Is it feasible to use distributed ledger technology for interbank transfers?

EXAMINING THE CHALLENGES AND OPPORTUNITIES OF DISTRIBUTED LEDGER TECHNOLOGY IN THE FINANCIAL SECTOR

AUTHOR: BURGYÁN JÁNOS ISTVÁN
THESIS ADVISOR: DR. PESUTH TAMÁS
Table of Contents

1. Introduction ................................................................. 2

2. Defining Distributed Ledger .............................................. 4

2.1. Bitcoin ................................................................. 4

2.1.1. Bitcoin is a type of distributed ledger, but not every distributed ledger is like bitcoin .... 4

2.1.2. How is a bitcoin transaction made? .................................. 4

2.1.3. Inventions of bitcoin: blockchain ..................................... 5

2.1.4. Inventions of bitcoin: distributed ledger .............................. 6

2.1.5. Inventions of bitcoin: proof-of-work mechanism ....................... 6

2.1.6. What gives value to bitcoin? ......................................... 7

2.1.7. Security ................................................................ 8

2.1.8. Significance of bitcoin .................................................. 8

2.2. The Archetypes of Distributed Ledgers .................................. 9

2.2.1. What are distributed ledgers? ......................................... 9

2.2.2. Public shared ledgers .................................................. 10

2.2.3. Private shared ledgers .................................................. 11

2.3. Why would financial institutions switch to DLT? ....................... 12

3. Analysing the feasibility of Distributed Ledger Technology adaptation ........................................ 14

3.1. Hypothesis ................................................................. 15

3.2. Current state of Distributed Ledger Technology ..................... 15

3.2.1. SWOT analysis ....................................................... 15

3.2.2. Challenges .......................................................... 17

3.2.3. Business value ....................................................... 22

3.2.4. Concluding the current state of DLT ................................. 23

4. Smart contracts on blockchains ............................................ 24

4.1. What is a smart contract? .............................................. 24

4.1.1. Defining Smart Contracts ........................................... 24

4.1.2. Smart Contract Lifecycle ............................................ 25

4.2. For what can smart contracts be used at financial services? .......... 25

4.2.1. Benefits .............................................................. 25

4.2.2. Relevant use cases ................................................... 26

4.3. Challenges in smart contracts .......................................... 27

4.4. Conclusion of smart contracts on DLT ............................... 29

5. Conclusion and Summary ................................................ 30

Bibliography .................................................................. 32
1. Introduction

In 2008 Satoshi Nakamoto published a paper entitled: *Bitcoin: A Peer-to-Peer Electronic Cash System*, and a new era of electronic settlement systems began. This does not sound as radical as it really is, but what it meant is a potential disruptor of the currently known bank system, the risk of traditional banks being replaced by IT companies in a somewhat similar way that Uber is replacing taxis – with the difference in market size and therefore the magnitude as well.

What Nakamoto created is not only a digital currency that is independent from any country – and as such, a so-called non-fiat currency. The underlying value of this currency comes from the computational power that is required to solve complex algorithms. These algorithms are not autotelic though – they are required to secure the transactions between the different parties. But the true revolution that Nakamoto introduced is the settlement and booking system that supports bitcoin: the blockchain. What it essentially is that all the transactions made in bitcoin are put in a definitive order, organized in blocks – a chain of blocks of transactions. And this is what makes the blockchain something revolutionary: a accounting system, that does not organize money by assigning it to accounts but it organizes it into transactions – between accounts. Also, it is not stored in one central server, but parallel at every user – it is a *distributed ledger*. And as such it is perfectly transparent, secure and provides trust between the parties – transparent, because the money’s route can be traced back due to the transaction based system, secure, because no money can be stolen – to do that not only one account but the whole system needs to be hacked – every user at the same time, and provides trust – all money has a unique identification and over all transactions a consensus is reached.

The reason why I have chosen this subject for my diploma thesis, is that I genuinely believe that the distributed ledger technology will have a significant impact on the banking system in the following 5-10 years. (PWC, 2016) It is one of the major components of todays’ buzzword, the FinTech revolution, however, for many it is still unclear, what it is about. My goal is to give a general overview of where the distributed ledger technology is today, what it is capable of, and what the future applications of this technology could be. Also, I would like to give further emphasis on the question: can currently used transaction accounting and methodology
between financial institutions be replaced by a distributed ledger system and what would be its benefits and drawbacks?

Method-wise, I would mainly use secondary sources, such as publications in professional magazines and newspapers – the analysis of these consist the first part of my thesis. The secondary sources include researches about bitcoin and generally blockchain and its use, studies about other applications of blockchain, the feasibility of the adaptation of distributed ledgers and smart contracts, case studies and report published by consulting firms and white papers published by companies specializing in distributed ledger technology. It is important to see that distributed ledger technology has two sides: a technological one and one related to business. My aim is to not to go too deeply into technological details, just to the necessary level to understand how it works, what does it enable, and what kind of prospects does it open.

Of course, distributed ledger technology is not the answer to everything nor it is perfect (yet). For this reason, I would like to formulate some criticism as well about the drawbacks of the technology.
2. Defining Distributed Ledger

2.1. Bitcoin

2.1.1. Bitcoin is a type of distributed ledger, but not every distributed ledger is like bitcoin

The most commonly known distributed ledger is the first pioneer of this technology, the bitcoin. It was created by an anonymous Japanese computer scientist, who published it open-source under the nickname of Satoshi Nakamoto in 2008. His goal was to create a technology that provides transactional trust between parties that de facto cannot trust each other. (Nakamoto, 2008) It provides trust by three new inventions: the blockchain technology, the shared ledger and the proof-of-work ledger consensus mechanism.

It is crucial to recognize, that the bitcoin blockchain is a very specific type of distributed ledger with very specific targets: providing transparent, immutable transactions and trust between parties that do not trust each other at all and there is not a central authority that controls the processes. Thus, its functionalities cannot be directly translated to newer, more developed distributed ledgers – others can differ in various points. The bitcoin is more of a first functioning prototype, a so-called proof-of-work. With that said, let’s look at first how the bitcoin works, what is that so revolutionary in it, and then examine the different types of distributed ledgers.

