Università degli Studi di Milano - Bicocca
Scuola di Scienze
Dipartimento di Informatica, Sistemistica e Comunicazione
Corso di Laurea in Informatica

Distributed Ledger Technology: analysis of the technology and design of prototypical solution

Relatore: Prof. Claudio Zandron

Co-relatore: Dott. Riccardo Mazzei

Relazione della prova finale di:
Nassim Habbash
Matricola 808292

Anno Accademico 2017-2018

TODO

Abstract

Blockchains have been a disrupting force in the financial market. Popularized by Bitcoin, blockchains, and its underlying technology, Distributed Ledger Technology (DLT), has shaped up to be much more than the foundation for cryptocurrencies.

DLT can have applications in cross-border payments, or financial market infrastructures but its potential is not only limited to the financial sector, as it can enable digital identity solutions, or tamper-proof decentralized records for the flow of any kind of good, service or transaction. More generally, this technology can enable more secure, resilient and efficient systems, making it possible for further decentralization, deintermediation, greater transparency and cost reductions.

However, the technology is still in its infancy and it's rapidly evolving. This coupled with the cost of the migration for existiting longstanding IT infrastructures to a DLT infrastructure poses many new risks and challenges.

The aim of this thesis is to provide an analysis of Distributed Ledger Technologies, with the objective of identifying their risks, opportunities and implementation viability on different scales.

The research work starts from a brief introduction to the technology and how the industry has been adapting to it, with statistical and analytical evidence presented. The thesis then develops on the comparative analysis between the main competing technologies.

In accordance to the research findings, the project also aimed to provide a proof-of-concept design of a solution for a prototypical system answering to at least one identified use-case using the most suited DLT implementation between the analyzed ones.

Objective

The aim of this project was to provide an analysis to Distributed Ledger Technologies, with the objective of identifying their risks, opportunities and implementation viability on different scales. The research work starts from a brief introduction to the technology and how the industry has been adapting to it, with statistical and analytical evidence. The paper then develops on the comparative analysis between the main competing technologies.

In accordance to the research findings, the project also aimed to provide a proof-of-concept architectural design of a solution for a credits interchange system using the most suited DLT implementation between the analyzed ones.

Structure of the thesis

- In the Introduction chapter a general introduction to the Distributed Ledger Technology is given, expanding on its technical design elements.
- In the Business analysis chapter, data on the the actual industry growth of the technology is presented, with statistical data and analysis from different sources.

Contents

List of Figures

Chapter 1

Introduction

1.1 Emergence of the Distributed Ledger model

Ledgers have values as *archives*, or, in other words, their value is their capability of being consulted to check, verify and manage records.

Ledgers have been a central element of commerce since ancient times, and are used to record a variety of informations, ranging from financial assets to real estate properties, but most importantly how these change hands, that is, transactions.

The medium on which transactions have been stored may have changed from clay tablets to hardware storage, but in all this time there haven't been notable innovations to the underlying architecture of the system. Each financial institution (i.e. banks, governments, investment funds) manages its own ledgers, each designed differently based on necessities, goals and customers (the would-be *counterparts* in the transaction), and in turn, the counterparts keep recorded their own views of the transactions.

This duplication of information amongst all parties partecipating in the transaction drives a need for costly matching between each copy of the information, reconciliation and error fixing. The plurality of technology platforms upon which financial entities rely adds to that, creating more complexity and operational risks, some of which potentially systematic.

For example, let's consider the need for a party to transfer an asset, be it cash or a stock, to another party. The transaction itself can be executed in microseconds, but the settlement - the ownership transfer of the asset - usually takes more time, from days to weeks. This length is due to different reasons: the parties don't have access to each other's ledgers, and can't automatically verify that the assets about to be transferred are in fact owned and not counterfeit. So a number of intermediaries are needed as guarantors of the assets and to verify the transaction. A number of steps have to be added just for this trusting mechanism, and in addition, the differences between infrastructures and technologies of each party acting in the transaction can be such that there's always a need for reconciliation process between parties (ie adjusting each ledger to the transaction), increasing costs and length of the operations.

