costs for the participants.

Ripple offers to solve this solution by enabling real-time borderless value exchange by providing liquidity on demand and reducing costs associated with treasury, payments operations, liquidity and regulatory requirements. To make markets with any currency, banks can hold Ripple's digital asset[17] on their own balance sheets, and thus don't need to hold nostro accounts when sending value across the world. Instead, banks should consolidate liquidity into one pool, thus only making markets between its domestic currency and globally distributable digital asset (often referred as a "Universal Bridge Asset").

For processing cross-border payments, banks currently incur substantial infrastructure costs of: i) FX spread; ii) the cost of hedging a basket of currencies held in nostro accounts worldwide; iii) treasury costs; iv) liquidity costs of the locked-in capital as well as costs of the time to fund nostro accounts; v) payment operations such as manual interventions and error handling; and vi) regulatory (i.e. Basel III requirements) costs of minimum liquidity coverage ratios. A typical cost breakdown is shown in the Figure 32.

Let's now evaluate potential implications and cost savings of a blockchain based infrastructure. We will use Ripple's example and consider its digital asset as a universal bridge asset. Currently, settlement delays and complex correspondent banking infrastructure lead to high operational costs – or 20.9[18] basis points on total payment volume (Figure 33).

Figure 32: Cost breakdown of international payment servicing (% of total)

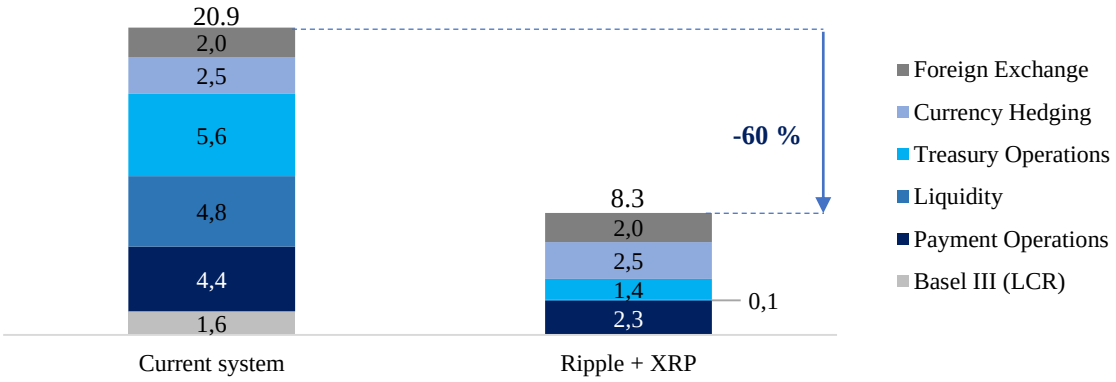


Source: Ripple (2016).

[17] Ripple's digital asset known as "XRP" (Ripple, 2016).
[18] Ripple's (2016, p. 7) estimate.

Should a representative bank use Ripple's payment infrastructure and should it convert 50 % of its payment related-float into XRP (while custodying XRP itself), then, since XRP is volatile as a new asset, only currency hedging cost would increase in the start. As institutions get to use and trade XRP widely, this volatility is expected to compress down, leading to total cost savings of 60 % compared to current system.

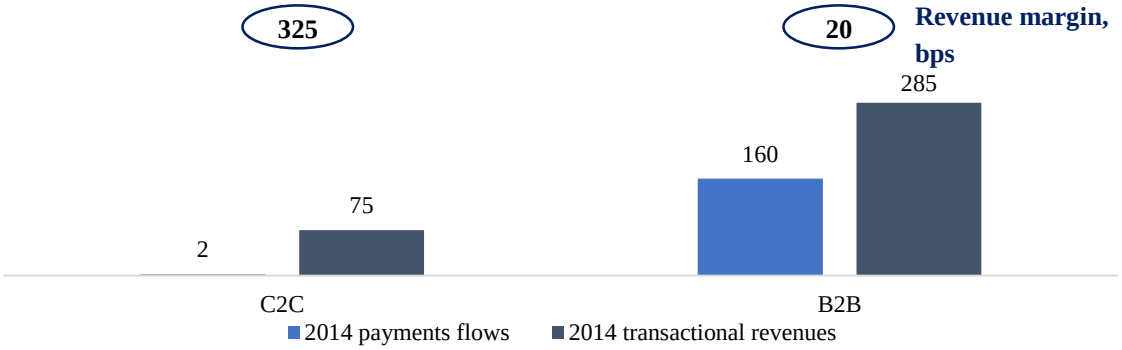
Figure 33: International payment infrastructure's cost reduction using blockchain based system (basis points)



Source: Ripple (2016).

Borderless and non-siloed blockchain's structure removes redundant liquidity and operations costs since banks do not require multiple nostro accounts. This further removes the need for expensive operational overhead and simplifies cash and account maintenance costs, leaving only foreign exchange spreads and currency hedging costs unchanged (Ripple, 2016). Although Ripple's model only considers cost reduction, I will, for the sake of estimation, use described proposal and assume that competition will equivalently drive down revenue margin of cross-border payments.

Figure 34: Cross-border payments flows ($ trillion) and industry revenues ($ billion)

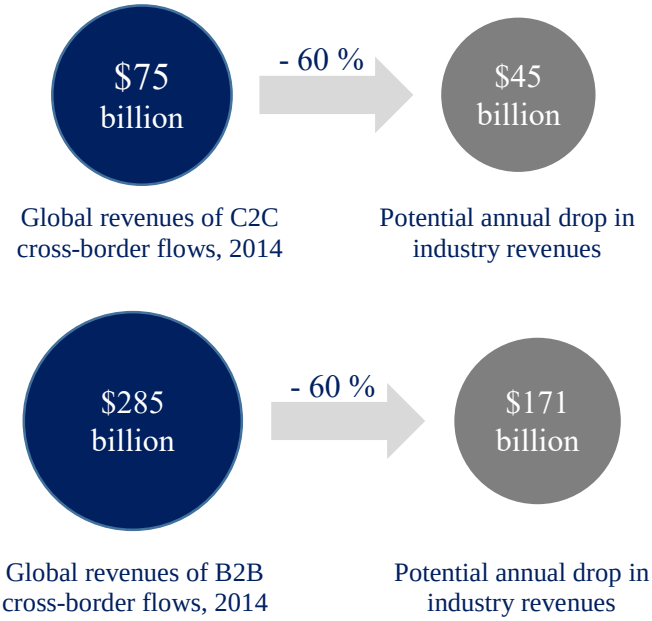


Source: McKinsey & Company (2016).

Consumer to consumer cross-border payment flows in 2014 were $2 trillion and business to business flows were $160 trillion. Although cross-border payments represent only 20 % of

global payment flows they represent 50 % of all transactional revenues. Healthy revenue margins of 325 basis points for consumer to consumer (C2C) payments and 20 basis points for business to business (B2B) payments led to industry revenues of $75 billion in C2C and $285 billion (Figure 34) (McKinsey & Company, 2016). When applying Ripple's proposed reductions, we get a potential annual $216 billion cut in cross-border industry revenues (see Figure 35).

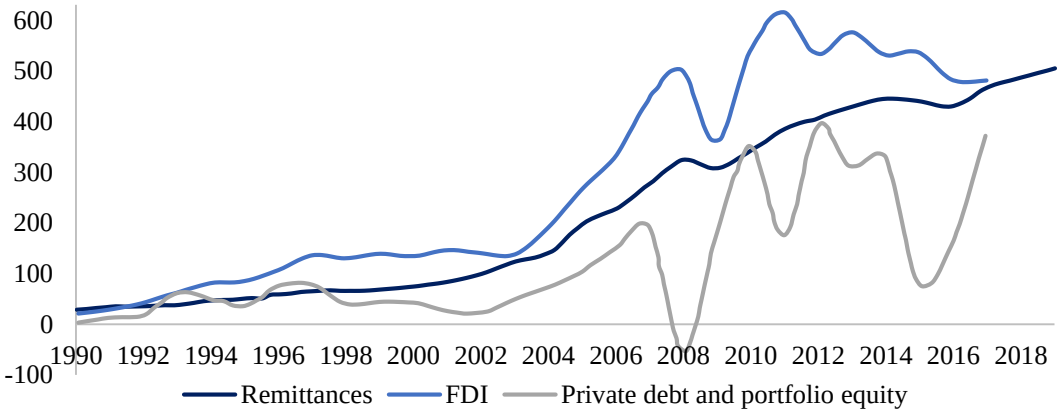
Figure 35: Annual cross-border industry revenue cut



Source: McKinsey & Company, 2016; Own work.

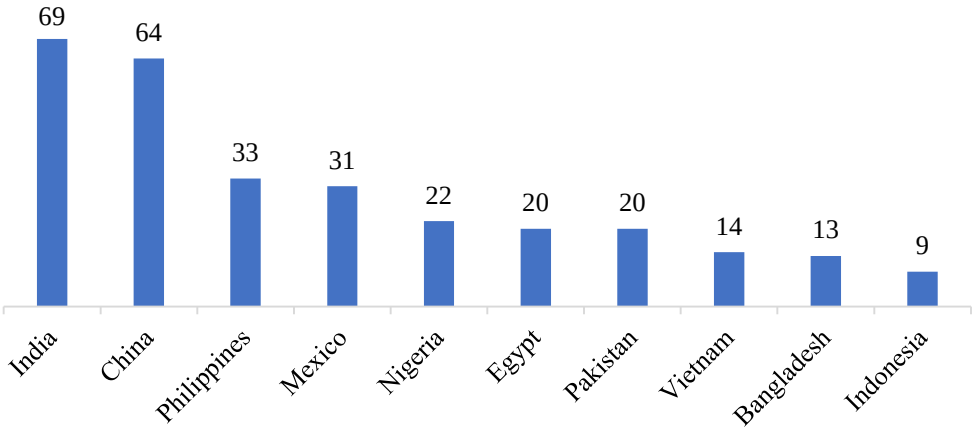
Figure 36 shows the sheer size of remittance flows. More than $613 billion funds were transferred in 2017. Middle and low income countries received more than two thirds of all remittances – especially important is the Asia Pacific region (APAC) region (Figure 37).

Figure 36: Development of remittance flows globally ($ billion)



Source: World Bank Group (2018). Data for 2017 and onwards are projections.