2.1.2. How is a bitcoin transaction made?

The easiest way to understand the way bitcoin works is walking through how a transaction is made.

Let’s say Alice would like to send 0.5 bitcoins to Bob. The transaction will need three pieces of information: an input (Alice’s bitcoin address) an amount (for example 0.5 bitcoins, equivalent of 582.83 USD as of Feb 26, 2017 at 09:35 GMT (coindesk, 2017)) and an output (Bob’s bitcoin address).
Note the use of the word “address” instead of “account” or “balance”. The bitcoins that are shown on an address are not there, but that address is just the last address that those specific bitcoins (marked with a unique identifier) have been sent to. It is important to understand that the bitcoins are not actually stored on somebody’s address but the sequence of transactions between all the different parties give the final result, that is shown on somebody’s address. (coindesk, 2015).

Alice will need two things to send 0.5 bitcoin: a bitcoin address (Bob’s address) and a private key to her address. An address is a randomly generated sequence composed of letters and numbers. The private key is also a sequence of the same kind, but unlike a bitcoin address, this is secret, only Alice knows it – it is necessary to validate transactions from the input side. (coindesk, 2015)

2.1.3. Inventions of bitcoin: blockchain

As the transaction is created it goes to a pool of pending transactions, from which it is put into a block of transactions that needs to be processed. Then the block goes through a complicated mathematical problem, the proof-of-work mechanism – detailed later – which is necessary to transmit the transaction and validate the block. Then the block is chained to all the previous blocks of transactions that create the “blockchain”. (Driscoll, 2013) As we can see, the blockchain is constructed of timestamped blocks attached to each other. This is what makes the blockchain immutable: it is not possible to alter a transaction from the past without having to change every transaction after that.

Bitcoin transactions are traceable back in time, the ledger is perfectly transparent but it is perfectly private at the same time. How is it possible? As we mentioned before, the bitcoins are not stored on accounts, but are only assigned to addresses – the amount which is assigned to the address is the result of all previous transactions made earlier on the ledger. To verify that on a certain address there is a sufficient amount of bitcoins assigned necessary for the transaction, the system must be able to trace back the origin of every single bitcoin. And it is able to do so: every bitcoin (and every fraction of bitcoin as well) has a unique identifier, that can be traced back through transactions back until its creation. This answers the traceability part. How the bitcoin ledger is perfectly transparent yet private at the same time? The ledger is public, every transaction between every address is visible publicly. However, there is a
catch: as we mentioned before, the addresses are randomly generated sequences, therefore it is impossible to tell that to whom or to what entity do they belong to – this is how the bitcoin ledger is transparent, traceable, yet private.

2.1.4. Inventions of bitcoin: distributed ledger

It is necessary to clarify, how the ledger is stored. It is not stored in a central database, but it is stored in parallel on many “nodes” and is continuously updated with the new blocks of transactions. That is why it is called a shared or **distributed ledger**. Besides the transaction-based timestamped accounting made available by blockchain, this is the other important revolution of the bitcoin. By continuously updating the ledger on every node, the painful and costly reconciliation processes that characterize today’s financial services industry can be spared.

The term distributed ledger and blockchain is often used as synonym. As we can see, they are not exactly the same thing, but since they are always applied together (one without the other is no use, they are so complementary), it is acceptable to use them as synonyms.

2.1.5. Inventions of bitcoin: proof-of-work mechanism

Putting transactions in order is a challenge in bitcoin: it is called the double spending problem. How is Alice prevented from spending a bitcoin again that she already spent once, but the transaction is not transmitted yet? In centralised systems, this is simply decided by the central authority. Here, since there is no central authority, to select which transaction is next, a kind of mathematical lottery is held – a block of transactions is transmitted by solving a complex mathematical algorithm requiring high levels of computing capacity\(^1\) – whichever node solves its version of the block the fastest “wins” – its version of the block on the blockchain gets validated by the rest of the nodes and attached to the end of the blockchain (solving this mathematical algorithm requires high level of computing capacity, but since this algorithm is a so-called one-way problem validating it can be done within seconds). This is how the bitcoin community arrives to a **consensus** that which block would be the next on the chain. It is called the **proof-of-work consensus mechanism**. (Nakamoto, 2008) (Bott-Milkau, 2016)

---

\(^1\) It can only be solved with trial-and-error method
2.1.6. What gives value to bitcoin?

A fiat currency is without intrinsic value that is used as money because of government decree. To a large extent, the acceptance of fiat money depends as much on expectations and social convention as on government decree. (Mankiw, 2015, p. 220) Fiat money was developed essentially to facilitate exchange by using paper instead of gold – then later on the possibility to exchange paper on gold has been left behind, and the use of money in exchange is a social convention: everyone uses fiat money, because they expect everyone else to value it. (Mankiw, 2009, p. 83)

![Figure 1: Bitcoin transaction process flow](source)

In the case of bitcoin the proof-of-work mechanism is what gives its inner value (besides the social convention): the winner node or pool of nodes\(^2\) gets a reward of a certain amount of bitcoins for solving the algorithm the fastest – so essentially the inner value of bitcoin is the computing capacity solving algorithms that is required to transmit transactions – this is why

\(^2\) Nodes (computers or computer servers) can join into pools, merging their computing capacity into one, which raises their probability to solve the algorithm first.
bitcoin is *non-fiat or commodity money* – as opposed to fiat currencies, bitcoin does have intrinsic value (computing capacity) and it is not a government issuing it – in fact there is not even a central authority behind it.

### 2.1.7. Security

What makes bitcoin so secure is that to validate a block, more than 50% of the nodes must agree. So, to hack the system, one must have control on more than half of the nodes (or, better said, half of the computing power present in the network) which is very unlikely. Also, to change a block in the past – to hack a transaction in the past – is even harder. As we have seen before, to hack a transaction in the past, every block must be changed after that point in time. Consequently, one must have to have so much computing capacity at its hands, that is able to solve every block in the past up to the block it wants to alter faster than the rest of the community solves one block. This is practically impossible.