Centralized infrastructures were until recently an unavoidable model, as there were few ways to consolidate technologies without effectively consolidating the financial entities themselves. The industry has been moving toward the standardization and sharing of data and some of the business logic behind the architectures through the delegation

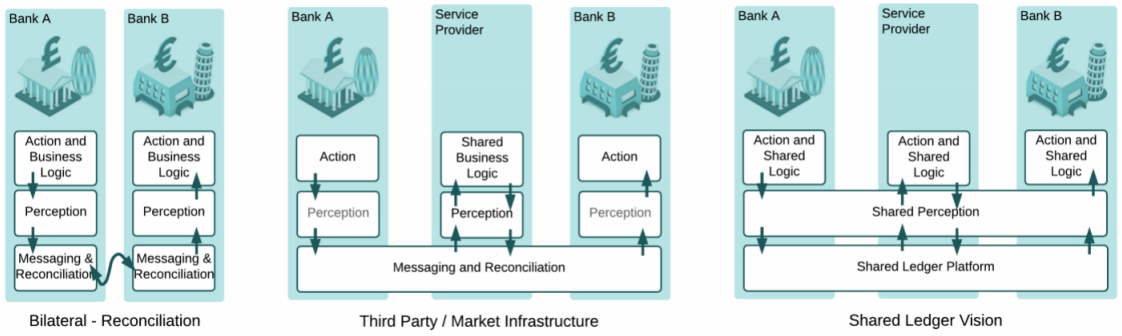

Figure 1.1: Comparison between architectures, Richard Gendal Brown, James Carlyle, Ian Grigg, Mike Hearn, "Corda: An Introduction".

of some part of the process to third-parties, but these steps are still lagging behind the evolution of the technology.

The term Distributed Ledger Technology refers to the processes, protocols and technologies that enable nodes in a distributed network to share data (propose, validate and record) between multiple synchronized data stores, collectively maintaned. The emergence of this technologies has had a stimulating effect in the FinTech industry, prompting the reconsideration of the entities needed in a financial transaction, how should trust be established, the representation of the transaction, the securing of data, and many more. Even if DLT is not the answer in every case, asking these questions alone can be a force to drive progress forward.

1.2 Brief history

In 2008, a white paper (Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System") written by an as yet unidentified person using the pseudonym of Satoshi Nakamoto, outlined a novel approach of transferring cash from one party to another without the need for a known and trusted third-party in a P2P manner, claiming, amongst other things, to have solved the issue of double-spend for digitalized currencies.

The technology outlined in the paper was named Blockchain, referring to the way of organizing data and transactions. Bitcoin has soared in terms of popularity and value through its cryptocurrency market, but is just one element in its whole architecture.

The effort of the industry since the introduction of blockchains has been directed to exploring different ways of leveraging this technology beyond Bitcoin, focusing on the core architecture of distributed record management. This use has gathered significant attention, reflecting the financial industry traditional reliance on multiple ledgers to maintain transactions. The use of DLT would be particularly effective for payment, clearing and settling activities because of the potential for simplification of the settling and reconciliation process between the parties involved.

Some of the resulting implementations of DLTs have been on a steady rise, such as Ethereum, that similarly to Bitcoin has seen a steep rise to the value of its cryptocurrency, Ether, and unlike its predecessor, offers a more malleable enviroment (which is the main

reason Vitalik Buterin created it), allowing for the transfer and recording of other assets like loans or contracts. Other rising implementations include R3 Corda, which showcases architecture heavily based on financial use-cases, IBM Hyperledger Fabric and Digital Asset Platform.

As the research and development of the technology progresses, real-world applications have highlighted some of the challenges associated with these use-cases, including the need for safe, secure and scalable systems.

As of 2018, the impact of DLTs in the financial sector seems still circumvented. Despite strong progress in the research, it would seem that in the near-to-medium term many of the benefits and efficiency gains of DLT are likely to be reaped by start-ups and financial institutions in the developing countries, such as ABRA, a company that offers instant P2P money transfers with no transaction fees through the Abra Network, combining cryptocurrencies with physical bank tellers; Ripple, that similarly deals in commercial cross-border and inter-bank payments with a peculiar dynamic approach towards transactions, where the flow of funds between a sender and receiver can go through a series of partecipating institutions that offer services (making customers, for example, find better foreign exchange transactions); ShoCard, a digital identity card that stores ID information on the Bitcoin blockchain, with the company currently being in the process of developing solution for different use cases like identity verification, fiancial services credentialing or automated registrations for online purchases.

What is a blockchain?

The term blockchain refers to the most well-known configuration of DLTs, and refers to a distributed ledger architecture where the data is stored in entities called transaction blocks, linked with each other through chained encryption. The blockchain itself is the data structure formed by these linked blocks. Blockchains make use of algorithmic methods and encryption to ensure immutability, security and truthfulness of the information.
New additions are initiated by one of the nodes that creates a new block of data, containing the encrypted transactions. Information about the block is then shared on the network, and all participants collectively try to determine the block's validity according to a pre-defined alghoritmic validation method (consensus). After the validation, all the participant can add the block to their copy of the ledger. With this mechanism, every change to the ledger is replicated across the entire network, and each node has a full, identical copy of the entire ledger at any point in time. As the chain grows and new blocks are added, earlier blocks cannot be altered.

