POLITECNICO DI TORINO

Facoltà di Ingegneria

Corso di Laurea in Engineering and Management

Tesi di Laurea Magistrale

Blockchain implementation for impact investment

Relatori
Ing. Sebastián Cea Echenique
Ing. Valentina Gatteschi

Candidato
Fabio Cofano

Anno accademico 2018-2019

Abstract

This dissertation delivers a general overview over blockchain technology and examines the impact that this technology can have in the current economy, by focusing over impact investment sector.
The thesis includes a technical part where the main blockchain features are analyzed, explaining a blockchain trilemma, possible designs and use-cases in the impact investment sector, a blockchain implementation in a Chilean NGO organization in the impact investment industry and a model that describes how a rational user chooses whether a Proof-of-Work or a Proof-of-Stake blockchain for its use-case.
The thesis proposes that a blockchain implementation in impact investment could lead to reduce inefficiencies of the sector.

KEYWORDS. Blockchain, Impact investment, Distributed ledger technology, Proof-of-Work, Proof-of-Stake.

Acknowledgements

I would like to thank the professor Sebastián Cea Echenique and his team who supported my work. I am also grateful to Pontificia Universidad Católica de Valparaíso that gives me the opportunity to attend classes and develop the thesis.

I would like to thank also the ing. Valentina Gatteschi who support me for the development of the thesis

I would like to thank my friends and my family for supporting me spiritually throughout writing this thesis and my life in general. Last but not the least, I would like to thank Chile and all the people who have shared with me this experience

Contents

List of Figures

Chapter 1

Introduction

1.1 Background

A peer-to-peer (P2P) system is a decentralized business model where individuals interact and transact goods and services directly with each other. These kind of markets “have emerged as alternative suppliers of goods and services traditionally provided by long-established industries" (Zerva et ali 2017). The growth of this platforms is due mainly to technological innovations that have brought lower transaction cost and increase transparency and easier access. The main technology that has permitted the spread of peer-to-peer business models is the internet. This technology allows people to transfer information and data in a secure way thanks to central third-parties that certify transactions.

Having many intermediaries involved in transactional processes that act as a trusted party is time and cost-intensive.

> Having many intermediaries“ leads to duplication of costs for record-keeping and often involves substantial costs for reconciling such records. Cutting out intermediaries could substantially reduce post-trade processing costs" (Chiu, J. and T. Koeppl 2018).

Broadridge (2015) evaluates that the expenses in processing trades in the financial industry is roughly $17bn to $24bn per year. Intermediation occurs in centralized markets where there is the need of a middleman who acts as a mediator in order to guarantee trust between unknown different parties.

Centralized economy’s structure leads to inefficiency and also expose companies as a single point of failure in case of data breaches, hacking and fraudulent use of private information.

> “A 2016 study of large companies estimated that cybercrime costs the

> average large US company $17 million. The global average is US$9.5 million" (Ponemon Institute Research Report, October 2016).

Another problem that affects centralization is the monopoly over the users' data, that nowadays becames a profitable business. According to a Mckinsey (2017) survey, data monetization efforts contribute more than 20% to more than one third of high performance company revenues.[1] The most recent scandal about improper use of users' data involved the biggest social network company Facebook that have shared data with Cambridge Analytica which used this information *to target voters with hyper-specific appeals* (Fortune 2018).

Thanks to the digital revolution we are seeing how the power is shifting from institutions to customers. The technology that threatens to disrupt markets and institutions is called blockchain.

> "A blockchain is essentially a decentralized [and distributed] peer-to-peer (P2P) network of transaction confirmations and ownership transfers, without a central authority or intermediary" (OECD 2018).