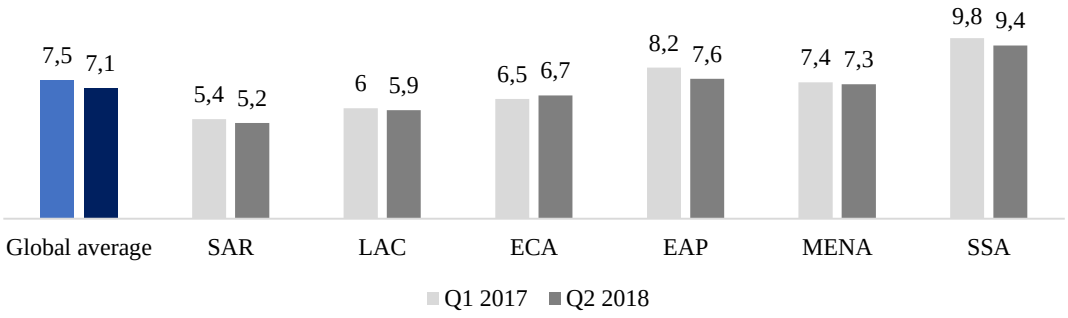
Figure 37: Top remittance receivers in 2017 ($ billion)



Source: World Bank Group (2018).

The cost of sending money according to the World Bank's Remittance Prices Worldwide Database remained high and stands at 7.1 % in 2018. Figure 38 below shows the cost to send $200 and compares global regions and average in Q1 2017 and Q1 2018.

Figure 38: Cost of sending $200 (% of total payment)



Source: World Bank Group (2018). EAP = East Asia and Pacific; ECA = Europe and Central Asia; LAC = Latin America and the Caribbean; MENA = Middle East and North Africa; SAR = South Asia; SSA = Sub-Saharan Africa.

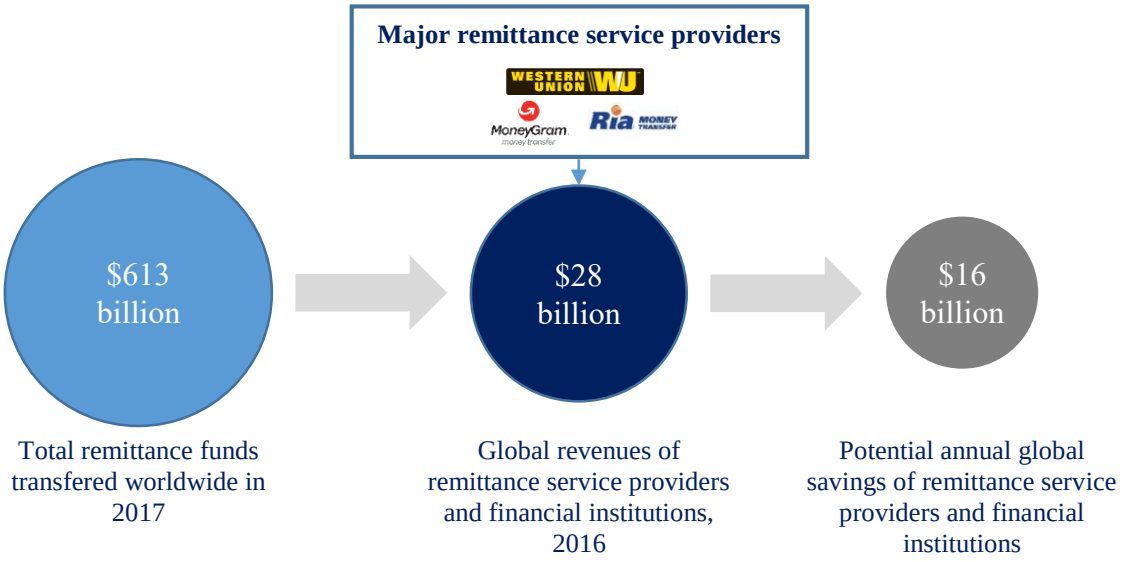
Some cost corridors across many African regions, small islands and APAC remain above 10 % of the total payment, mainly due to low volumes of formal flows, inadequate penetration of new technologies and lack of a competitive market environment. In some regions numbers are reaching 18 %[19], which is almost unimaginable in today's modern and interconnected world (World Bank Group, 2018).

McKinsey & Company (2017, p. 7) estimates global revenues of specialist RSPs and other financial institutions providing remittance services at $28 billion in 2016. Recent results of

[19] It costs more than 18 % to send money from South Africa to China for example. It is even more surprising that the cost of sending a payment from UK to Bulgaria or Albania is close to 10 % (World Bank Group, 2018).

Ripple's blockchain infrastructure show possible savings between 40 – 70 % on remittance payments which can be passed down to consumers (Ripple, 2018). Therefore, if we use Ripple's estimates and use an average savings rate of 55%, we get a potential cost cut in the amount of $16 billion per annum (Figure 39) – an amount which can help migrants worldwide send money home much more efficiently.

Figure 39: Market opportunity and potential cost savings in remittance industry



Source: McKinsey & Company, 2017; Own work.

3.2 Fundraising

Digitized and automated smart contracts on blockchain based platform enable smart securities and offer the following benefits:

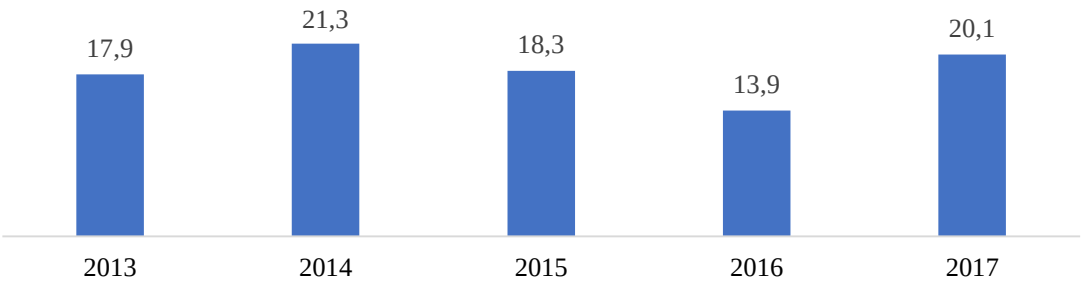
- Settlement risk exposure can be reduced by over 99 %, thus dramatically lowering capital costs and systemic risk
- Quick and efficient clearing and settlement processes enable huge industry savings
- Remove counterparty risk as settlement happens in real time
- Traceable and auditable transactions, with system available 24/7
- Operational costs of manual processes are greatly reduced
- Reduced cost of issuance due to removal of third-party intermediaries and the fees associated with them
- Faster and cheaper capital market transactions

Blockchain allows for automated issuance process. Still, the issuer has to appoint an investment bank as a book-runner, which is responsible for placing new equity, debt or any other security issue with investors. Digitized placement of securities enables near real-time book building process where the Master Book is available for all participants in the

blockchain. Blockchain's single version of truth removes the need for internal and external reconciliation, thus cutting manual effort and reducing the entire book building time by about 35% to 50% (Capgemini Consulting, 2016a).

We have to look at the revenues investment banks around the world generate when evaluating blockchain's use case in the book-building process. Forbes estimates total global equity underwriting fees to be at $20.1 billion in 2017 (Figure 40).[20]

Figure 40: Global equity underwriting fees ($ billion)



Source: Forbes (2018).

Since blockchain technology does not require any reconciliations and allows for direct dealings between issuers, syndicate members and the investment banks, the sales team of the investment bank involved can steadily be eliminated. Half of the 7 % average underwriting fees for an equity IPO is charged as a commission for the investment bank's sales team. So, when taking removal of the sales team into account, the underwriting fee gets cut by half and implies global savings of $10 billion per annum (Figure 41).

One could argue that the quality of service would deteriorate when the sales team is completely removed. I agree with that and think that the best solution will encompass only a small portion of today's workforce.

Figure 41: Potential annual savings in the book-building process

Source: Forbes 2018; Own work.

[20] See Forbes (2018).

3.3 Clearing – US cash equities

I will use US cash equities market example to show blockchain's potential impact in post-trade settlement and clearing process. Removing duplicative and often manual reconciliation of trade data across buy-side clients, broker-dealers, trust/custody banks, and the DTCC can help bring massive savings to market participants via lower headcount and lowered back office costs. On the other side, this effect is not going to translate to execution venues as price discovery, anonymity and the need to match counterparties will still be required. In fact, this process is already quite efficient today. And although blockchain represents risk to a certain slice of revenue of both banks and clearing houses, they are expected to leverage the technology and will still have to play a strong role in the ecosystem for the foreseen future.

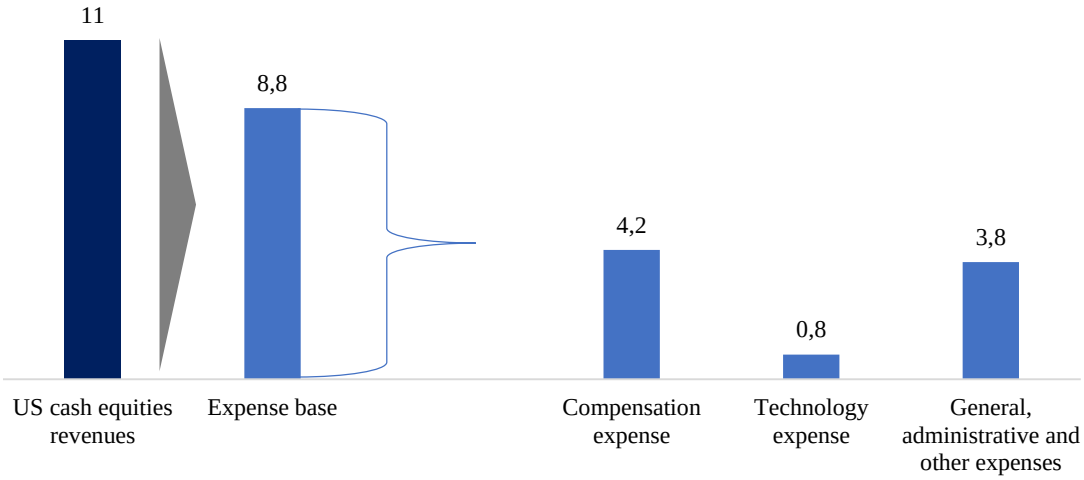
Depending on the type of order and the type of a client (institutional trade, retail trade, etc.) the current process flow of a US cash equity trade can take different paths. Still, DTCC serves as the central securities depository and central counterparty where all equity trades in the US are processed, held, cleared and settled. Once a buy-side investor seeks to buy stock, order details are sent to their broker/dealer(s), which then directs that trade to one or several exchanges for execution. Once an order gets executed on an exchange, the trade confirmation and details are sent back to the executing broker. Once the client and broker/dealer agree on a trade, the trade details are sent to DTCC and are shared with custody banks (who are DTCC's clearing members). Following that, both parties adjust their books to reflect the trade and upcoming settlement of securities for cash.

6.4 billion trades per day in 2017 were traded in the US cash equities market, making it the most traded equity market in the world. Blockchain offers to deliver cost savings to two primary areas across US cash equities: operating expenses (back office, headcount, systems and clearing) and capital requirements (Goldman Sachs, 2016). For the sake of this thesis I will try to evaluate potential cost savings from reduced operating expenses only.