The cryptocurrency aspect is what has made Bitcoin garn the most fame. Bitcoin was designed specifically for creating a digital currency free of government control, while also anonymizing the identity of the participants. The consensus process involves the generation of a reward to the node that validated the last block of the blockchain, that being the currency in itself.

Double-spending

Double-spending is an issue unique to digital currencies, and is the risk that a digital currency can be spent twice. Physical currencies do not have this issue, as they're not easily reproduced, but digital information, on other hand, is easily replicated.

With digital currency, there is a risk that its holder could make a copy of the digital token and send it to another party, while retaining the original.

1.3 Distributed Ledger taxonomy

It is emphasized that DLT is not a single, well-defined technology, but as of today there is a plurality of blockchains and distributed ledgers in active development.

DLs can be designed in a number of ways pertaining to main idea behind them and the use-cases they're designed to respond to. Such arrangements usually involve several key technical design concepts that specify how the information has to be kept on the ledger and how the latter has to be updated. There usually are four core attributes of DLTs, these are:

1. The distributed nature of the ledger
2. The cryptographic mechanisms
3. The consensus mechanism
4. The network access permission level

These four elements play are fundamental in ensuring the distributed ledger ability to store and exchange data across different, self-interested parties, without the need for a central record-keeper, without the need for trust amongst the concerned parties, as it is guaranteed by the system itself, and while assuring that no double-spending takes place. Each DLT addresses these attributes in their own specific way, but their abstract taxonomic aspects remain the same.

1.3.1 Distributed nature of the ledger

In its simplest form, a distributed ledger is a data store held and updated by each participant (or node) in a network. The control over the ledger does not lie within any single entity, but within several, if not all the network participants. This sets the technology apart from cloud computing or data replication, which are commonly used as shared ledgers.

There are different configurations to be analyzed regarding how the data is maintained over the ledger. In blockchains, no single entity of the network can amend past data entries, and no single entity can approve new additions to the ledger, which have to go through a predefined consensus mechanism. At any point in time there exists only one version of the ledger, and each network participant owns a full and up-to-date copy of it. After validation the new transaction(s) are added to all the ledgers to ensure data

consistency across the network. In configurations like Corda's, each node maintains a separate ledger. The entirety of the ledger is the union of these ledgers, but isn't public, each peer can only see a subset of the facts on the ledger, and no peer is aware of the ledger in its entirety. This is due to Corda's design, where data is shared only on a need-to-know basis and only to directly involved parties.

Generally, this distributed nature of DLs allows the removal of a trusted central party, increasing speed and potentially removing friction costs and inefficiencies associated with the matching and reconiculiation processes. It also improves security, removing the single point of attack and single point of failure that is represented by the central trusted entity. To potentially gain control over the network, a malicious third party would have to gain control over 50%+1 nodes in the network.

Security risks aren't completely solved: the software layer built over the distributed ledger can become an additional attack surface.

1.3.2 Cryptographic mechanisms

Cryptography is at the core of the DLT. Asymmetric cryptography plays an important role by identifying and authenticating participants, confirming data entries and facilitating ledger updates. Each data entry is hashed, producing the so-called digest. The data is in this way hidden to anyone that is not intended to look at it, as the digest, which looks random and unrelated to the original input, is in fact deterministic, meaning that from one original input there's only one hash possible. Digital signatures, which are a common and robust method used in a wide array of application are used as a means of authentication. Each network participant has a private key, that is used for signing digital messages and only known to the key owner, and a public key, which is public knowledge and used for validating the identity of the sender of the original message. participants proposing changes will authenticate themselves using digital signatures, and the validators will use cryptographic tools to verify whether the participant has the proper credentials, and so on. The validators can be either a counterpart, a third party, or the whole network depending on the type of DL and operation the change refers to.

In the blockchain subset of DLs in particular, encryption plays a fundamental role, as they're essential in the chain encryption mechanism between the blocks that make up the blockchain itself.

1.3.3 Consensus mechanism

The purpose of the consensus mechanism is to verify that the information being added to the DL is legitimate. It is fundamental in handling conflicts between multiple simultaneous competing entries (ie double spending), or take-overs by bad actors in the network. It's a derivative property of the distributed nature of the ledger, and it requires participants in the network to reach a consensus over the information being added. There exist many different consensus algorithms and mechanisms, with different purposes, advantages and disadvantages.

Consensus usually involves two steps:

1. Validation, where each validator involved identifies that the state change is consistent according to the rules of the ledger. This operation may rely on records of previous states or a last agreed state.

2. Agreement, where each validator agrees to the state changes to the ledger. This step involves the mechanisms to resolve eventual conflicts and ensuring that valid changes are made only once, thus ensuring that the whole network is synchronized.