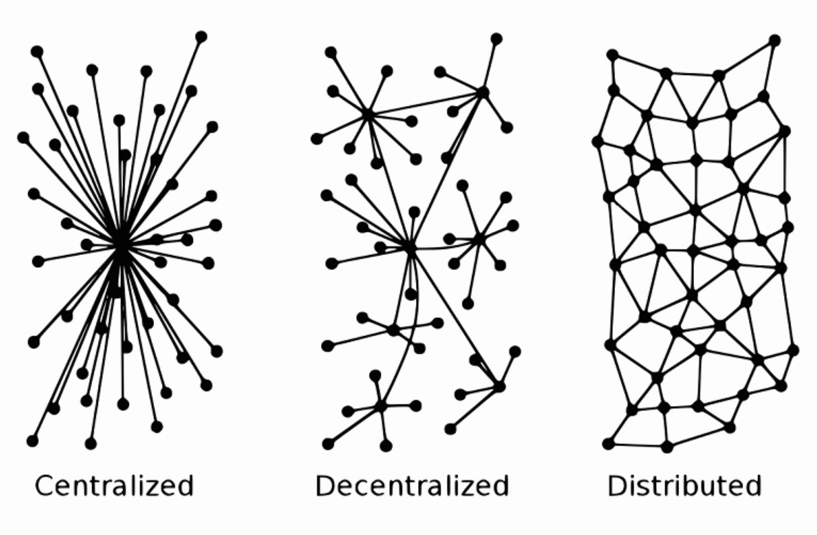


Figure 1.1. Different Types Of Business Models [51]

It is a combination of three well-known technologies: distributed ledger, cryptography and smart contracts. All the transactions are shared and hold between

[1] McKinsey explanation is "High performers are organizations that, according to respondents, had annual growth rate of 10% or more for both organic revenues and EBIT over the past three years."

the different nodes and once they are validated they are stored in blocks and linked with the previous blocks. This chain-like architecture permits to ensure the immutability of the transactions, preventing tampering and enhancing accountability.

“Because of its immutability and decentralization, blockchain has the potential to create transparency, provide distributed verification, and build trust across multiple systems" (Lapointe and Fishbane 2018). Different from internet that enables only the transfer and publishing of digital information, blockchain features lead to secure transfer of value and data, authenticate the ownership of assets, making them unique and traceable, enhancing cyber-security and privacy.

It is possible to identify three different stages of the blockchain technology. Blockchain 1.0 was born with Bitcoin and then was improved by other cryptocurrencies. Blockchain 2.0 saw the integration of more sophisticated smart contracts thanks to Ethereum (www.Ethereum.org) and is about registering, confirming, and transferring contracts or properties. “Smart contracts could enable the creation of new kinds of organizations, such as decentralized autonomous organizations (DAOs), by encoding the rules for making decisions and managing groups of people" (Gatteschi at ali 2018). In Blockchain 3.0, the application field is focused on social impact initiatives as those in government, health, aid, philanthropy, etc.
Blockchain is a foundational emerging technology that is receiving increasing attention from different kind of industries where 43% of companies call it one of their “top 5 strategic priorities" (Deloitte 2018).

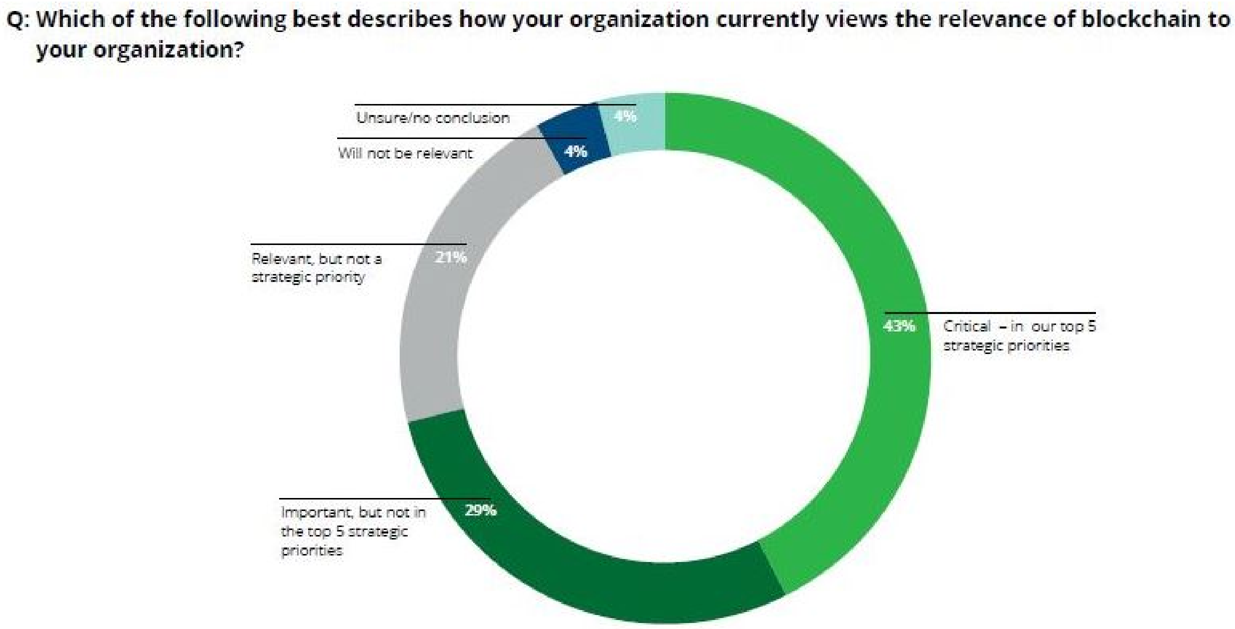


Figure 1.2. Deloitte - Blockchain Relevance Within Organizations [26]