Goldman Sachs (2016, p. 47) estimates that the global equity trading revenue pool stood at $47 billion in 2015. US equity trading revenue accounts for roughly 23% of total or $11 billion annually. Typical 20% pre-tax margin implies approximately $8.8 billion in expenses within US cash equities businesses. Taking 38%[21] as an industry average compensation-to-revenues ratio gives us $4.2 billion in estimated industry compensation expenses. Banks on average spend 7% of revenue on technology, implying approximately $0.8 billion in total technology expenses. The rest gets split between general, administrative and other expenses (Figure 42).

[21] See New Financial (2016).

Figure 42: US cash equities revenues, expense base and composition ($ billion)



Source: Goldman Sachs, 2016; Own work.

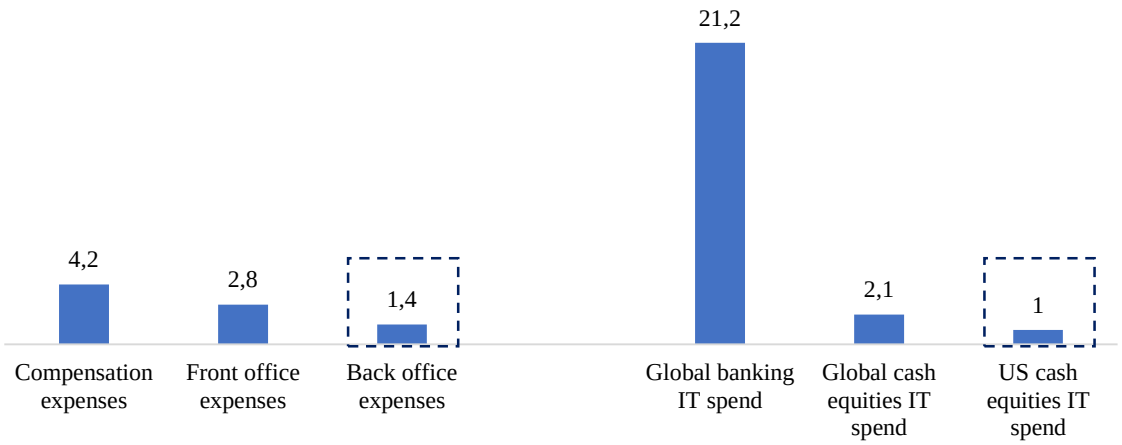
Blockchain's main promise is to reduce resource spend needed to settle and clear transactions. Major savings are expected to occur when the technology is fully implemented as the need for manual reconciliations is greatly reduced. Therefore, market participants should see main improvements in overall compensation and IT expenses.

Industry's back office expenses account for approximately one third of total compensation expenses, or $1.4 billion. The rest goes for front office expenses. I use Goldman Sachs's estimate when deriving total IT spend that is related to US cash equities clearing and settlement. Goldman estimates that roughly 10% of $21.2 billion of total IT spending for the banking sector in 2015 is related to equity trading globally. US cash equities account for 50% of that spend, or $1 billion. Hence, when we combine both we arrive to annual expense base of $2.4 billion that can be streamlined with blockchain's implementation (Figure 43).

Manual reconciliation and manual data entry account for the majority of back office costs (requiring both labor and IT resources). In my opinion, blockchain's distributed nature of information can derive greatest efficiencies in those areas as the whole chain of market participants shares the same platform where data does not require any manual intervention. Therefore, I think that the vast majority of those costs can be totally eliminated, potentially saving at least 30% to 50% per annum. This equates to approximately $0.7 billion to $1.2 billion in back office and IT spend savings per year, or to roughly 8% to 14% of the estimated total cost base in US cash equities trading.

Since counterparty and settlement risks are greatly reduced, I believe blockchain could also bring substantial savings by reducing the aggregate amount of capital required at clearing houses. Goldman Sachs's (2016) estimates that such savings could amount to $500 million per annum.

Figure 43: Estimated potential reductions in back office expenses and US cash equities IT spend ($ billion)



Source: Goldman Sachs, 2016; Own work.

Overall, when we combine savings from both areas, we get approximately $1.2 billion to $1.7 billion in total savings of both lower capital requirements and reduced expenses (labour and IT). Even though estimates show healthy reductions, the real effect remains to be seen and will be heavily dependent upon the scope of technology's successful implementation.

4 CURRENT BLOCKCHAIN APPLICATIONS AND MAJOR PLAYERS

4.1 Digital Asset Holdings

Digital Asset Holdings is building blockchain based products for use by regulated financial institutions such as financial market infrastructure providers, CCPs, CSDs, exchanges, banks, custodians and other market participants. Their platform called Digital Asset Platform (DA Platform) offers to provide a common infrastructure on which various financial services applications can be built. Their main value proposition is to mutualize financial market infrastructure across different distinct market participants, while maintaining confidentiality and scalability that are needed for large and regulated markets.

Permissioned DA Platform aims to eliminate discrepancies between different and duplicative siloed data records, thus reducing current latency, errors, risk, cost and capital requirements involved in processing financial transactions – and thus giving regulators true market transparency. Each participant in the infrastructure utilizes network-wide, replicated blockchain log and can create its own subsection of the ledger.

Up till now, Digital Asset Holdings announced several projects with regulators and household corporates:

- **Australian Securities Exchange (ASX).** ASX selected Digital Asset as a partner to develop a CHESS (Clearing House Electronic Subregister System) private blockchain based replacement system. After successful preliminary testing, ASX gave green light to substitute CHESS, the core system performing processes of clearing, settlement, asset registration and other post trade services in the Australian market.
- **Depository Trust & Clearing Corporation (DTCC).** After a successful proof-of-concept, DTCC and Digital Asset Holdings proceeded with further steps in developing a clearing and settlement solution for repo transactions.
- **SIX Securities Services (SIX).** Developed a blockchain based solution for the Swiss financial market covering the entire bond life-cycle – from issuance to settlement.

The company formed strategic relationships and received more than $115 million in funding from leading global companies such as Accenture, Citi, CME Group, Deutsche Börse Group, Goldman Sachs, IBM and JP Morgan Chase (Digital Asset Holdings, 2016).

4.2 Ripple

Ripple Labs is a San Francisco based company that is developing the Ripple payment protocol and its coinciding exchange network (i.e. RippleNet), which will connect banks, payment providers and digital asset exchanges (Figure 44). Home to its decentralized native digital asset "XRP", Ripple protocol enables real-time gross settlement system, currency exchange and remittance payments. Ripple was initially released in 2012 and its network now enables secure, instant and almost free world-wide transactions of almost anything of value - fiat currency, cryptocurrency, commodity, stocks or even mobile minutes.

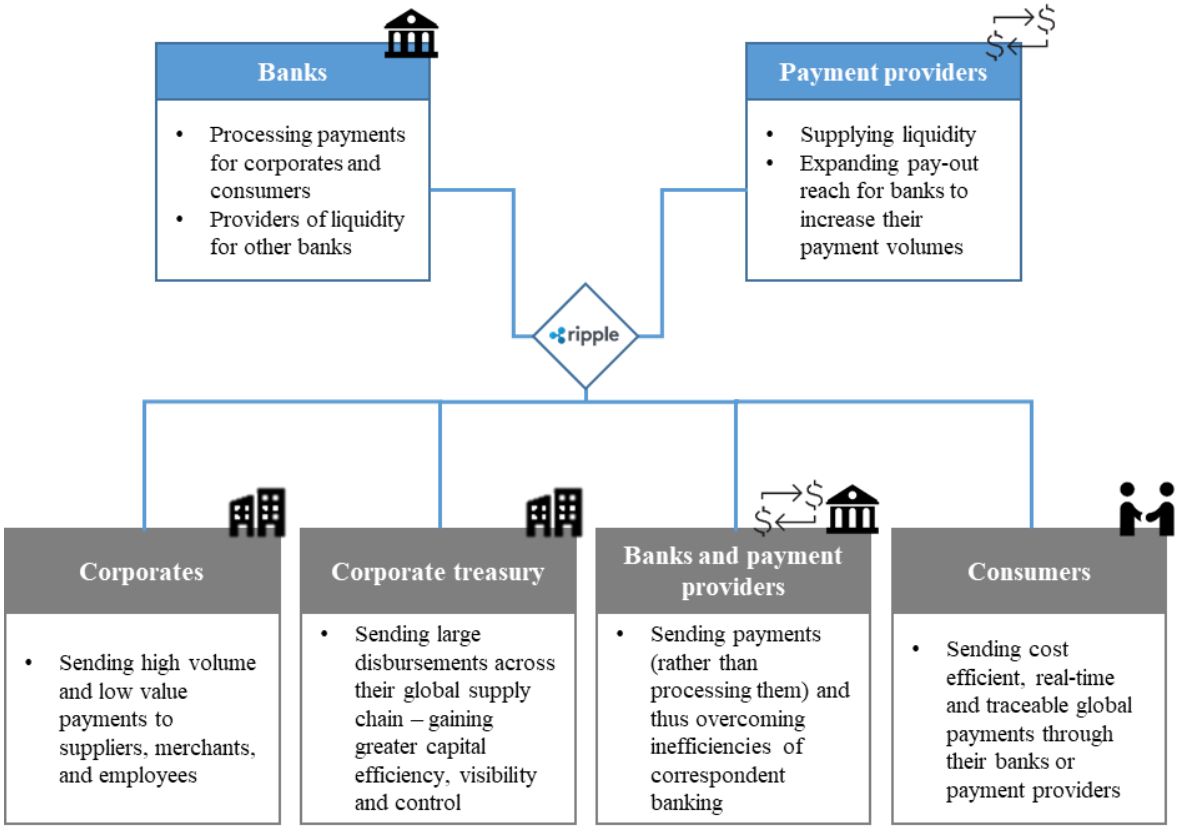
RippleNet is a decentralized network based on agreement between Ripple and network participants. All parties benefit from usage of the same standardized technology and infrastructure that provides real-time messaging, clearing and settlement of transactions. Two key groups exist in the RippleNet system and use its infrastructure: Network members as enablers of RippleNet and Network users as customers (i.e. originators) of RippleNet.

Its network operates as a permissioned public ledger, whose validators are 55 preselected companies such as Microsoft, MIT, WorldLink, Bahnhof (Swedish ISP), AT Tokyo Corporation, etc.[22] Validators confirm transactions that meet protocol requirements and have the same cost of running as an email server (in terms of electricity consumption). More than 100 household name customers are currently included and are using RippleNet – Royal Bank

[22] Data as of July 17, 2017. See Ripple (2017).

of Canada, American Express, Santander, Standard Chartered, UniCredit, Crédit Agricole, etc (Ripple, n.d.).