### 2.1.8. Significance of bitcoin

The invention of bitcoin was a very significant event – it was the first blockchain based shared ledger, and as such it had an indispensable role in starting the reform of the financial services industry. However, the importance of bitcoin itself, as a currency, gets often overvalued. It is recent news that the bitcoin reached parity with gold on 3rd of March 2017 – and its true. The bitcoin price per unit (ounce and bitcoin in the case of gold and bitcoin respectively) is now constantly higher. It is a significant comparison, since the bitcoin is often viewed as “digital gold” due to its non-fiat features and inner value. (Blummer, 2016) What everyone forgets about is that the market capitalisation of gold is about 350 times the market capitalisation of bitcoin (coindesk, 2017) (YahooFinance, 2017), but even the average S&P 500 company has twice the bitcoin’s market capitalisation. (Siblisresearch, 2017) Will bitcoin eventually become the digital gold? Probably, but it just isn’t quite there yet.

---

3 1256 USD in the case of bitcoin (coindesk, 2017) and 1199 USD/ounce in the case of gold spot (YahooFinance, 2017)

4 The current market cap of the S&P 500 is $21,351,504.0 million, of the Gold $7,211,306 million, of bitcoin $20,209 million.
2.2. The Archetypes of Distributed Ledgers

As mentioned before, bitcoin is a very specific variation of Distributed Ledger Technology (DLT), which works well as a first “proof-of-concept”\(^5\), but it has many defects, such as slow transaction time, or total anonymity which makes it a catalyst for illegal commerce. On the long term, however it is more viewed as a kind of “digital gold” as mentioned before. A common mistake that many make, is judging the DLT’s capabilities and limits by examining only bitcoin as main point of reference.

2.2.1. What are distributed ledgers?

“A shared ledger is a view of the current state of a marketplace, and also all of the transactions that led to that current state.” (David Birch, 2016, p. 119) With today’s technology, it can be achieved that every participant in a given market stores a copy of the shared ledger – which is essentially a list of every transaction made between \textit{all the participants of the market} – and it is capable to update it with the new transactions in a relatively short time. But, since minor differences can occur due to fraud or errors there is a need for a consensus mechanism. (David Birch, 2016) The consensus mechanism in the case of bitcoin was the proof-of-work mechanism, which is essentially a democratic system to decide, which ledger is needed. It is needed because there is no central authority in the case of bitcoin. However, when a central authority is present (for example: central bank in case of domestic interbank transactions), the consensus can be supervised by that authority.

In the following part of the chapter the goal is to give a general overview of the different kinds of distributed ledgers, and then go into more details in the ones which are relevant to the original question – so the ones that are more suitable for financial services application. Essentially there are two ways to differentiate between distributed ledgers: Public and private

\(^{5}\) bringing an idea to realisation in order to prove its feasibility (Techopedia, 2017)
The shared ledgers more suitable for financial services use are the private shared ledgers. (David Birch, 2016)

2.2.2. Public shared ledgers

If anyone can use the ledger then the ledger is *public*. If only a restricted group of participants can use the ledger, it is *private*. Let’s break down first the public ledgers.

If every user can use the ledger, the users must participate in the consensus mechanism to maintain the integrity of the ledger. We have seen, in the case of bitcoin the users are motivated through monetary incentives on the ledger. But these users need permission from the ledger controllers to participate in the consensus finding process – in the case of bitcoin, they have to solve an algorithm the fastest. This is why this type of public shared ledger is called *double permissionless ledger*.

The main advantage of double permissionless ledgers is that they can be used as a currency which is independent from any state or legal entity but still accepted internationally – mainly in online trading and marketplaces. However – although a new type of double permissionless ledger, the ethereum is becoming more widespread than bitcoin due to its superior smart
contract capabilities and shorter settlement time – they will never replace traditional fiat currencies and remain in the use of somewhat niche target groups.

The second type of public shared ledger is called the permissionless ledger. This is different from the double permissioned ledger regarding two aspects: all members are “permissioned” per default to participate in the consensus mechanism and because contributing to the consensus has some costs, the contributing members are incentivised. However, this happens externally, off ledger. A common example for this is land registry, where the land registry is stored on a shared ledger, and the contributing (consensus making) members are for example the real estate agents (motivated either by law or by monetary incentives). (David Birch, 2016)

The primary benefit of the simple permissionless ledgers is the fact that they can be used as publicly accessible and immutable databases – perfect in the public sector where they are a great tool to provide an immutable database to fight corruption and prevent fraud. A project to fight land-fraud in Honduras with blockchain-based land registry database was run but stalled in 2015 (Shelkovivnov, 2016) but another blockchain based land registry system begins testing in March 2017 in Sweden (Rizzo, 2017).

Having went through the different kinds of public ledgers, it is safe to say that public shared ledgers can’t be applied in interbank transactions due some fundamental incompatibilities: in an interbank system only strictly controlled and regulated members could take part, and the ledger cannot be neither public or anonym. The participants have to be clearly identifiable, however, due to reasons of business privacy for a certain member (bank or other financial institution) only those transactions must be visible, in which the member itself takes part in, so bank A should not be able to see a transaction between bank B and C.

2.2.3. Private shared ledgers

If there is only a certain group of participants who can use the ledger, then the ledger is private or permissioned – in the case of the permissioned ledger updaters need the control of whoever controls the ledger. If not all the members maintain the integrity of the ledger (take

---

6 “A smart contract is a digitally signed, computable agreement between two or more parties. A virtual third party—a software agent—can execute and enforce at least some of the terms of such agreements.” (Morrison, 2016)
part in the consensus-finding mechanism) – so they need further permission to vote for the consensus, then the ledger is *double permissioned*. (David Birch, 2016) For example, if a shared ledger is used for retail interbank transfers\(^3\), then the banks’ customers can see the ledger of the interbank transfers (or at least a part which is relevant for them), but in the consensus mechanism only the banks and financial institutions (and perhaps a regulator) can take part.