According to the DLT configuration, the mechanisms to avoid double-spendings fit in either of the two steps.

The Bitcoin blockchain uses Proof-of-Work (PoF) to establish consensus. To add a new block to the blockchain, a node has to provide a proof of work. This is a computationally taxing problem, but easy to verify, and is solved by brute-forcing cyptographic hashing algorithms until the correct string that satisfies certain conditions is generated. This process is called "mining". Each miner that produces a valid PoF is then rewarded Bitcoins, which serves as an economic incentive to maintain system operation and integrity.

The Ethereum blockchain uses Proof-of-Stake (PoF). Its process is quite different from the PoF of Bitcoin, as there's no mathematical problem to solve, but instead, the creator of the new block is chosen in a deterministic way based on their stake, that is, how many coins or tokens they possess. A key advantage to this approach is the energy efficiency. The Bitcoin network, for example, requires an annual energy consumption comparable to that of Columbia (57.6 TWh annually). Thus PoS systems are well suited to platforms where there is a static coin supply, without inflation from block rewards. The rewards consist only in the transaction fees.

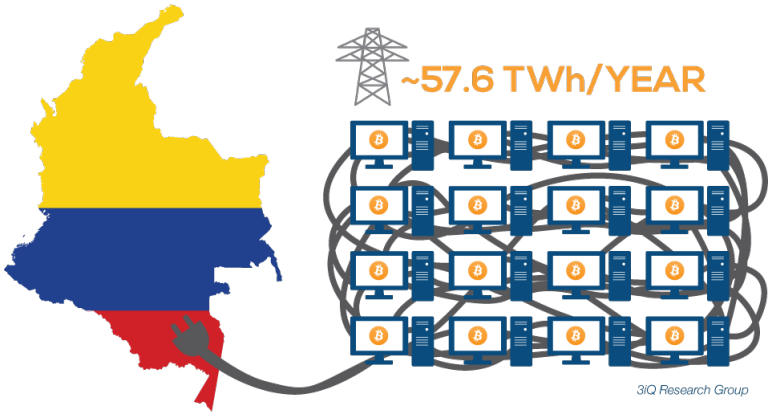

Figure 1.2: Data as at April 3rd, 2018. Retrieved from https://digiconomist.net/bitcoin-energy-consumption

The Corda distributed ledger, utilizes a unique "pluggable" consensus service, due to its peculiar distributed ledger architecture. It divides consensus in two types, validity consensus and uniqueness consensus. Given a proposed transaction, the first type of consensus checks whether the two parties satisfy a set of validity conditions, going back through all the parties' transaction histories, while the latter has the purpose to avoid double spend, and the consensus is provided by a Corda network service called "Notary", by attesting that, for a given transaction, there hasn't been proposed another competing one.

1.3.4 Network access permission level

The partecipation in the DL network can be open (permissionless) or permissioned. Bitcoin and Ethereum are the most prominent examples of completely permissionless blockchain, where participants can join or leave the network at will. This plays as one of their strengths, as a large, open permissionless system with a large number of nodes incentivized to validate new changes to the ledger and accurately and establishing a consensus is directly related to its network security (1.3.3).

In permissioned DLs its members are pre-selected by someone - an owner, or a network service - who controls network access and sets the rules of the ledger. The regulations of network access usually permit the use of a non-computationally expensive consensus mechanism, as there is no need for any trust between participants. This, however, means there's now a centralized trust entity playing a coordinating role and bearing the responsibility over the trusting mechanism. In permissioned DLs it's possible to have different degrees of transparency over the ledger, and faster transaction processing (thanks to the lighter consensus algorithm) allows for higher transaction volumes.

The identity verification needed for the access solves some problems with governments and regulators with concerns about the identity verification and legal ownerships clarifications.

Permissionless DLs have open access to the network, so anyone can join and leave as they wish. There's no central owner or administrator, the ledger is wholly transparent and the security is established by having a large scale network. It is required to have a complex consensus algorithm to guarantee the integrity of the information, and there are some legal concerns over the lack of ownership, as no legal entity owns or controls the ledger.

Some industry players make distinctions between public/private, in term of access, and permissioned/permissionless, in term of roles in the network. For example, Ripple has a permissioned ledger, but the data is validated by all participants, therefore being a public, permissioned ledger. Corda, on the other hand, has a permissioned ledger, but the data is validated only by a set of participants (those which the data concerns), hence being a private, permissioned ledger.