Figure 44: RippleNet's two key groups



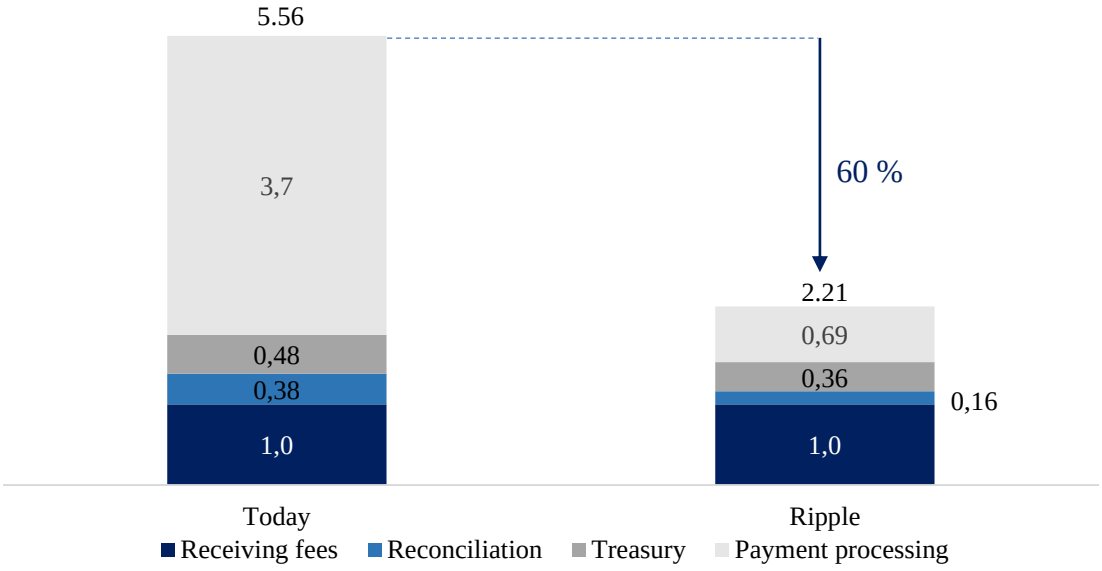
Source: Adapted from Ripple (n.d.).

Opposite to current inefficient and batch payments that result in high processing costs, lengthy settlement times and deliver poor customer experience, Ripple offers to deliver an efficient, on-demand infrastructure where payments are settled in real time, hence removing settlement risk and ensuring transaction certainty. This promise, with data rich messaging between all transacting parties, should enable high volume, low value individual payments and thus help mitigate disintermediation from online, non-bank payment providers.

Ripple claims its system can reduce operational costs for cross-border payments for up to 60% compared to legacy systems. Figure 45 shows Ripple's estimation of a reduced total cost per payment for a sample bank or a payment provider.

RippleNet further offers banks to source liquidity on demand and in real time, without having to pre-fund nostro accounts. To compete with modern payment infrastructure, Ripple currently handles 1,500 transactions per second, 24x7, and promises to scale its throughput to handle the same as Visa (Ripple, 2016).

Figure 45: Ripple's estimated total cost per payment reduction (basis points)



Source: Ripple (2016). Modelled use-case. Annual payment volume: $100 million; Number of annual payments: 200,000; Average payment size: $500; Cost corridor: CADUSD.

4.3 Ethereum

Ethereum is an open-source, public blockchain based distributed computing platform offering smart contract functionality. It is home to the second biggest cryptocurrency per market cap Ether, which is used to compensate participant mining nodes and can be transferred between different accounts. It was proposed by Vitalik Buterin in 2013 and has seen value of its native token Ether rise for more than 14,000% from start of trading.[23] Ethereum is designed to operate as a decentralized platform that runs smart contracts and dapps (i.e. distributed applications) without any possibility of downtime, censorship or third-party interference. It gives everyone opportunity to create a tradeable digital token that can be used as a currency, a representation of any (physical) asset, a virtual share or a proof of ownership of virtually anything. Blockchain's functionalities offer a shared global infrastructure that can move value around and represent the ownership of property in a totally decentralized way. While project gained lots of early praise for the technical innovations of Ethereum, questions about its security and scalability were also raised.

Ethereum has seen remarkable use of its smart contracts functionality recently as more than 4000 ICOs emerged globally. Some of the biggest are Augur, Raiden, OmiseGo, Golem, Iconomi, Basic Attention Token and have used decentralized infrastructure to "tokenize" securities, dividends, collateral deals, voting systems or have "tokenized" real commodities such as gold or silver. Crowd sales and auctions were used to sell virtual shares in real or blockchain organizations or to pre-sell products. Funds locked in smart contracts will be,

[23] See CoinMarketCap (n.d.).

depending on the outcome, released to the project owners or returned to the contributors – all using a trustless systems not requiring a centralized third-party arbitrator or a clearinghouse. Furthermore, as smart contracts enable voting, virtual and transparent organizations whose members vote on issues or perform shareholder voting are created daily. Not only it is possible to create a decentralized autonomous organization that is run democratically and has rules encoded in smart contracts, it is even possible to create own country (Ethereum Foundation, n.d.).

CONCLUSION

The blockchain technology is a significant invention and presents a creative way of information transfer. Not only is it an incorruptible digital ledger that can be programmed to record transactions of any kind, it can serve as an ultimate trust machine that has the ability to transfer virtually anything of value without the need for a single trusted intermediary. Chronologically recorded and cryptographically secured entries allow for efficient, permanent and immutable record of transactions. I believe Blockchain technology and systems built with its help will truly disrupt the financial industry and will bring greater transparency, simplicity and efficiency to the world of financial transactions.

Technology enables different versions of blockchain based money that is transferable in a decentralized peer-to-peer manner. Central banks have the opportunity to create a widely used blockchain based medium of exchange that can bring more transparency and efficiency in the current system. On the other side, privately issued cryptocurrencies that offer a truly disruptive way of value exchange and are governed by a distributed consensus could in the future potentially compete with to the ones issued by governments.

Transaction and information flows in clearing, settlement and payments are very opaque, time consuming, require significant amount of reconciliations and typically involve multiple intermediaries. I believe cryptographically-secured digital assets and shared ledgers can truly disrupt legacy infrastructure in those segments by bringing unprecedented cost-efficiency and thus eliminate huge revenue portions of various intermediaries should blockchain's broad-scale adoption occur.

Smart contracts will bring significant value to all segments of finance and will lead to high risk reduction, great cost savings and enhanced efficiencies. If used in the traditional security issuance processes, they can allow for direct dealings between issuers, syndicate member, investment banks and help track real-time ownership of securities. They also enable a new way of capital raising via so called initial coin offerings. This new method vastly improves liquidity of the early stage start-up financing and offers an alternative that can bypass both traditional banking and non-banking capital raising methods. Furthermore, asset managers can use blockchain to store clients' data, account transactions and transfers of ownership.

With greater transparency, quick on boarding processes and real-time performance reading trust into investment management industry should return.

If blockchain gets used widely and if it is properly implemented in domestic consumer payments it could totally disintermediate current four-party model and potentially make merchant acquirers and their revenues obsolete. Yet some barriers still exist; firstly, the market will have to determine who is going to pay for the consensus mechanism, and secondly, scalability and customer experience need to match at least that of the current infrastructure. On the other side I think that cross-border payments are more suitable for the adoption of the technology, at least in the short term. Correspondent banking model that requires banks to hold huge amounts of capital around the world is made out of a long chain of intermediaries exchanging unstandardized information and presents error prone and siloed systems that lead to low transaction visibility, uncertainty in funds delivery and slow payments. I expect annual industry revenues to drop by 60 % (or $216 billion) when blockchain will be properly implemented in the system. Remittance industry which also presents a huge portion of international payment flows will see a similar decline in industry revenues – I estimate $16 billion per annum could be removed from revenues of financial institutions and specialist RSPs.

Digitized placement of securities enables near real-time book building process where the Master Book is available for all participants in the blockchain. Quick and efficient processes can significantly cut settlement risk exposure and the need for internal and external reconciliation can virtually be eliminated by a single version of truth. This cuts manual effort and reduces the entire book building time by about 35 % to 50 %. Removed reconciliation and a direct flow of information between issuers, syndicate members and the investment banks virtually removes the need for the sales team of the investment bank, leading to a 50% cut in the underwriting fees – representing $10 billion annual savings in global underwriting fees.

Removed duplicative and manual reconciliation can lead to lower headcount and lowered back office costs of buy-side clients, broker-dealers, trust/custody banks, and the DTCC. Blockchain offers to deliver cost savings to two primary areas across post trade settlement and clearing processes of US cash equities market: operating expenses (back office, headcount, systems and clearing) and capital requirements. My analysis shows that market participants can save roughly $0.7 billion to $1.2 billion in back office and IT spend. Significantly reduced counterparty and settlement risks also bring $500 million in savings by reducing the aggregate amount of capital required at clearing houses. In total, I believe that a blockchain based infrastructure can bring $1.2 billion to $1.7 billion in annual cost savings to the US cash equities market.

Digital Asset Holdings and Ripple are building innovative solutions that are leveraging private permissioned systems. If successfully implemented across the network, they can increase speed, transparency and vastly reduce complexity and inefficiencies of current

financial infrastructure. Open source project Ethereum that uses a public unpermissioned blockchain represents a distributed computing platform that has smart contract functionality and gives everyone the opportunity to create a tradeable digital token that can be used as a currency, a representation of any asset, a virtual share or a proof of ownership of virtually anything. As such, it represents an innovative system that can transfer value and information representing ownership of assets in a totally decentralized way.

To conclude, blockchain's transparency, security, and efficiency make it a particularly good choice for reshaping businesses that are bogged down by inefficiencies. Shared infrastructure enables totally new business models based on distributed marketplaces and technology. Even though a new type of database technology that can be distributed across organizations creates the opportunity to disrupt markets and existing participants, the real effect remains to be seen and will be heavily dependent upon the scope of technology's successful implementation in the future.