### 2.3. Why would financial institutions switch to DLT?

Why would banks use permissioned distributed shared ledgers instead of the already functioning SQL\(^7\) based centralised databases? Blythe Masters\(^8\) said in an interview with Bloomberg: “I had seen the financial crisis unfold, and I had seen the credit derivatives market get operationally ahead of itself, which resulted in systemic risk counterparty exposures. I began to believe that distributed ledgers had the capability to tackle that problem. (...) With private chains, you can have a completely known universe of transaction processors. That appeals to financial institutions that are wary of the bitcoin blockchain. (...) You should be taking this technology as seriously as you should have been taking the development of the Internet in the early 1990s,” (Masters, 2015)

In short, the answer to the upper posed question is efficiency. Currently, every bank has their own IT system with their own method of storing and maintaining data by operating two different ecosystems. Every transaction is stored twice, and costs twice than the necessary to maintain: it is stored once in the sending side and once in the receiving side. Moreover, since no two internal transaction storage systems are the same, discrepancies happen – and the reconciliation process is costly for three reasons:

1. Since the IT environment is not the same, *harmonizing data* is a challenge.
2. If there is a difference in the booked amounts, it is hard to decide, which party is right.

That is why a *central authority* is necessary to be involved, it has the rights to decide.

---

\(^7\) Structured Query Language

\(^8\) Blythe Masters is a former J.P Morgan executive and the founder of one of the largest blockchain startups, Digital Asset Holdings, which is backed by many leading companies in the financial services industry. (LinkedIn, 2017) Creator of Credit Default Swaps, the asset that played an important role during the 2008 crisis, Wall Street thought leader.
3. Usually a central authority uses a ledger, that is independent from the previous two, and it is maintained separately, and consequently it has its own costs.

Thus, even by looking at just one transaction reconciliation, we can safely say that the maintenance, data storage, reconciliation etc. happen in three places simultaneously, so the costs relevant to them are at least tripled as well in comparison to the optimal. The transactions inevitably involve a trusted third party and erasing discrepancies takes precious time and resources. Taking in consideration, that even in the case of a domestic financial market there are not two but many participants meaning many separately maintained ledgers and IT systems, it becomes obvious, why are financial companies so enthusiastic of this technology.

By using a common core ledger – a distributed shared ledger – in a single market, the costs related to data and transaction would be reduced to their fraction. Since all participants share one single ledger, the costs are also shared, moreover reconciliation practically would not be needed anymore: if there is one single ledger, discrepancies are not possible. Of course, banks would probably keep their own IT systems anyway, because a shared ledger cannot perfectly adapt to the inner processes of all financial corporations. However, the related information (transactions date, amount and direction) would come from the shared ledger to these organisational systems (which might of course be swapped for separated blockchain based systems as well) and not the other way around. This saves precious time in transaction processing – today’s standard is two days, but in this way, it could be almost instantaneous.

Moreover, there is one more argument, that financial institutions often mention, when discussing blockchain: Smart Contracts. "Economic transactions on a digital ledger can be programmed to record virtually anything of value, and as a consequence, also any type of financial instrument. It is possible to record the actual business logic that has been agreed to between the parties in a financial transaction." (Masters, 2015) The potential that lies here is enormous. A transactional system based on blockchain could support transactions in an end-to-end manner: concluding the deal, settling it and following up whether the real transfer of assets has happened – or actually satisfying the agreed terms.

Summarized, the following strengths are the reason why banks and financial institutions should switch to Distributed Ledger Technology:
1. **Information propagation** – there’s up-to-date information available for the full network, in almost real time: all nodes share the same source of truth.

2. **Full traceability** – participant as well as 3rd parties (such as regulators) are able to trace back information (ownership and transaction history or origin) on the immutable shared ledger.

3. **Simplified reconciliation** – local access to complete and verified data due to the fact that the information is mutualised – all participants are working from and on the same data in real time

4. **Trusted dispersed system** – it is trustable without a central body through a validation mechanism with digitally signed transactions

5. **High resiliency** – seamless operation without a central system, pervasive and persistent data stored in multiple nodes. (SWIFT, Accenture, 2017)

+1. **Business automation** – business logic can be programmed into the ledger providing a digitally signed, computable agreement between two or more parties. (Morrison, 2016)

These are the reasons why the topic of this thesis is not about whether it would be beneficial for the financial ecosystem to introduce DLT – this has been discussed and proven already – but it is about exploring the feasibility. Introducing an accounting perspective so different from anything else that has been used before for centuries has its challenges on its own, but the change also has a high cost-barrier due to new technologies and compatibility issues and faces challenges on the legal and compliance side as well.

In the following chapters the target is to break down all the pros and cons of this new technology, present some already known use cases and to bring up further potential benefits that could make DLT even more attractive – such as Smart Contracts.
3. Analysing the feasibility of Distributed Ledger Technology adaptation

3.1. Hypothesis

Before getting into the analysis of pros and cons of distributed ledger technology, let’s build a hypothesis: *In the timespan of 2 to 5 years blockchain technology will be used in multiple domestic markets for interbank transfers, and on an international level it will be applied in 5 to 10 years.*

Of course, it is hard to determine for sure, what will happen in the future. That is why the final goal is not to approve or disapprove the hypothesis, but to analyse the feasibility while keeping it in mind and to list all the factors that can influence the likelihood of the completion of this statement either in a positive or in a negative way. The following analysis will heavily rely on reports from specialist professional organisations and authors.

3.2. Current state of Distributed Ledger Technology

3.2.1. SWOT analysis

In the previous chapter, mainly the positive side of the DLT was discussed. The strengths revolve around the great stability of the decentralised network structure and the transaction-based accounting format. Its biggest opportunities are related to reducing reconciliation and transaction costs, diminishing systemic risk, the incidence of fraud, and increase transactional speed by introducing a new business model that enables faster transmission of transaction and automating business logic. However, there are still many challenges that this technology must face. As it is with every new technology, it has many compatibility issues with other already existing systems. The user experience could only be better – it is difficult to use it as a user and the developer user experience is poor. The distributed ledger technology works well with the current niche market sizes – however if it goes mainstream, it must be much better scalable – the current capacity\(^9\) is insufficient. Moreover, besides all these difficulties, it has to earn the trust of institutions to invest in it and convince future end-users.