According to a PWC (2018) survey, 84% of organisations have some involvement with blockchain technology, where 32% of them are in the development stage, 10% in pilot stage and 15% are in the live stage and seeing United States and China as blockchain leaders. The main industry involved in the implementation of blockchain is the Financial sector. Others are Industrial products and manufacturing, Energy and utilities and Healthcare (PWC 2018).

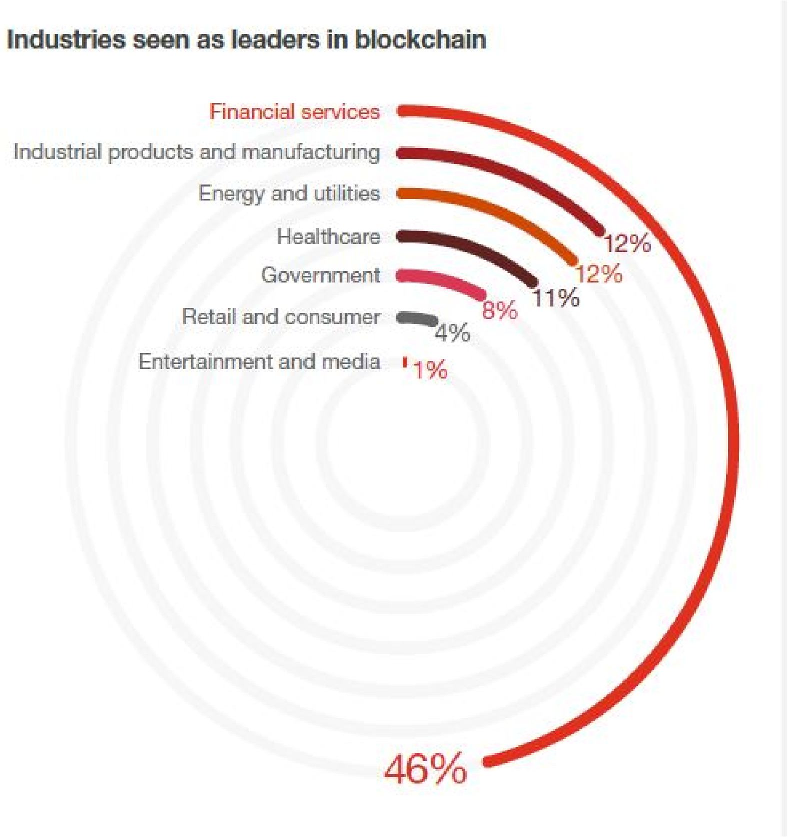


Figure 1.3. PWC - Industries Involved In Blockchain Investment [25]

In the last 2 years there have been Blockchain initiatives dedicated toward social impact, in which “34% were started in 2017 or later, and 74% are still in the pilot or idea stage. But, 55% of social-good blockchain initiatives are estimated to impact their beneficiaries by early 2019" (Galen and El-Baz 2018). The unique combination of blockchain’s attributes as trust, immutability and transparency allow it to be suitable for impact investment, improving digital identity, asset tracking and organization efficiency. For Impact investors, "the ability to measure and demonstrate the impact of portfolios, individual investments, and impact organizations has become increasingly vital" (Social Impact Investment Taskforce 2014). Blockchain has the potential to disrupt this sector. Until blockchain revolution, measuring and evaluating impact data has been economically or technically unfeasible in a cost-effective way. instead nowadays, this technology, by increasing accountability, transparency and efficiency, ensure that the right services and goods will be delivered to the targeted beneficiaries.

Companies are facing different barriers that are slowing down the implementation of this technology. “The most common barriers for the adoption of this technology are regulatory issues, replacement or integration with legacy systems, potential security threats, and uncertain return on investment" (Deloitte 2018).