REFERENCE LIST

1. Abel, A. & Bernanke, B. (2005). *Macroeconomics (5th Ed.)*. Pearson, pp. 266–269, ISBN 0-201-32789-9.
2. Accenture. (2017). *Banking on blockchain: A value analysis for investment banks*. Retrieved on August 10, 2017, from https://www.accenture.com/t20170120T074124Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Consulting/Accenture-Banking-on-Blockchain.pdf
3. Al-Naji, N., Chen, J. & Diao, L. (2017). *Basis: A Price-Stable Cryptocurrency with an Algorithmic Central Bank*. Retrieved on February 19, 2018, from https://www.basis.io/basis_whitepaper_en.pdf
4. Bank for International Settlements. (2018). *Cryptocurrencies: looking beyond the hype*. BIS Annual Economic Report 2018. Retrieved on July 10, 2018, from https://www.bis.org/publ/arpdf/ar2018e5.htm
5. Bank of Finland. (2018). *The great illusion of digital currencies.* BoF Economics Review. Retrieved on August 14, 2018, from https://helda.helsinki.fi/bof/bitstream/handle/123456789/15564/BoFER_1_2018.pdf
6. BCG. (2017a). *Global Asset Management 2017 – The Innovator's advantage*. Retrieved on May 15, 2018, from http://image-src.bcg.com/Images/BCG-The-Innovators-Advantage-July-2017_tcm9-163905.pdf
7. BCG. (2017b). *Global Payments 2017: Deepening the Customer Relationship*. Retrieved on April 20, 2018, from http://image-src.bcg.com/Images/BCG-Global-Payments-2017-Oct-2017_tcm9-173047.pdf
8. Bech, M. & Garratt, R. (2017). *Central Bank Cryptocurrencies*. BIS Quarterly Review September 2017. Retrieved on July 5, 2018, from https://ssrn.com/abstract=3041906
9. Bheemaiah, K. (2015). *Block chain 2.0: The Renaissance of Money*. Wired. Retrieved on August 10, 2017, from https://www.wired.com/insights/2015/01/block-chain-2-0/

10. Bitcoin Wiki. (2017a). *Mining*. Retrieved on August 30, 2017, from https://en.bitcoin.it/wiki/Mining
11. Bitcoin Wiki. (2017b). *Bitcoin*. Retrieved on August 28, 2017, from https://en.bitcoin.it/wiki/Main_Page
12. Bitcoin Wiki. (n.d.). *Proof of work*. Retrieved on June 5, 2018, from https://en.bitcoin.it/wiki/Proof_of_work
13. BitShares. (n.d./a). *Delegated Proof-of-Stake Consensus*. Retrieved on June 9, 2018, from https://bitshares.org/technology/delegated-proof-of-stake-consensus/
14. BitShares. (n.d./b). *Price-Stable Cryptocurrencies*. Retrieved on April 10, 2018, from https://bitshares.org/technology/price-stable-cryptocurrencies/
15. Bloomberg. (2018). *Cryptocurrencies: Here's What Maduro Has Said of Venezuela's Petro Cryptocurrency*. Retrieved on August 23, 2018, from www.bloomberg.com/news/articles/2018-08-20/here-s-what-maduro-has-said-of-venezuela-s-petro-cryptocurrency
16. Bolt, W. & van Oordt, M. (2016). *On the Value of Virtual Currencies*. De Nederlandsche Bank Working Paper No. 521. Available at SSRN: https://ssrn.com/abstract=2842557 or http://dx.doi.org/10.2139/ssrn.2842557
17. Business Insider. (2018). *One photo shows that China is already in a cashless future.* Retrieved on June 15, 2018, from https://www.businessinsider.com/alipay-wechat-pay-china-mobile-payments-street-vendors-musicians-2018-5
18. Buterin, V. (2013). *What Proof of Stake Is And Why It Matters*. Bitcoin Magazine. Retrieved on August 30, 2017, from https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/
19. BuyBitcoinWorldwide. (n.d.). *The Bitcoin Volatility Index.* Retrieved on August 20, 2018, from www.buybitcoinworldwide.com/volatility-index/
20. Capgemini Consulting. (2016a). *Blockchain Disruption in Security Issuance – Enabling the issuance of fully digitized smart securities*. Retrieved on August 15, 2018, from www.capgemini.com/wp-content/uploads/2017/07/blockchain_securities_issuance_v6_web.pdf
21. Capgemini Consulting. (2016b). *Smart Contracts in Financial Services: Getting from Hype to Reality*. Retrieved on June 5, 2018, from www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/smart_contracts_paper_long_0.pdf
22. Coindesk Research. (2018). *State of Blockchain Q2 2018*. Retrieved on August 15, 2018, from https://media.coindesk.com/uploads/research/state-of-blockchain/2018/q2/sob2018q2-2018.pdf
23. Coindesk. (2017). *A Short Guide to Bitcoin Forks*. Retrieved on April 20, 2018, from https://www.coindesk.com/short-guide-bitcoin-forks-explained/
24. Coindesk. (n.d.). Cumulative ICO and VC funding. Retrieved on August 3, 2018, from https://www.coindesk.com/ico-tracker/
25. CoinMarketCap. (n.d.). *Cryptocurrency market capitalizations.* Retrieved on August 5, 2018, from www.coinmarketcap.com

26. Conley, J. (2017). *Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings*. Vanderbilt University Department of Economics Working Papers, VUECON-17-00008.
27. Credit Suisse. (2016). *Blockchain*. Retrieved on September 15, 2017, from https://www.finextra.com/finextra-downloads/newsdocs/document-1063851711.pdf
28. Credit Suisse. (2018). *Blockchain 2.0*. Retrieved on March 5, 2018, from https://research-doc.credit-suisse.com/docView?language=ENG&format=PDF&sourceid=csplusresearchcp&document_id=1080109971&serialid=pTkp8RFIoVyHegdqM8EllLNi1z%2Fk8mInqoBSQ5KDZG4%3D
29. Deloitte. (2017). *Investment management firms getting started with blockchain*. Retrieved on Sept 5, 2017, from https://www2.deloitte.com/us/en/pages/financial-services/articles/im-firms-getting-started-blockchain.html
30. Digital Asset Holdings. (2016). *The Digital Asset Platform*. Retrieved on June 30, 2017, from http://hub.digitalasset.com/digital-asset-platform-non-technical-whitepaper
31. Doepke, M. & Schneider, M. (2017). *Money as a unit of account*. NBER Working Paper Series, Working Paper 19537, National Bureau of Economic Research.
32. Economist staff. (2015). *Blockchains: The great chain of being sure about things*. The Economist. Retrieved on August 20, 2017, from www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable
33. Ethereum Foundation. (n.d.). *Ethereum*. Retrieved on June 5, 2018, from www.ethereum.org/
34. Forbes. (2018). *Equity Underwriting Fees For The Largest U.S. Investment Banks Recovered To $6 Billion In 2017*. Retrieved on June 8, 2018, from www.forbes.com/sites/greatspeculations/2018/03/27/equity-underwriting-fees-for-the-largest-u-s-investment-banks-recovered-to-6-billion-in-2017/#d05de0e2656f
35. FSI. (2015). *Financial markets*. Retrieved on June 13, 2018, from http://fsi.gov.au/publications/interim-report/02-competition/financial-markets/
36. Garrat, R. (2016). *CAD-coin versus Fedcoin*. R3 report. Retrieved on January 10, 2018, from http://www.r3.com/wp-content/uploads/2017/06/cadcoin-versus-fedcoin_R3.pdf
37. Giddy, I., Saunders, A. & Walter, I. (1996). *Alternative models for clearance and settlement: the case of the single European capital market*. Journal of Money, Credit and Banking, *28*(4), 986–1000.
38. Goldman Sachs. (2016). *Profiles in Innovation: Blockchain*. Retrieved on July 12, 2017, from https://msenterprise.global.ssl.fastly.net/wordpress/2017/07/Goldman-Sachs-Blockchain-putting-theory-to-practice.pdf
39. Greco, T. (2001). *Money: Understanding and Creating Alternatives to Legal Tender*. White River Junction, Vt: Chelsea Green Publishing (2001), ISBN 1-890132-37-3.
40. Greenwich Associates. (2016). *Blockchain Adoption in Capital Markets*. Retrieved on May 10, 2018 from https://www.greenwich.com/fixed-income-fx-cmds/blockchain-adoption-capital-markets

41. Haber, S. & Stornetta, W. (1991). *How to time-stamp a digital document*. Journal of Cryptology. 3(2): 99 – 111. Retrieved on August 10, 2017.
42. Hoepman, J. (2008). *Distributed Double Spending Prevention*. 15th Int. Workshop on Security Protocols.
43. ING. (2018). *Cracking the code on cryptocurrency*. Retrieved on June 25, 2018, from https://think.ing.com/uploads/reports/ING_International_Survey_Mobile_Banking_2018.pdf
44. Kaal, W. & Dell'Erba, M. (2017). *Initial Coin Offerings: Emerging Practices, Risk Factors, and Red Flags*. Forthcoming, Fintech Handbook, Florian Möslein & Sebastian Omlor eds., Verlag C.H. Beck (2018); U of St. Thomas (Minnesota) Legal Studies Research Paper No. 17–18. Available at SSRN: https://ssrn.com/abstract=3067615
45. Keynes, J. M. (1936). *The General Theory of Employment, Interest, and Money*. London: Macmillan.
46. Koning, J. (2016). *Fedcoin: a central bank issued cryptocurrency*. R3 report. Retrieved on May 5, 2018, from https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/58c7f80c2e69cf24220d335e/1489500174018/R3+Report-+Fedcoin.pdf
47. Kursh, S., & Gold, N. (2016). *Adding FinTech and Blockchain to Your Curriculum*. Business Education Innovation Journal, *8*(2).
48. Lee Kuo Chuen, D. (2015). *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Academic Press.
49. Malviya, H. (2017). *Blockchain for Commercial Real Estate*. Independent. Retrieved on June 5, 2018, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2922695
50. Mango Startups. (2017). *A new era for ICO investing in Latin America*. Retrieved on February 15, 2018, from https://medium.com/@MangoStartups/a-new-era-for-ico-investing-in-latin-america-da9aed3b90c1
51. Mankiw, G. (2007). *Macroeconomics (6th Ed.)*. New York: Worth Publishers, pp. 22–32, ISBN 0-7167-6213-7.
52. McKinsey & Company. (2014). *The Internet of Things: Sizing up the opportunity*. Retrieved on March 8, 2018, from https://www.mckinsey.com/industries/semiconductors/our-insights/the-internet-of-things-sizing-up-the-opportunity
53. McKinsey & Company. (2016). *McKinsey on Payments: Rethinking correspondent banking*. Retrieved on July 15, 2018, from www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Rethinking%20correspondent%20banking/Rethinking-correspondent-banking.ashx
54. McKinsey & Company. (2017). *McKinsey Global Payments Map 2017*. Retrieved on August 5, 2018, from https://www.mckinsey.com/industries/financial-services/our-insights/global-payments-2017-amid-rapid-change-an-upward-trajectory
55. Mundell, R. (1999). *A reconsideration of the twentieth century*. Nobel Prize in Economics documents 1999-5, Nobel Prize Committee.
56. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved on June 30, 2017, from https://bitcoin.org/bitcoin.pdf