\(^9\) Number of processed transactions in a given timeframe (Ex: 100.000 transactions per second)
There are some external threats as well, the most important of them being the legal barrier – the fundamentally different accounting logic on which the blockchain operates brings in many legal questions and issues – being aware of the general rigidity of legal systems, this is a legitimate threat: changing the legal approach might be just too difficult for DLT – DLT should adapt to the current legal system, to some extent. The same rigidity can be said of institutions (private and public), and governments that are unable to adopt the technology – but hostile political attitude can also be a barrier for the diffusion of DLT. And finally – although the technology seems to be very stable indeed, failures of the technology can result in abandoning the solution by institutions. (David Furlonger, 2017)
3.2.2. Challenges

According to SWIFT’s\(^{10}\) position paper on Distributed ledger technologies, there are eight key industry requirements of the financial industry towards value transfer, that DLT has to gain before becoming widely utilized in the industry. (SWIFT, Accenture, 2017) \((\text{Figure 3})\)

Let’s define each key industry requirement and the key challenges regarding them.

![Key industry requirements]

\(\text{Figure 4: Financial asset transfer key industry requirements}\\\text{Source: Self-made, based on SWIFT-Accenture report}\)

1. **Strong governance**

Clearly defined roles and responsibilities of the different parties, businesses and technical operating rules. It is key to ensure effective, predictable and sustainable services. The currently functioning permissionless ledgers do not provide the necessary transparency and accountability that is necessary. (SWIFT, Accenture, 2017) However, the better suited

\(^{10}\) SWIFT is a global member-owned cooperative and the world’s leading provider of secure financial messaging services (SWIFT, 2017)
permissioned ledgers\textsuperscript{11} can provide the necessary trust, transparency, accountability and control over participants – there are no working examples yet, however the Hyperledger project\textsuperscript{12} is a well-elaborated implementation.

2. Data Controls

Controlled data access and availability while preserving data confidentiality: personal and business data is sensitive. Since the whole ledger containing all the data is shared between all participants, this raises security questions – currently this is tackled by all participants having a hidden identity. But once the real identity is used everything will become visible. (SWIFT, Accenture, 2017) The solution here can be the use of further encryption, but further development is yet necessary – it is an operational challenge in terms of managing all the encryption keys and validating the transactions. One solution can be the Zero-Knowledge-Proof\textsuperscript{13} algorithms.

Although it is important to mention that not all distributed ledger solutions involve encrypted validation key mechanisms. When all the participants of the ledger are trusted parties (and there might be a trusted third party involved for control and validation as well) the transactional public-private keys and the proof-of-work consensus mechanism are not all that necessary anymore – and so achieving data control will become much more feasible.

3. Compliance with regulatory requirements

The ability to comply with regulatory requirements. Despite keeping transactions private, business use of distributed ledger technology requires compliance with regulators and access for them to investigate transaction records. (Hyperledger, 2016) In the post-crisis environment regulatory requirements increased heavily, and the pressure is continuously increasing. DLT’s compliance with regulatory requirements still requires a significant amount of work – it is not clear yet that who and by whom should be regulated, especially in cross-border cases. Also, it is unclear whether current regulations will be adapted or new will be needed to create. (SWIFT, Accenture, 2017) It is important to mention that regulators approach to the new technology is essentially positive – the new technology promises greater

\textsuperscript{11} See chapter 2.1.3
\textsuperscript{12} Will be detailed later.
\textsuperscript{13} Allows the verification of content without learning anything about it during the process. (Barak, 2007)
transparency for them. Also it is the regulators that has to follow the development of the technology and not the opposite – it is an important challenge to overcome, but compliance certainly not will be an absolute barrier.

4. Standardisation

Standardisation at all levels to guarantee STP\textsuperscript{14}, interoperability and backward compatibility. DLT is an emerging technology, and as such, it lacks standardisation at all levels (technical, data format and smart contracts), not just compared to existing technologies, but also the different, currently existing distributed ledgers are not interoperable.

During future development standardisation will be heavily required, focusing on interoperability, clearing time, speed, cost and reach. Standardisation will raise further questions throughout the transition period from traditional to DLT – interoperability must be ensured also when only a part of the financial firms has adopted the new technology – resulting in interoperability necessity between legacy and DLT environment. Also, the standardisation of smart contracts should happen as well as being able to handle errors in smart contracts.

This brings up potential standardisation questions around

1. Integrating current operational processes into future operations.
2. Creating assets that can function both in the current and future DLT environment.
3. At last deactivating legacy systems.

(SWIFT, Accenture, 2017)

5. Identity framework

To be able to identify parties involved to ensure accountability. A stable identity framework is necessary to ensure the identity of the parties involved in a particular area of business service. This is crucial to provide the necessary trust and the support of claim processes. The currently functioning permissionless ledgers fail to satisfy this requirement in terms of identification and traceability, however, a permissioned ledger could solve many issues regarding transparency, providing a closed system of trusted participants. (Hyperledger, 2016)

\textsuperscript{14} STP – Straight Trough Processing: shift from the nowadays used T+3 settled trading to same-day settlement.
At the moment, on existing distributed ledger networks private keys are necessary to confirm transactions. However, there is no facility to recover keys in case of being lost or revoke keys in case of being stolen. The way to go for the future development to achieve a better identity framework is to use a central Certification Authority (CA) operated by a neutral trusted third party. (SWIFT, Accenture, 2017)

It would be responsible for either revoking and recovering keys or for taking on the role of keys entirely regarding the identification and validation function. Both of the possibilities has its pros and cons: keeping the key solution does preserve the distributed responsibility and authority that comes as natural advantage with DLT, however it can bring up efficiency issues; while handing over the controlling and validation function to a Central Authority would be more efficient, but would concentrate too much power in one hand, which could cause systemic risks.

6. Security and cyber defence

The increasing amount and always more sophisticated cyber-attacks call for improving the ability to detect, prevent and resist them (SWIFT, Accenture, 2017). The proof-of-work consensus mechanism is robust and resistant against cyberattacks – it has been designed with the presumption that several the network’s users are ill-intentioned. But, due to its high computing capacity requirements, it would not be usable in a large scale financial services environment – its cost would outweigh its benefits. Also in closed networks where participant access is strictly controlled (so supposedly no participants are malicious) there is no need for such a strict consensus mechanism, therefore an alternative solution could function.