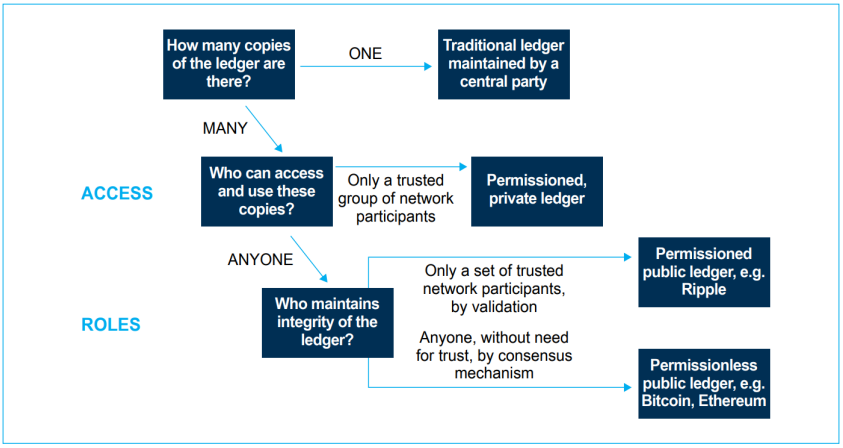

Figure 1.3: Network Access Ledger Taxonomy, Dave Birch, "Distributed Ledger Technology: beyond block chain".

1.3.5 Roles

Nodes in the network may play a variety of roles, depending on the participants intentions or technical arrangement of the DL. The Committee on Payment and Market Infrastructures of the Bank for Internation Settlements proposed a generalized framework, with the following different, non-exclusive roles for a node:

1. System Administrator: node controlling access to the system and provides dispute resolution and notary services. This role is not required in permissionless DLs.
2. Asset Issuer: node enabled to issue assets. In the Bitcoin blockchain, there's no entity playing this role as the system creates assets (Bitcoins) by itself, according to its rules.
3. Proposer: node enabled to propose ledger updates.
4. Auditor: node enabled to view the ledger, but not to make updates. Can be used by regulators or supervisors.
5. Validator: node enabled to validate requests for addition of transactions in the ledger. This role is performed by the consensus mechanism in permissionless DLs.

What are smart contracts?

Smart contracts are self-executing contracts with the terms of the agreement between two parties of a transactions, written as code. The code and the agreement exist distributed across a distributed ledger network. Smart contracts allow for trusted transactions and settlements to be carried out among different and possibly anonymous parties without the need for a central authority, legal system or enforcement mechanism. They render transaction transparent, irreversible and traceable.

Chapter 2

Business analysis

2.1 Industry growth

2017 has been a year of exponential growth for the cryptographic asset market (term indicating the cryptocurrency market enabled by certain configurations of DLT). The outlook for 2018 seems to be set on the creation of solid regulatory frameworks required to provide consumer protection and guidelines.

Within less than a decade, the industry of cryptoassets has developed into a thriving ecosystem with a total market capitalisation of over 300 billion USD. The focus the cryptographic asset market is receiving through media and political coverage (Cryptoassets have topped the G20 agenda in March) has put increasing pressure on the actors playing in the market to match the needs and valuations from governance and financial institutions (the latter being players themselves).

It can be identified a drive from the investment banking industry (hereon sell-side) born out by the investment and participation in big consortia like R3 (which developed Corda) and DL platforms like Digital Asset. Institutional investors (hereon, buy-side) seem to be falling behind, and the risks this poses are of being presented with technology architectures with terms dictated by the sell-side self-interest.

The Bank of England identified this threat in a recent paper *"... if a DL (or other) technological solution for settlement ultimately succeeds in replacing existing settlement methods, it is likely to be characterised by network externalities and decreasing average costs. This suggests that the industry may well retain its high degree of concentration. It is possible and likely that a small number of Central Securities Depositories (CSDs) will be replaced by a small number of DL network providers and as a result future settlement services may be associated with some form of monopoly pricing"* Evangelos Benos, Rodney Garratt, Pedro Gurrola-Perez, *The Economics of Distributed Ledger Technology for Securities Settlement*. The buy-side failure to action may end up delegating to the sell-side the most of the definition and development of DLT infrastructure, the sell-side being a party with potentially diverging interests from them, while if it actually ended up participating in the development and research of DLT it could add another strong player in the industry with a sizeable budget to invest in the technology.

2.2 Governments stance

It is fair to say that DLT has been on a steady rise in the governments' agenda in light of its saving, automatization and security advantages. Central banks around the world are exploring DLT-based digital currencies - UK, Russia, Sweden, Canada and China's central banks are assessing risks and benefits of issuing fiat currencies backed by digital currencies, and investigating their potential effects on the economy and on financial stability.