57. New Financial. (2016). *Taking stock on pay: what we do and don't know about pay at investment banks and asset managers.* Retrieved on August 10, 2018, from newfinancial.eu/taking-stock-on-pay-what-we-do-and-dont-know-about-pay-at-investment-banks-and-asset-managers/
58. Oliver Wyman & J. P. Morgan. (2016). *Unlocking Economic Advantage with Blockchain – A guide for asset managers*. Retrieved on July 10, 2017, from www.oliverwyman.com/content/dam/oliver-wyman/global/en/2016/july/joint-report-by-jp-morgan-and-oliver-wyman-unlocking-economic-advantage-with-blockchain-A-Guide-for-Asset-Managers.pdf
59. Oomes, N. (2003). *Network Externalities and Dollarization Hysteresis: The Case of Russia*. IMF Working Paper, ISBN 9781451851939.
60. Ostroy, J. M. & Starr, R. M. (1988). *The Transaction Role of Money*. UCLA Economics Working Papers, No. 505, UCLA Department of Economics.
61. Poon, J. & Dryja, T. (2016). *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments.* Retrieved on June 19, 2018, from http://lightning.network/lightning-network-paper.pdf
62. PricewaterhouseCoopers. (2014a). *Retail Banking 2020: Evolution or Revolution?*. Retrieved on August 5, 2017, from https://www.pwc.com/gx/en/banking-capital-markets/banking-2020/assets/pwc-retail-banking-2020-evolution-or-revolution.pdf
63. PricewaterhouseCoopers. (2014b). *Stand out for the right reasons: How financial services lost its mojo – and how it can get it back*. Retrieved on January 28, 2018, from https://www.pwc.co.uk/assets/pdf/fsrr-consumer-survey-final.pdf
64. Ripple. (2016). *The Cost-Cutting Case for Banks*. Retrieved on July 20, 2018, from https://ripple.com/files/xrp_cost_model_paper.pdf
65. Ripple. (2017). *XRP Ledger Decentralizes Further With Expansion to 55 Validator Nodes*. Retrieved on September 20, 2017, from https://ripple.com/insights/xrp-ledger-decentralizes-expansion-55-validator-nodes/
66. Ripple. (2018). *Democratizing Global Payments: xRapid's Cost Savings and Benefits*. Retrieved on June 20, 2018, from https://ripple.com/insights/democratizing-global-payments-xrapids-cost-savings-benefits/
67. Ripple. (n.d.). *Solution Overview*. Retrieved on June 5, 2018, from ripple.com/files/ripple_solutions_guide.pdf
68. Santander InnoVentures, Oliver Wyman & Anthemis Group. (2015). *The Fintech 2.0 Paper: rebooting financial services*. Retrieved on February 10, 2018, from santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf
69. Sehra, A., Smith, P. & Gomes, P. (2017). *Economics of Initial Coin Offerings*. Allen & Overy. Retreived on January 20, 2018, from www.allenovery.com/publications/en-gb/Pages/Economics-of-Initial-Coin-Offerings.aspx
70. Shaofang, L. & Marinč, M. (2015). *Competition in the Clearing and Settlement Industry*. Journal of International Financial Markets, Institutions and Money, Forthcoming, doi:10.1016/j.intfin.2015.09.004. Available at SSRN: https://ssrn.com/abstract=2667462

71. Standard Chartered. (2016). *Blockchain and T2S: A potential disruptor*. Retrieved on July 10, 2018, from https://av.sc.com/corp-en/2016-06-16-BeyondBorders-Report-SCB_Nema_Block-Chain-Paper-Final.pdf
72. Tether. (2016). *Tether: Fiat currencies on the Bitcoin blockchain.* Retrieved on March 15, 2018, from https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf
73. The Nilson Report. (2018a). *Europe's Top Acquirers – Ranked by Transactions in 2017*. Issue 1132. Retrieved on August 10, 2018, from nilsonreport.com/ publication_chart_and_graphs_archive.php
74. The Nilson Report. (2018b). *Top U.S. Acquirers in 2017 Purchase Transactions*. Issue 1127. Retrieved on August 10, 2018, from nilsonreport.com/publication _chart_and_graphs_archive.php
75. Treasury Alliance Group. (2018). *Fundamentals of Global Payment Systems and Practices*. Retrieved on July 15, 2018, from www.treasuryalliance.com/ assets/publications/payments/Fundamentals_of_Payment_Systems.pdf
76. Visa. (2006). *The Inefficiencies of Cross-Border Payments: How Current Forces Are Shaping the Future*. Retrieved on July 3, 2018, from http://euro.ecom.cmu.edu/ resources/elibrary/epay/crossborder.pdf
77. William, C., L. & He, Z. (2018). *Blockchain disruption and smart contracts*. National Bureau of Economic Research, Massachusetts, 2018. Retrieved on June 1, 2018, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985764
78. World Bank Group. (2018). *Migration and remittances*. Retrieved on June 30, 2018, from www.knomad.org/sites/default/files/2018-04/Migration%20and%20Development %20Brief%2029.pdf
79. World Economic Forum. (2015). *Deep Shift: Technology Tipping Points and Societal Impact*. Retrieved on July 8, 2018, from http://www3.weforum.org/docs/WEF _GAC15_Technological_Tipping_Points_report_2015.pdf
80. Yang, B. Z. (2007). *What is (not) money? Medium of exchange ≠ means of payment*. American Economist, Vol. 51, No. 2.
81. Zuckerman, E. W. (2003). *On Networks And Markets by Rauch and Casella, eds*. Journal of Economic Literature, *41*(2): 545–565.

APPENDIX

Appendix 1: Povzetek (Summary in Slovene language)

UVOD

Digitalna revolucija drastično spreminja podobo finančne infrastrukture. Nove tehnologije, kot so elektronska plačila, podatkovna analitika, umetna inteligenca in blockchain vodijo do večjih hitrosti, večje preglednosti in nižjih transakcijskih stroškov. Glavna obljuba blockchain tehnologije je pravzaprav zagotovitev novega pristopa k upravljanju podatkov in vrednosti. Do sedaj so bila najpogostejša vprašanja zasebnosti, varnosti in zaupanja v prenos podatkov in vrednosti med različnimi strankami rešena z uporabo zaupanja vrednih posrednikov. Zaupanje je bilo tradicionalno zagotovljeno z izmenjavo podatkov prek nevtralnih centralnih organov, ki jim obe pogodbeni stranki zaupajo. Naloga neodvisnega posrednika je, da služi kot mediator in da zagotovi, da si stranke res lastijo tisto, kar so želele izmenjati. Poleg tega pa morajo zagotoviti, da se transakcija zgodi in da na koncu res pride do izmenjave sredstev. Blockchain ponuja dokončno različico resnice, ki lahko olajša prej omenjene probleme. Računalniška moč in kriptografija se uporabljajo za vzdrževanje distribuirane, časovno žigosane in nespremenljive knjige vseh preteklih transakcij. Distribuirana struktura ponuja novo arhitekturo, s pomočjo katere si vsi udeleženci na kapitalskih trgih delijo skupno knjigo podatkov, kar močno racionalizira ali celo odpravi številne obstoječe podporne operacije. Poleg tega pa blockchain podpira še številne aplikacije; od pametnih pogodb, registrov premoženja do direktnih ali "peer-to-peer" prenosov informacij ali lastnine (Kursh & Gold, 2016).

Da bi raziskal možnosti uporabe blockchain tehnologije, sem najprej opisal pomanjkljivosti sedanjih transakcijskih sistemov. Sodobna finančna infrastruktura temelji na uporabi verige posrednikov. Ker pa ti uporabljajo različne sisteme, si med seboj delijo nestandardizirane podatke, ki morajo biti znova in znova posodobljeni in usklajeni. Nato sem opisal prednosti in slabosti, ki jih imajo različne izvedbe blockchaina. V drugem delu naloge sem raziskal različne aplikacije tehnologije v tradicionalni infrastrukturi kapitalskih trgov. S svojo zasnovo blockchain spodbuja vertikalno integracijo in lahko obstoječe poslovne modele naredi zastarele. Zato poskusim opisati načine, kjer bi uporaba te tehnologije privedla do zmanjšanja stroškov in povečanja učinkovitosti v naslednjih segmentih znotraj verige vrednosti finančne infrastrukture: valute izdane z blockchain tehnologijo, kliring in poravnava, plačila, zbiranje sredstev, pametne pogodbe in upravljanje naložb. V tretjem delu s pomočjo empirične analize ocenim dodano vrednost blockchaina in morebitna zmanjšanja provizij ter virov prihodkov za tri glavne segmente financ: plačila, kliring in zbiranje sredstev. V zadnjem poglavju raziščem vodilna podjetja, ki razvijajo nove rešitve zgrajene s pomočjo blockchaina. Opišem njihove poslovne modele, predstavim infrastrukturo, ki jo gradijo, in ocenim, kje bi lahko ta pomagala racionalizirati obstoječi sistem.

PREGLED FUNKCIONALNOSTI BLOCKCHAIN TEHNOLOGIJE

Distribuirana veriga zaporednih podatkov ali transakcij omogoča rešitev problema dvojne porabe. Podatkovni bloki so kriptografsko zaščiteni in porazdeljeni po omrežju, tako da ima vsak od udeležencev možnost ogleda vseh preteklih transakcij, ki so zapisane v t. i. skupno knjigo podatkov. Časovno zabeleženi in kriptografsko zavarovani vnosi omogočajo učinkovito, trajno in nespremenljivo evidenco transakcij. Glavna lastnost, ki loči bazo podatkov, zgrajeno s pomočjo blockchain tehnologije, od obstoječih rešitev je t. i. porazdeljeno soglasje ali konsenz. Pri tem skupina udeležencev za zagotavljanje veljavnosti podatkov potrjuje pravilne transakcije, nepravilne pa zavrne. Javna knjiga podatkov služi kot mehanizem zaupanja, ki ima zmožnost prenosa praktično kakršnekoli vrednosti, ne da bi pri tem potrebovali zaupanja vrednega posrednika.

Uporaba blockchaina lahko privede do veliko boljše preglednosti, enostavnosti in učinkovitosti v obstoječi finančni industriji, kjer danes vsi udeleženci vodijo lastne in ločene evidence transakcij. Vrednost v digitalni obliki je izpostavljena grožnji, da je podvojena in da se jo lahko porabi večkrat. Večina finančnih transakcij prav zato poteka preko zaupanja vrednega posrednika ali centralnega serverja, kar jih naredi drage in neučinkovite. Poleg tega lahko med izvršitvijo in poravnavo velikokrat mine več kot tri dni. Kljub raznim pobudam za zmanjšanje zapletenosti in za povečanje medsebojne povezanosti teh sistemov se udeleženci na finančnih trgih še vedno opirajo na zastarelo infrastrukturo, ki zahteva zamenjavo nestandardnih podatkov med njimi. Neučinkovita struktura ustvarja potrebo po dragih postopkih, ki zahtevajo ogromno ročnega posredovanja, kar ustvarja ogromno trenje pri izmenjavi podatkov in vrednosti. To vodi k visokim obratovalnim stroškom na kapitalskih trgih in posledično dražjim transakcijam za končne kupce (Credit Suisse, 2016).