Another aspect of security is to protect non-encrypted data that is stored by the participants. This is a significant risk for data leakage even in the case of a private ledger. The right solution to this issue us to allow partial or complete data protection on the ledger using selective distribution or encryption, in a way that only the stakeholders can decrypt and execute them. If necessary, even smart contract based business logic can be cryptographically secured. (Hyperledger, 2016)

7. Reliability

Be always available to support financial services. In the case of financial services an extremely high availability and ability to recover quickly after failure is required. A ledger must be able
to operate without interruption for over a hundred years, and still allow discoverability, search, identity resolution and other key functions with adequate responsivity. (Hyperledger, 2016) Due to its nature of shared capacity, the DLT is very reliable – there are many backup nodes to keep the system alive.

But because the system providers are the different nodes, and there is no central control, the availability depends on the participants. Consequently, it is important to define pre-requisites for each and every participant regarding availability, qualification and software update implementation in order to keep the system secure and reliable. The key here is a strong software release qualification management cycle, and enforcing the implementation of it at every participant. There is still R&D necessary to define a perfect software management and release policy in order to make DLT fully reliable – but it is very reliable in the current state as well. (SWIFT, Accenture, 2017)

Also, in a distributed ledger there is the possibility of the formation of “partitions” – two or more different versions of the ledger that occur in the case of network communication problems, resulting in part of the ledger operating separately – after the network communication is restored the ledger gets restored and merged with the partition.

8. **Scalability**

The ledger must be ready to serve large amount of traffic, several thousands of transactions per second. Likewise, the number of nodes and transactors on a given network could become extremely large over time and the ledger must be able to handle such expansion without performance degradation. (Hyperledger, 2016)

Although the proof-of-work mechanism is not scalable due to its low transaction per second rate, and its tendency to develop “forks”, alternative consensus mechanisms solve both of the problems, allowing low latency trading on large volumes. There still has to be a working example to prove this, but the technology seems promising. There are two challenges left: to be able to support High Frequency Trading (HFT) and since the DLT stores all transactions forever, this can pose challenges from the storage and network bandwidth standpoint.

---

15 Parallel versions the distributed ledger, which later will have to be merged into one – a lengthy process.
So, the path for future R&D in the case of scalability is clear: find and test alternative, better consensus mechanisms. This consist of two tests:

1. validation against the CAP theorem\(^{16}\) (Consistency, Availability, Partition tolerance) to understand its limits in practice.
2. Simulation of DLT behaviour in WAN\(^{17}\) environment

(SWIFT, Accenture, 2017)

3.2.3. Business value

![Blockchain Business Value](image)

*Figure 5: Forecast: Blockchain Business Value, Worldwide 2017-2030 (David Furlonger, 2017)*

Although Distributed Ledger Technology still has many challenges to face, threats to avoid and weaknesses to strengthen, according to a Gartner\(^{18}\) prediction published in March 2017 (*Figure 3*),

- At least one distributed ledger-based business will be valued over 10 billion USD in 2022.

---

\(^{16}\) It states that it is impossible for a distributed computer system to simultaneously provide more than two out of three of the following guarantees: Consistency (each node receives the most recent information), Availability (every request receives a non-erratic response), Partition tolerance (No set of failures less than total network failure is allowed to cause the system to respond incorrectly) (Browne, 2009)

\(^{17}\) WAN – Wide Area Network, geographically distributed *private* telecommunications network

\(^{18}\) Gartner, Inc. (NYSE: IT) is the world's leading information technology research and advisory company. (Gartner Inc., 2017)
• The whole technology’s business value will be valued at around 176 billion USD in 2025,
• and the business value will climb to 3.1 trillion USD by 2030.

The last one is also because by 2030, 30% of all customers globally are predicted to be things (robots or computers), and use distributed ledger based technology. (David Furlonger, 2017)

3.2.4. Concluding the current state of DLT

From the analysis of the challenges, it is visible that there are two main things two develop, which were recurring at almost every key requirement:

1. A private, permissioned and selectively shared ledger – only accredited participants can be part of it (banks and financial institutions for example) and the participants can only see those transactions in which they are involved.
2. A better consensus mechanism, that does not require so much time and computing capacity – involving a trusted third party could ease the consensus.

The “blockchain revolution” is not going to happen just from one day to another, but it will take a much longer period (5 to 10 years) and it will not be a revolution, rather just a gradual, but thorough and very significant reform. Entirely changing the technological background of one of the largest and most significant industries, the financial services industry, would take several years even if the technology would be perfectly ready to adapt – which is not the case, although it is developing astonishingly fast.

When the bitcoin (and together with it the blockchain) entered the public consciousness, the experts were talking about the Fintech-blockchain-bitcoin startups taking over the banks. Obviously, this is not the case: it is more the banks taking over blockchain and the distributed ledger technology, and using it to improve their services. Although there are still many challenges to face, the transition is going to happen, it is just a matter of time (and funding).

With DLT can be reached so advanced levels of service quality, speed, transparency, reliability, security, asset management possibilities, which are not possible with the currently used technological standards – but to get there, it will take serious effort.
4. Smart contracts on blockchains

Smart contracts are the “one more thing”\(^{19}\) of the distributed ledger technology, the reason why every industry specialist is so excited about the opportunities that blockchain offers. It is impossible to talk about distributed ledger technology and not to mention the Smart Contract. Because blockchain is not only about time and cost efficiency during the reconciliation process or transactional transparency – without doubt these are very important features. But smart contracts promise such a wide array of future opportunities in terms of automation, faster business processes, further reduced costs, new products that can be now made possible, that in the end this is what truly complements the blockchain technology, makes it an innovation breakthrough and convinces companies’ CEOs to invest into the Research & Development of DLT.