The UK Government's Office of Science published a major report on DLT in January 2016, Dave Birch, "Distributed Ledger Technology: beyond block chain", assessing the possibilities of DLT use in private and public areas. The Department for Work and Pensions in the UK has been testing from June 2016 the use of DLT for welfare benefit payments, that trough a phone application lets welfare claimants manage their benefit money, having transaction recorded on a DL with the aim to create a more solid and efficient welfare infrastructure preventing frauds.

The Estonian government has been experimenting with DLTs for a long time, as apparent from its Estonian Government, *E-Residency* platform, where it's possible to verify government records like birth or marriage certificates, which are only a couple of the services provided by, as the e-Residency project seem to be trying to encompass a whole variety of utilities, like opening a bank account or starting a company (in Estonia), but most importantly, providing a form of transnational digital identity, so far as to having NASDAQ partnering with the platform to enable secure e-voting in shareholders meetings.

By 2020 Dubai wants to become the first government in the world to conduct all of its transactions using blockchain. The emirate estimates that adding visa payments, license renewals and other documents to the blockchain could save 1.2 billion EUR annually in document processing alone, and also cut CO2 emissions and redistribute 25.1 million hours of economic productivity.

The European Union Intellectual Property Office (EUIPO) is investingating how blockchain could combati counterfeiting, which costs the EU about 60 billion EUR each year according to the agency. In June 2018 the EUIPO organized a Hackathon competition in Brussels to develop a series of anti-counterfeiting blockchain solutions, drawing

Sell-side and Buy-side

Sell-side and buy-side are terms belonging to the financial investment world.
Sell-side refers primarily to the investment banking industry. It refers to the key function of the investment bank - namely helping companies to raise debt and equity capital and then sell those securities to investors. The investment bank role is that of a seller of corporate securities to insititutional investors.
Buy-side broadly refers to such insititutional investors, such as mutual funds, hedge funds, insurance companies, endowments and pension funds. They raise money from investors and invest that money across various asset classes using a variety of different trading strategy.
As of 2014 the estimated flow of money between the two sides is of approximately 227 trillion USD in global assets.

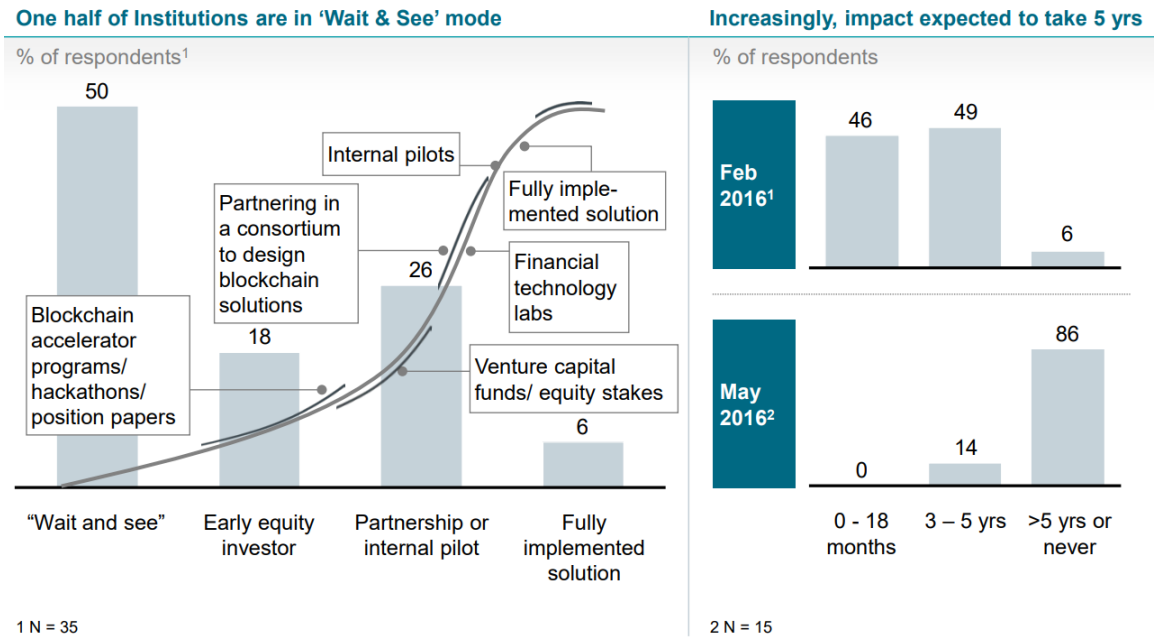

Figure 2.1: Infographic on the industry response to DLT, based on survey of senior executive leadership in financial institutions, Feb 2016 and May 2016, McKinsey & Company.

support from specialists in law, IP and anti-counterfeiting.