Tehnologija blockchain omogoča, da je baza podatkov oziroma transakcij enakomerno porazdeljena med deležniki v omrežju, kar pomaga pri učinkovitem in stalnem beleženju transakcij med strankami. Ker se podatkov ne da spreminjati za nazaj, ko so bili enkrat zapisani, to omogoča njihovo verodostojnost ter preprosto preverjanje vnosov (Bheemaiah, 2015). Za zagotavljanje veljavnosti transakcij se uporabljajo inovativni koncepti doseganja konsenza, saj mora skupina t. i. rudarjev neprestano preverjati veljavnost podatkov. Obstajajo tri različice distribuirane podatkovne baze, izbira le te pa je vedno pogojena s kompromisom med stroški in varnostjo pri zagotavljanju podatkov. Popolnoma pregledna in odprta struktura je značilna za odprto javno bazo podatkov kot je "unpermissioned public ledger", saj ima vsakdo možnost ogleda preteklih transakcij ter lahko sodeluje pri potrjevanju prihodnjih. Takšna struktura je na primer značilna za Bitcoin. Na drugi strani obstajata dve zaprti različici knjige. V prvi t. i. "permissioned public ledger" strukturi lahko knjigo podatkov vidi vsak, zapis transakcij pa je omogočen le lastnikom in predhodno izbranim udeležencem. V drugi t. i "permissioned private ledger" strukturi pa sta tako zapis kot branje podatkov omogočena le izbranim udeležencem, kar poslabša varnost zaradi centralizirane knjige transakcij oziroma informacij (Credit Suisse, 2016).

UPORABA BLOCKCHAIN TEHNOLOGIJE V FINANČNI INDUSTRIJI

Ankete opravljene med direktorji vodilnih svetovnih podjetij nakazujejo, da bo imela blockchain tehnologija največji vpliv in uporabno vrednost v panogah, katerih infrastruktura je trenutno zapletena in posledično nudi drage storitve. Soglasno prepričanje je, da bodo finančne storitve, še posebej področja plačil in kapitalskih trgov, doživele največje spremembe.

Trenutno se veliko govori o denarju, ki omogoča digitalno "peer-to-peer" izmenjavo vrednosti. V preteklosti je direktno menjavo med strankami omogočala le gotovina, elektronske različice denarja, kot so bančni depoziti, pa so bile izmenjane s pomočjo zaupanja vrednega posrednika. Takšne inovativne izpeljanke denarja, ki omogočajo varno in učinkovito "peer-to-peer" izmenjavo vrednosti, ljudje pogosto imenujejo kar kriptovalute, ki za izmenjavo potrebujejo le mobilni telefon in dostop do interneta. Obstajata dve različici takšnega denarja. Prva je izdana privatno in uporablja distribuiran konsenz, kjer mreža uporabnikov brez centralnega organa ali posrednikov potrjuje verodostojnost transakcij v omrežju. Primer takšnega denarja je popularen Bitcoin, katerega tržna kapitalizacija je presegala 300 milijard EUR. Ker pa so takšne valute pogosto zelo volatilne, so se pojavila mnoga vprašanja o možnosti uporabe teh v izmenjavi dobrin, saj se lahko vrednost denarja dnevno spremeni tudi za deset odstotkov. Da bi se izognili tej težavi, so se pojavile nove in stabilne različice tega denarja. Tako imenovani "stablecoini" so zasnovani tako, da s pomočjo dinamičnega spreminjanja izdanih enot ohranjajo svojo vrednost stabilno. Na drugi strani pa imamo kriptovalute, ki so izdane s strani centralne banke. Tehnologija daje tem možnost, da ustvarijo digitalen medij izmenjave, ki lahko prinese večjo preglednost in učinkovitost v sedanji sistem. Tudi v tem primeru bi centralna banka delovala kot pooblaščeni subjekt, ki ima možnost izvajanja monetarne politike, saj bi še vedno imela popoln nadzor nad izdajanjem denarja.

Storitve kliringa in poravnave omogočajo učinkovito delovanje kapitalskih trgov z zniževanjem transakcijskih stroškov vlagatelja ob trgovanju (Giddy, Saunders & Walter, 1996). Ti procesi so trenutno zelo netransparentni, zamudni, zahtevajo znatno količino medsebojnih uskladitev in vključujejo več posrednikov. Infrastruktura zgrajena s pomočjo blockchain tehnologije bi lahko zagotovila varnejši, hitrejši in učinkovitejši postopek po opravljenem trgovanju, saj lahko različnim ponudnikom znotraj verige vrednosti ponudi skladen in enoten "vir resnice" lastništva premoženja. Register podatkov in premoženja na skupni infrastrukturi je v realnem času deljen med uporabniki, ki imajo dovoljenje, da vidijo in urejajo te podatke. Banke, klirinško depotne družbe in regulatorji tako na primer lahko komunicirajo in izmenjujejo standardizirane podatke direktno, kar znatno zmanjša stroške ročnih medsebojnih uskladitev. Prav tako lahko znatno skrajšamo trenutni T+2 cikel poravnave ter tveganja izpostavljenosti (Credit Suisse, 2018).

Udeleženci plačilne industrije pomagajo pri prenosu vrednosti v kakršnikoli obliki denarja. Za izvedbo plačila originatorji uporabljajo vrsto različnih kanalov. Od teh ima vsak različne

operativne značilnosti, pravila in mehanizme poravnave. Vrednost, ki se prenaša, je običajno shranjena na depozitnih računih pri bankah ali drugih finančnih institucijah. Za omogočanje plačil morajo biti banke in ostale finančne institucije povezane z vrsto različnih plačilnih sistemov, saj se ti med seboj pogosto razlikujejo. V trenutni infrastrukturi so prav zato povezane s široko paleto plačilnih sistemov, pogosto na več kot 50 hkrati. Banke, ki delujejo v različnih državah, se povezujejo s plačilnimi sistemi v vsaki od držav, v katerih poslujejo neposredno ali prek korespondenčne banke. Ker je zelo pomembno, ali pot plačila prečka mejo države in ali je plačilo opravljeno v različnih valutah, ločimo domača in mednarodna plačila. V segmentu domačih plačil sem se zato osredotočil na kartična plačila, v primeru čezmejnih plačil pa sem opisal trenutni model korespondenčnega bančništva. Trg plačilnih in debetnih kartic temelji na tako imenovanem "four-party" sistemu, ki je nastal v šestdesetih letih prejšnjega stoletja. V tej shemi so med potrošnikom in trgovcem trije dodatni posredniki – "merchant acquirerji", kartično omrežje ter banka trgovca (ang. "issuing bank"). Z uporabo blockchain tehnologije pa se lahko tem posrednikom izognemo, saj lahko transakcije potekajo direktno med samim kupcem in prodajalcem, kar znatno zmanjša transakcijske stroške.

Približno 80 % čezmejnih plačil danes poteka preko tako imenovanega sistema korespondenčnega bančništva. Da lahko poslujejo s tujino, banke ohranjajo korespondenčne bančne odnose z lokalnimi bankami po vsem svetu, ki za njih zagotavljajo likvidnost za mednarodna plačila s pomočjo t. i. "nostro" računov. Za opravljanje teh plačil mora banka vzpostaviti kreditno linijo pri korespondenčni banki ali vnaprej financirati "nostro" račun. Za to, da je plačilo opravljeno, mora denar prečkati različne sisteme. Ti velikokrat niso zgrajeni na enaki infrastrukturi in imajo slabo medsebojno usklajenost. To vodi do dvojega knjigovodstva, kar podaljša poravnavo (ta pogosto traja 3–5 dni) in poveča nagnjenost k napakam. Vse to pa naredi transakcije zelo drage (Visa, 2006).

Izdaja vrednostnih papirjev (npr. delnic in obveznic) danes pogosto še vedno temelji na izdaji papirnatih potrdil, ki imetniku dajejo pravico do lastništva. Proces izdaje je nepregleden, drag in vključuje verigo posrednikov, ki morajo pogosto voditi redundantne in med seboj ločene evidence lastnikov vrednostnih papirjev. To lahko privede do več različic resnice, saj morajo izdajatelji, investitorji in regulatorji ohranjati ločene različice preteklih transakcij in lastništva. Pri poravnavi posla pogosto mine več kot tri dni, s tem pa je tveganje nasprotnih strank (ang. "counterparty risk") dodatno povečano. Pametne pogodbe, ki jih omogoča blockchain, se lahko uporabljajo tako v javnih kot zasebnih postopkih izdajanja vrednostnih papirjev, pri tem pa so digitalni vrednostni papirji izdani na porazdeljeni knjigi transakcij. Takšna standardizirana in digitalizirana struktura omogoča neposreden pretok informacij med izdajatelji, člani sindikata in investicijskimi bankami ter pomaga pri spremljanju lastništva vrednostnih papirjev v realnem času. Odstranitev fizične dokumentacije in popolnoma digitalizirana rešitev lahko zmanjšata uporabo posrednikov in skrbnikov, s čimer je proces veliko bolj učinkovit in vitek. Za razliko od tradicionalne začetne izdaje delnic (ang. "initial public offering"), ki si jo lahko privoščijo le velika podjetja, blockchain tehnologija omogoča financiranje podjetij s pomočjo izdaje žetonov.

Tako imenovana prvotna izdaja žetonov (ang. "initial coin offering") omogoča možnost zbiranja sredstev za razvojni projekt zgodnje faze in ponuja alternativo, ki lahko zaobide storitve tako tradicionalnih bančnih kot nebančnih institucij (npr. tveganega kapitala). Na ta način dobi podjetje sredstva potrebna za razvoj izdelka, medtem ko vlagatelji, ki sodelujejo pri prodaji, prejmejo lastništvo žetona, ki lahko služi kot način za dostop do platforme podjetja ali pa predstavlja del lastništva. Ker podjetja za izdajo žetonov ne potrebujejo storitev renomiranih bančnih institucij, je izdaja posledično veliko cenejša in hitrejša (Conley, 2017).

Pojem pametna pogodba se je prvič pojavil že leta 1994. Ameriški kriptograf Nick Szabo je v članku predstavil osnovno idejo o pametnih pogodbah, ki omogočajo, da se obligacijska razmerja prenesejo v programsko opremo z namenom, da se njihovo izvrševanje avtomatizira. Blockchain tehnologija je osnovno idejo o pametnih pogodbah nadgradila in omogočila nove načine uporabe. Pogodbeni pogoji v pametni pogodbi se najprej šifrirajo in vnesejo v blockchain, kopija katerega se nato deli v več vozlišč v omrežju. Ker so podatki razporejeni po omrežju, sodelujoči subjekti poznajo pogodbene pogoje in s tem povezane prenose vrednosti. To pomeni, da so transakcije enostavno sledljive in preverljive. Tradicionalna infrastruktura za razrešitev sklepov zahteva prisotnost tretjih oseb (npr. sodnikov in sodišč) in zahteva veliko človeškega posredovanja, kar vodi v večjo negotovost in povzroča dodatne stroške. Ker se pametne pogodbe izvajajo samodejno s pomočjo programske kode, omogočajo avtomatsko in nekonfliktno izmenjavo vrednosti, denarja, premoženja, storitev ali izdelkov (William, L. & He, Z., 2018). Pametne pogodbe se lahko uporabijo v vseh segmentih industrije finančnih storitev, saj nudijo zmanjšanje tveganj, prihranke pri stroških in večjo učinkovitost trenutnih procesov. Sprejetje skupnih standardov pametnih pogodb med udeleženci na trgu bo verjetno privedlo do avtomatizacije celotnih procesov in tako odpravilo ogromne stroške povezane s skladnostjo (ang. "compliance"), vodenjem evidenc, preverjanjem in ročnim posredovanjem (Capgemini Consulting, 2016b).