4.1. What is a smart contract?

4.1.1. Defining Smart Contracts

As defined by Nick Szabo, the creator of the term, the idea behind smart contracts is that many kinds of contractual clauses can be embedded into an algorithm, in a way that it makes the breach of contract (punitorily) expensive for the breacher or the breach of contract requires more effort than the profit gained from it. It works in a similar way to the vending machine. The machine takes in coins, and via a mechanism, returns change and product according to the displayed price. Essentially, it is a contract: anybody who has coins is able to participate in an exchange with the machine. Security mechanisms protect the stored coins and contents from attackers, sufficiently enough to allow deployment of vending machines. Smart contracts go beyond that: they propose to integrate contracts in all sorts of asset that is has a value and is controllable by digital means. (Szabo, 1997)

So, in short, a digitally signed, computable agreement between two or more parties. A virtual third party – software agent – executes and enforces the terms of such agreements.

\(^{19}\) Apple’s previous CEO, Steve Jobs used to introduce breakthrough products at his presentations with this figure of speech. (Ewan Spence, 2013)
The smart contracts execute themselves when predefined conditions occur. For a simple example: payment gets received, and the smart contract algorithm automatically sends the goods to the predefined address in the terms.

As early as it was defined in the early years of 1990, just after the worldwide web started to catch on, it was essentially untouched until the blockchain made it possible. Of course, even before the blockchain technology came, there were some imperfect implementations of the smart contract, such as the transaction processing systems of banks use algorithms that resemble smart contracts. (I. Mendelowitz & Brammertz, 2016) However, it is the blockchain technology that has brought the real breakthrough: when the smart contracts are attached to the distributed ledger, they get the DLT’s unique features: immutability, security, transparency and extreme reliability. It is then when the smart contract technology can achieve its fullest potential.

4.1.2. Smart Contract Lifecycle

1. **Recording the terms** between the parties on a distributed ledger, which gets then validated by the validators. It is accessible by relevant authorities and involved companies (Banks, insurers etc.)
2. **Connecting with systems** – internal: banks; external: balance, share prices, etc.
3. **Evaluating**: the contracts pre-defined conditions get evaluated by external factors, such as regulators, auditors. Compliance and reporting has access to data in this stage.
4. **Self-executing** – when the pre-defined conditions get fulfilled by the triggers, the contract self-executes. Compliance and reporting has access to data in this stage as well.

Based on: Capgemini Consulting, 2016

4.2. For what can smart contracts be used at financial services?

4.2.1. Benefits

Smart Contracts attached to blockchains offer multiple benefits when applied at banks or capital markets:
1. **Lower operational fix and variable costs**, which lead to financial products at a higher margin (Capgemini Consulting, 2016) This is essentially the result of automating many processes and eliminating paper from all the contractual workflows and this makes the processes often a lot quicker, and provides more visibility of the asset in the workflow. (Hardjono, 2016)

2. **Faster processes**, that are easier to execute and require much less manual intervention. (Capgemini Consulting, 2016) It is due to lower error rate, taking the paper out of the and of course faster settlement times – the benefit of DLT.

3. **Easier compliance and reporting**, and reduced administration costs (Capgemini Consulting, 2016) There are better opportunities to conduct analyses supporting of risk management, finance, accounting, asset or liability management (I. Mendelowitz & Brammertz, 2016)

4.2.2. Relevant use cases

Some of the relevant use cases in products and solutions for smart contracts that could be used financial services:

1. **Syndicated Loans and Leveraged Loans**– They are still working based on faxes and digital documents, but when stored on blockchain, settlement can be significantly reduced to 6-10 days. (Vandenreydt, 2016)

2. **Collateral, especially Mortgage Loans** - with collateral ownership information, they can be stored in a trusted manner and if payments are missed, smart contract revokes access to collateral. (BBVA Research, 2015), also processing fees can be reduced.

3. **Trade clearing and settlement**, Stock Exchange Market Infrastructure – automated approval workflows between counterparties, calculation of trade settlement amount and automatic fund transfer. (Deloitte, 2016)

4. **Inheritances** – automatic allocation after the verification of death. (BBVA Research, 2015)

5. **Automated insurance claim processing** – error checking, routing, approval, calculating pay-out based on claim and policy. (Deloitte, 2016)

6. **Escrow** – only when the physical asset and ownership has been transferred from seller to the buyer the contract would release automatically the funds to the seller that the...
buyer previously transferred to the contract account. This is already enabled today. (Capgemini Consulting, 2016)

7. **Programmable money** – it can be programmed up to be spent only on certain kind of assets, at a certain geographical area or in between two dates. (BBVA Research, 2015) A good use case could be the use in vouchers and coupons.

8. **Crowdfunding for Startups and SMEs** – this is already in use through several platforms on the public ledger called ethereum\(^2\). It essentially takes out the middlemen from crowdfunding, and substitutes it with a software, reducing the intermediary costs to at its fraction. (ConsenSys, 2015)

### 4.3. Challenges in smart contracts

The two biggest challenges in smart contracts can be generally described as lack of privacy and security of users and transactions, and inflexibility of smart contracts. (Capgemini Consulting, 2016)

It can be said the challenges to be solved before widespread use in the case of smart contracts are often very similar to those of the Distributed Ledger Technology. For this reason, in the following brief analysis only the challenges particular to the Smart Contracts are detailed. There are essentially three main categories of the issues regarding smart contracts: technological, legal and organisational issues.

1. **Technological**

   The technological challenges resound the ones that have been detailed at key the challenges of Distributed Ledger Technology (Chapter 3.2.2), especially regarding scalability (8.) and standardisation (4.).