Briefly, other relevant government-backed applications and researches include the USA's Food and Drug Administration's exploring blockchain solutions for patent sharing, Denmark's Liberal Alliance blockchain voting platform and Georgia's blockchain land registry project.

2.3 Financial stance

The two biggest trends in DLT development seem to be:

1. Commercial FinTech startups developing applications for different purposes utilizing public blockchain infrastructure, like BitCoin and Ethereum.

2. Industry consortiums researching and developing private, permissioned distributed ledgers to address a set of industry-specific enterprise use-cases.

A survey by Greenwitch Associates, Greenwitch Associates, *Addressing the Latest Trends in Distributed Ledger Technologies*, gathering 400 market partecipants (as in financial companies, funds, etc) working on DLT has tried to assess opinions on the key trends and issues in the current state of DLT development. The report finds engagement across the sample at 63%, with Market Infrastructure providrs in the high end with 75% engagement, and Asset Managers in the bottom, with 32% engagement.

This presents a picture of lagging in the adoption of the technologies, due to the competition of other competing technologies. According to a recent survey from Keith Hale, Sern Tham, *A Turning Point for the Global Asset Management Industry - The Multifonds Every Fund Survey 2017*, big data analytics, AI and robo-advice are currently

higher up in the Asset Managers' agenda than DLT, accounting for more than half (55%) of responses, explaining that it is "probably down to the fact that these new technologies are relatively easier to implement than more revolutionary DLT concepts".

But as Dr Ian Hunt, Chris Mills, *Distributed Ledger Technology – An Emerging Consensus on the Buy-Side* reports, recent evidence shows that the industry is notwithstanding operating in the research and development department. Examples (extrapolated from the report), include:

- Schroders announcement that they have joined the Hyperledger Project
- Northern Trust's implementation of a blockchain platform for Private Equity fund administration in partnership with Unigestion and IBM
- BlackRock's announcement of their intention to Blockchain-enable Provider Aladdin, a private platform / dashboard to streamline transactions with BlackRock's Custodians
- The launch of a Blockchain-based solution for syndicated loan servicing by Synaps (a joint venture of Ipreo and Symbiont), with involvement from Asset Managers including Eaton Vance and Alliance Bernstein
- Calastone's launch of Blockchain-based distributed market infrastructure
- FNZ 's development of FNZChain as a private blockchain for Asset Management registers
- SETL's launch of Iznes, in collaboration with various asset managers, as a Pan-European Distribution and Transfer Agent Platform for fund subscriptions, distributions and settlements
- The announcement from Natixis in July 2017 that they had successfully sold funds directly to clients through FundsDLT, a fund distribution platform developed by a partnership of the Luxembourg Stock Exchange / Fundsquare, InTech and KPMG;
- The news that SEB are working with NASDAQ on the development of a trading platform for Swedish mutual funds
- The rise of crypto fund launches in 2017, representing the fastest growth of any hedge fund sector in the industry's history, Hedge Fund Alert, *Bitcoin Rise Ignites Crypto Fund Explosion*

2.4 Adoption considerations

It is clear that many market players and public authorities have embarked on a learning process that has familiarised many of them with the foundations of DLT. Investment in the technology has started to gain momentum, and is expected to grow at a very high pace in the near future.

The technology has the potential to support attractive models for the tech-savvy generation of consumers who wants more control over their investments and finances, delivered via their favoured media, thus providing a strong and agreeable user base.

The effective use case execution of said solution will depend highly on the collaboration among players in an ecosystem. In the financial services case, a strong interest has been outlined by banks and financial institutions and fintech companies, with a 400 million USD estimated capital market spending by 2019. It is believed that right now the biggest challenge for DLT is going to be shaping a regulatory environment and the agreement on key standards and active collaboration across all required players.

It is hence believed that entering the market in this moment seems to be the prime time to ripe the benefits provided by the assessing ecosystem to solidify a strong and longstanding position among current and future competing solutions.