V okolju negotove rasti trga, šibkih neto prilivov in zmanjševanja pristojbin se bodo morali člani industrije upravljanja naložb spoprijeti z novimi izzivi. Da bi bili v prihodnosti konkurenčni, bodo morali s pomočjo novih tehnologij preoblikovati način dela (Oliver Wyman & J. P. Morgan, 2016). V vrednostni verigi upravljanja naložb obstajajo različne dejavnosti. Za zagotavljanje storitev mora vsak upravljavec naložb izvesti določene vrste dejavnosti, od katerih bodo nekatere bolj verjetno izboljšane s pomočjo blockchain tehnologije. Sem sodijo postopki, ki zahtevajo več članov za izdajo odobritev, in postopki, ki zahtevajo stalno revizijo, skladnost in regulativni nadzor. Blockchain omogoča učinkovito shranjevanje podatkov o profilih strank, ki lahko vsebujejo njihove naložbene preference, vrednosti premoženja in profile tveganja. Trenutno upravljanje dokumentov, poravnava, prenos lastništva in komunikacija z vlagatelji so obremenjujoči, dolgotrajni in dragi procesi. Stroge zahteve za vstop v sklade in naložbe zahtevajo, da kupci ločeno zagotovijo dokaz o identiteti, prebivališču, zakonskem stanu, virih bogastva in poklicu. Namesto da čaka dneve ali tedne za zbiranje podatkov, bo družba za upravljanje z naložbami imela dostop do knjige podatkov, ki vsebuje javni profil svojega potencialnega kupca oziroma investitorja. Sistem

bo omogočal preprosto revizijsko sled za spremljanje kakršnihkoli sprememb ter preprosto in instantno poročanje o vseh transakcijah in trgovanju. Prenos sredstev bo izveden praktično v sekundah in brez uporabe tretje osebe. Poleg možnosti hitrega vstopa v naložben produkt bodo vlagatelji lahko deležni informacij o svojem portfelju in tveganju v realnem času, kar jim bo omogočilo boljši vpogled v razumevanje njihove izpostavljenosti (Deloitte, 2017). Ta večja preglednost bo, kot predvidevata družbi Oliver Wyman in J.P. Morgan (2016), posledično povrnila zaupanje v industrijo upravljanja naložb.

EMPIRIČNA ANALIZA MOŽNIH ZMANJŠANJ PRIHODKOV GLAVNIH SEGMENTOV FINANČNE INDUSTRIJE Z OSREDOTOČENJEM NA PRIHODKIH PLAČIL, KLIRINGA IN ZBIRANJA DENARJA

Kot omenjeno, večina sedanjih kartičnih plačil temelji na t. i. "four-party" sistemu. Po zasnovi je le ta prepreden s posredniki, vsak od njih pa doda k skupnemu znesku provizije plačila s kartico. Trgovcu se zaračuna skupek provizij, ki jih sestavljajo provizije "merchant acquirerjev", kartičnega omrežja in banke kupca ter so po navadi enake 2 % celotnega plačila. Od končne provizije za trgovca "merchant acquirer" vzame v povprečju 0,35–0,4 %, medtem ko se preostanek razdeli med proviziji za kartično omrežje in banko kupca. "Merchant acquirerji" v Združenih državah Amerike in Evropi so leta 2017 obdelali transakcije v skupni vrednosti $8,7 trilijonov, povprečna provizija pa je znašala 0,6 %. S svojo analizo sem pokazal da bi se prihodki kartične industrije zmanjšali za $52 milijard na leto, če "merchant acquirerji" ne bi bili več potrebni. Kot taka tehnologija blockchain ponuja dva možna primera uporabe, ki bi drastično spremenila sistem kartičnih plačil. Prvič, Bitcoin ali podobna kriptovaluta z javno knjigo podatkov postane množično uporabljena kot plačilno sredstvo. In drugič, uvedena je uporaba zasebne knjige podatkov, katere podatke lahko vidijo vsi v udeleženci v sistemu, le pooblaščeni udeleženci pa lahko sodelujejo pri oblikovanju soglasja. Čeprav so kartična omrežja trenutno zelo učinkovita, varna in omogočajo skoraj brezhibno izkušnjo kupcev, verjamem, da je dovolj prostora za znižanje trenutnih 2 % provizij. Ta redukcija izhaja predvsem iz nižjih marž "merchant acquirerjev" ter marž bank kupcev. Prav tako si upam trditi, da bo dolgoročno prišlo do drastičnih sprememb v sedanjem "four-party" sistemu in da večina domačih plačil v prihodnje ne bo več vključevala verige posrednikov, saj se bo plačilo izvedlo direktno ali "peer-to-peer".

Kriptografsko zaščiteni žetoni, ki jih je mogoče izmenjati brez uporabe zaupanja vrednega posrednika, so zelo primerni za svet mednarodnih plačil. Omogočajo učinkovite in enostavnejše transakcije, kjer banke ne potrebujejo odpreti in vzdrževati številnih bančnih računov po vsem svetu. Trenutne rešitve s pomočjo blockchain tehnologije omogočajo prenašanje vrednosti v realnem času, zagotavljanje likvidnosti na zahtevo in zmanjšanje stroškov povezanih z zakladništvom, plačilnimi operacijami ter regulatornimi zahtevami. Ripple ponuja distribuirano in medsebojno povezano infrastrukturo, s pomočjo katere lahko banke odpravijo odvečne operativne stroške in stroške zagotavljanja likvidnosti, saj več ne potrebujejo "nostro" računov. V primerjavi s sedanjim sistemom ima takšna struktura stroške nižje za 60 odstotkov. S pomočjo slednje predpostavke sem tako določil potencialno

zmanjšanje prihodkov v industriji čezmejnih plačil – prihodki C2C plačil se zmanjšajo za $45 milijard, prihodki B2B plačil za $171 milijard letno, skupno pa to predstavlja $216 milijardno redukcijo v industriji čezmejnih plačil.

Blockchain tehnologija s pomočjo pametnih pogodb omogoča veliko bolj avtomatiziran postopek zbiranja denarja. Kljub temu pa mora izdajatelj določiti investicijsko banko, ki je odgovorna za izdajo novega lastniškega kapitala ali dolga. Digitalna izdaja vrednostnih papirjev omogoča proces izdelave knjige interesa skoraj v realnem času. Zaradi distribuirane infrastrukture in enakomernega deljenja podatkov je ta na voljo vsem udeležencem v sistemu, kar odpravlja potrebo po redundantnih medsebojnih uskladitvah. S tem se zmanjša količina ročnih vnosov in celotni čas procesa zbiranja sredstev za približno 35–50 %. Neposredne transakcije med izdajatelji, člani sindikata in investicijskimi bankami lahko tako popolnoma izločijo prodajno ekipo investicijske banke, slednje pa lahko s tem prihranijo približno $10 milijard na leto.

Odstranitev podvojenih in pogosto ročnih uskladitev podatkov o transakcijah med investitorji, posredniki, brokerji, skrbniki in DTCCjem lahko pripomore k precejšnjemu prihranku udeležencev na trgu, saj se znatno znižajo število zaposlenih ter stroški zaledne pisarne. S pomočjo blockchain tehnologije lahko tako dosežemo nižje operativne stroške (zaledna pisarna, število zaposlenih, sistemi in kliring), boljša preglednost pa vodi do nižjih kapitalskih zahtev. Udeleženci ameriškega delniškega trga bi tako letno lahko prihranili od od $1,2 milijarde do $1,7 milijarde.

VODILNA PODJETJA, KI RAZVIJAJO REŠITVE S POMOČJO BLOCKCHAIN TEHNOLOGIJ

Infrastruktura, ki jo gradi podjetje Digital Asset Holdings bo omogočala učinkovitejšo medsebojno povezanost udeležencev finančnih trgov, kot so klirinško depotne družbe, brokerji, banke in skrbniki. Platforma imenovana "Digital Asset Platform" bo nudila skupno infrastrukturo, na kateri bo mogoče graditi različne aplikacije finančnih storitev. Poleg tega da skuša medsebojno povezati različne udeležence na trgu, ki bodo med seboj avtomatsko izmenjevali standardizirane podatke, je naloga platforme ohranjati zaupnost in razširljivost, ki sta potrebna za velike in regulirane trge.

Ripple Labs je podjetje s sedežem v San Franciscu, ki razvija plačilni protokol in infrastrukturo imenovano "RippleNet". Ta bo povezovala banke, ponudnike plačil ter borze in bo s pomočjo žetona "XRP" omogočala bruto poravnave, menjavo valut in plačila v realnem času. Podobno kot infrastruktura Digital Asset Holdinga je ta zgrajena s pomočjo zasebne knjige, zaradi standardizirane tehnologije in podatkov pa omogoča instantno pošiljanje podatkov, sporočil, kliring in poravnavo. Ripple trdi, da lahko v primerjavi z obstoječim njegov sistem zmanjša stroške poslovanja za čezmejna plačila kar do 60 %, saj banke ne potrebujejo "nostro" računov po svetu. Sistem je trenutno zmožen opraviti več kot

1500 transakcij na sekundo, naj pa bi bil zmožen preseči tudi število transakcij, ki jih omogoča Visa.

Ethereum je odprtokodna platforma, ki ponuja pametne pogodbe in za delovanje uporablja svoj žeton imenovan "Ether". Ethereum je leta 2013 zasnoval Vitalik Buterin, tako da deluje kot decentralizirana platforma, ki izvaja pametne pogodbe in t. i. porazdeljene aplikacije (ang. "dapps"). Udeležencem prav tako daje možnost ustvaritve lastnega žetona, ki se lahko uporablja kot valuta ali reprezentacija navideznega deleža ali dokazila o lastništvu. V zadnjem času je Ethereum doživel pravi razcvet, saj se je po svetu pojavilo več kot 4000 primerov zbiranja denarja s pomočjo tako imenovane začetne izdaje žetonov. Nekatere izmed največjih izdaj so uprizorila podjetja, kot so Augur, Raiden, OmiseGo, Golem in Iconomi, osnovni namen pa je bil uporabiti decentralizirano infrastrukturo za "tokeniziranje" vrednostnih papirjev, dividend, zavarovanj, glasovalnih sistemov ali realnih sredstev, kot sta zlato in srebro. Sredstva, ki so bila zbrana in so zaklenjena s pametnimi pogodbami, se bodo na podlagi dobrih rezultatov lahko posredovala lastnikom projektov ali pa se vrnila investitorjem. Vse to pa je doseženo s pomočjo sistema, ki ne potrebuje nobenega posrednika in za potrditev veljavnosti transakcij ne zahteva centraliziranega arbitra ali klirinške hiše.