2. **Legal**

   *The enforcement of smart contracts* in legal circumstances is yet to be elaborated. It is particularly true when the smart contract is on a public, permissionless ledger, where is not

\(^2\) Ethereum is essentially the next-generation of bitcoin (but developed separately). It is an open-source, double permissionless ledger, a cryptocurrency on a blockchain, that runs smart contracts. (Ethereum, 2014)
present any central authority. Consequently, there is nowhere to go in case of legal disputes, that turn up from contracts that have been automatically executed. This is why, also in the case of smart contracts, private, permissioned ledgers, with central authority seem to be a better option. In the case of legal disputes besides the obvious need of a central authority, an automated clause delegation mechanism could reduce friction, by sending the issue to an external adjudicator that resolves the disagreements. (BI Intelligence, 2016)

**Contractual secrecy**, meaning the secrecy of contracts and especially the execution of contracts is a challenge for enterprise-related smart contracts. Transactional records should be seen only by the related participants, but to achieve it, privacy has to be further developed by a better cryptographic key management. (Hardjono, 2016) It is a question that what data should be shared with participants, and when not visible for all the participants, how is authenticity and security of data ensured (Solomon, 2016) – which leads back to the zero-knowledge-proof problem discussed earlier.

**Flexibly altering contracts after agreement** is also a legal challenge. Currently smart contracts work in a way that all aspects of the negotiations are fixed before the transaction. But in real situations, contracts are often imprecise, because the events after the agreement often cannot be predicted. For this reason, smart contracts should be able to allow parties to amend their agreements when at mutual consent (BBVA Research, 2015) – something that paper based contracts can do, whilst smart contracts are still incapable of.

**Liability** and especially impeachment becomes difficult. With smart contracts, there is the opportunity to create decentralised automated versions of the peer-to-peer services\(^\text{21}\). This means connecting people and creating transactions between them without an actual company (and a legal entity) in between them – as a result regulators currently have no one to target. (BBVA Research, 2015)

However, regulators are already actively working on adapting the legal circumstances to smart contracts, and when in permissioned ledgers in a few year time most legal challenges will be probably possible to overcome. One of the first of its kind in these regulatory frameworks is the BitLicence Regulatory framework, that has been published by the New York State of the

\(^{21}\) Services that are typical to the shared economy, such as AirBnb or Uber.
United State in June 2015. (Department of Financial Services, New York State, 2015)

3. Organisational

The lack of talent is becoming such a severe problem, that it can impede or slow down the development of smart contracts. Lawyers that can read codes, or blockchain developers that understand law are very hard to find. Some organisations, startups and universities have already started to provide trainings on the platforms that they support to train “code-lawyers” that are competent in smart contracts. These usually consist on knowledge about blockchain, smart contract, and building enterprise-grade smart contract applications. (Capgemini Consulting, 2016) (Crain, 2016)

Governance will, as we have already seen from different aspects previously, go through radical change. The function of the trusted intermediaries will be replaced by transparency and consensus amongst participants provided by DLT. (Capgemini Consulting, 2016) After the introduction of DLT and smart contracts, even if the need for them will not completely disappear, their significance will drastically diminish. “For private blockchains, several prominent startups like R3CEV and Digital Asset Holdings are working on ‘contract description languages’ to allow the conditions of a complex financial contract to be represented formally and unambiguously in a computer readable format”, says Gideon Greenspan, CEO and founder of MultiChain, a private blockchain platform. (Greenspan, 2016)

4.4. Conclusion of smart contracts on DLT

There are two key takeaways, that can be said, after analysing the opportunities that smart contracts offer, and the challenges that lay ahead.

1. With smart contracts on blockchains, not only further cost cuts and faster transactional and settlement speed is possible, but a level of business automation can be achieved that has been never seen before. We have not talked about the relationship between the Internet of Things and smart contracts, because it is not in the scope of this thesis, but, in many cases the main users of smart contracts will be things not humans – which further develops the idea of business automation. Nevertheless, there are many areas in the financial services as well, where smart contracts could be used right away.
2. The same way smart contracts promise more advantages than plain distributed ledgers, they have more challenges to face as well. The difficulties are not only about whether or not smart contracts are technically feasible, but there are a wide array of legal questions to be solved relating to the lack of legal entities or enforceability – concepts that have been around not just for decades but for centuries or even more. It is not accidental that whilst the concept of smart contracts have been described already in the ‘90s, the real life implementation still lags behind of that of the Distributed Ledger’s that has been invented much later. But probably, with the widespread use of distributed ledger technology and the spread of IoT, smart contracts will also become mainstream.

5. Conclusion and Summary

During this thesis, it was analysed why the Distributed Ledger Technology is so revolutionary, what are its challenges and what prospects it holds. It is a transparent, safe and fast solution to replace todays financial information and communication legacy systems. It will make the transaction processes quicker (or even real time), much cheaper, more transparent, better traceable or with the implementation of smart contracts even partially or totally automated. It is one of the few cases of innovation where both regulators and enterprises are supporting the change. Regulators are supporting it, because with the new technologies their requirements will be much easier to satisfy – compared to todays’ situation where corporations struggle to provide the necessary information required by regulators. Enterprises are supporting it mostly because of the cost reduction on the long term and faster transaction settlement times, but the prospect of business automation is also a significant selling point.

However, the transition to a distributed ledger based ecosystem will be anything but seamless. The most significant issues seem to revolve around standardisation, compatibility, data protection, scalability, governance and legal issues – it is not a short list. Most of these issues are purely technical, meaning that they can be solved in a reasonable timeframe, with a reasonable amount of funds and effort put into it. But some of the challenges require significant change in how companies work today, bringing up issues related to company governance, responsibility and legal frameworks. With distributed ledger technology comes
an intense need for standardisation, that many companies could struggle to adapt to. And smart contracts bring even more difficulties: who will be responsible for automated business conducted by smart contracts automatically? What if it goes wrong? What will be the legal framework applied? Distributed Ledger Technology is yet at its early stage – it is normal that there are still many issues to be solved, the important thing is that the intention is there from virtually all the stakeholders.

Nevertheless, it is safe to say that the transition to Distributed Ledger Technology in interbank financial transfers is feasible to some level in the future – but it is yet too early to tell more, when no proof-of-concepts are live yet. Will the change restrict only to exchange market infrastructure and trading, or will it extend to all bank transfers? Will the change stay on domestic markets or will it extend also to international markets or just the latter? Will the change happen in five years or just in fifteen? As Bill Gates said “We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten. Don’t let yourself be lulled into inaction.” (Gates, 1995)
Bibliography


Vandenreydt, F., 2016. capgemini consulting interview [Interview] (June 2016).