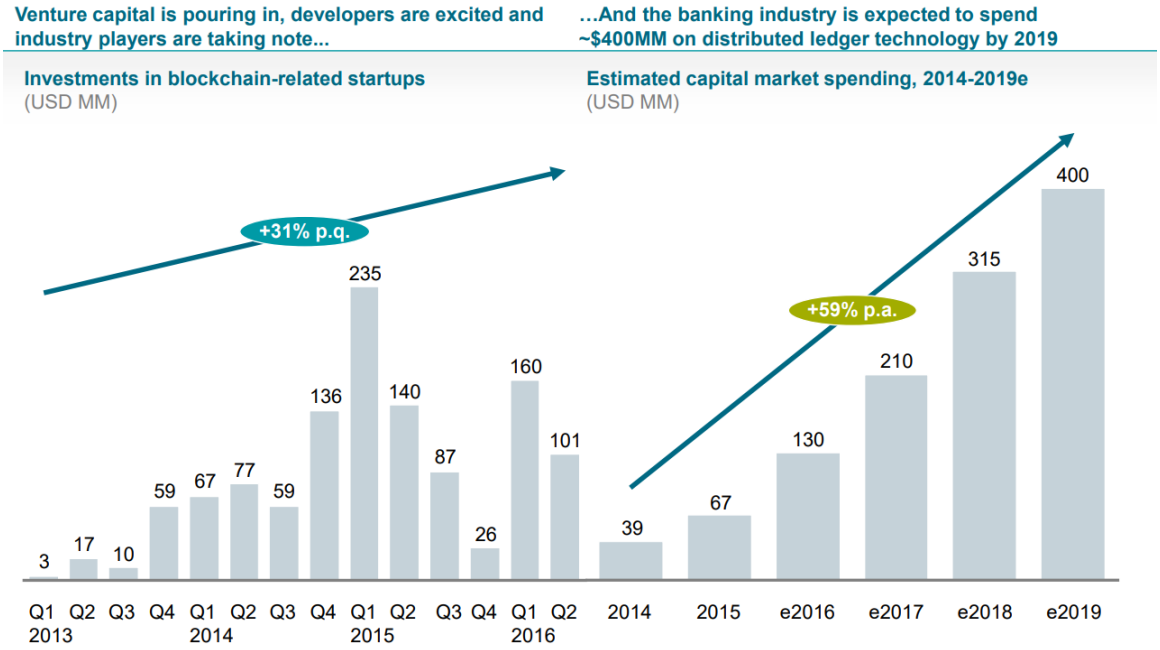

Figure 2.2: Infographic on the investments in DLT development, based on data from AITE Group, Tabb Group, CoinDesk

Chapter 3

Comparative Analysis

This chapter aims to analyze three major DLTs: Ethereum, Corda and Hyperledger. It will provide an overview of each DLT, and then dive into a comparison between the technical aspects of each, in order to showcase the major differences among them.

3.1 Ethereum overview

Ethereum has one of the biggest following among users and developers, with more than a thousand applications already built on top of the blockchain. It was developed as a permissionless public blockchain, where anyone can build application or write smart contracts using its own programming language, Solidity. Ethereum's development team's goal was to provide a generic toolbox for providing support to a wide range of decentralized applications, with a particular emphasis on situations where rapid development time, security and of different applications to efficiently interact are important.

The structure of the Ethereum blockchain is very similar to Bitcoin's. Every node on the network stores a copy of the entire transaction history. With Ethereum, every node also stores the most recent state of each smart contract, in addition to all the transactions.

3.2 R3 Corda overview

Corda is a DLT backed by R3, a consortium made up of many big financial institution. It was developed as a global ledger, with its main goal is to provide an architecture to enable frictionless, well-regulated, reliable and private agreements between parties. Corda was developed specifically on financial use-cases, its main field of application being the financial services industry.

3.3 Hyperledger Fabric overview

Bibliography

[1] ABRA. *Abra*. URL: https://www.abra.com/.

[2] Dave Birch. "Distributed Ledger Technology: beyond block chain". In: (2016).

[3] Dr Ian Hunt, Chris Mills. *Distributed Ledger Technology – An Emerging Consensus on the Buy-Side*. URL: https://www.ibm.com/industries/uk-en/banking/pdf/Distributed_Ledger_Technology.pdf.

[4] Estonian Government. *E-Residency*. URL: https://e-resident.gov.ee/.

[5] Evangelos Benos, Rodney Garratt, Pedro Gurrola-Perez. *The Economics of Distributed Ledger Technology for Securities Settlement*. 2017.

[6] Greenwitch Associates. *Addressing the Latest Trends in Distributed Ledger Technologies*. URL: https://www.greenwich.com/corporate-banking/addressing-latest-trends-distributed-ledger-technologies.

[7] Hedge Fund Alert. *Bitcoin Rise Ignites Crypto Fund Explosion*. URL: https://www.hfalert.com/search.pl?ARTICLE=175427.

[8] Keith Hale, Sern Tham. *A Turning Point for the Global Asset Management Industry - The Multifonds Every Fund Survey 2017*. 2017.

[9] Richard Gendal Brown, James Carlyle, Ian Grigg, Mike Hearn. "Corda: An Introduction". In: (2016). URL: https://docs.corda.net/_static/corda-introductory-whitepaper.pdf.

[10] ripple. *RippleNet*. URL: https://ripple.com/.

[11] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". In: (2008). URL: https://bitcoin.org/bitcoin.pdf.

[12] ShoCard. *ShoCard*. URL: https://shocard.com/.