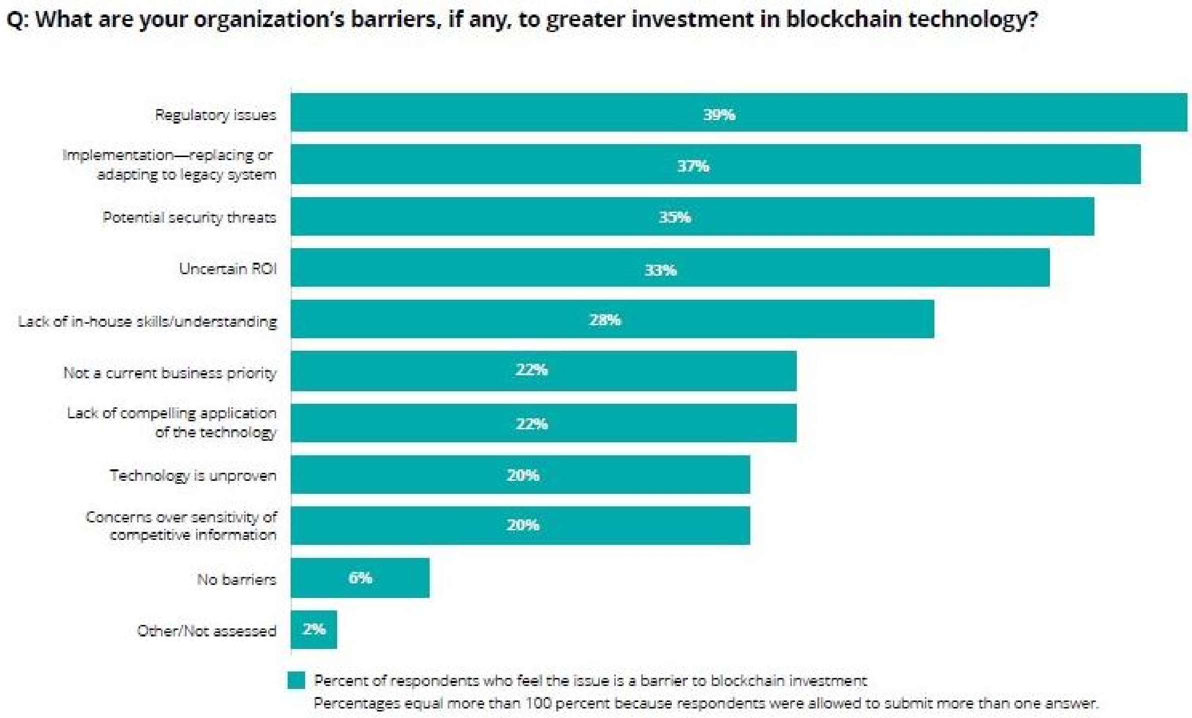


Figure 1.4. Deloitte - Barrier To Adoption [26]

There should be cooperation

> “to develop a consistent regulatory framework that enables businesses to innovate and develop the technology in a competitive environment, subject to rules that preserve fundamental values such as safety and integrity. To do so will require defining best practices, coordinating to prevent regulatory arbitrage amongst governments, and cooperating to develop relevant standards" (OECD 2018)

Despite the potential of blockchain applications, since it is not a fully mature technology, some experts believe that it is overhyped. Their application outcomes often could be achieved with already-mastered alternatives. It is not always worth considering a blockchain-based solution because it also present downsides that should be evaluated carefully. According to Galen and El-Baz (2018) “Of the blockchain initiatives researched, only 20% are providing a solution to a problem that could otherwise not have been solved without it, 66% say that blockchain solution is an improvement over other methods of solving their problem and finally 14% say blockchain is one way to solve their problem, but others may be better."

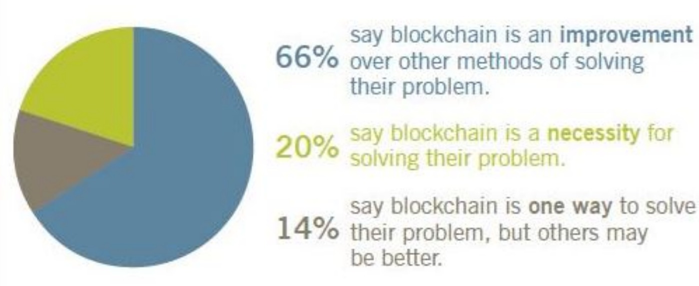


Figure 1.5. Galen and El-Baz - What Does Blockchain Enable? [17]

1.2 Thesis goals

The purpose of this thesis is to analyse blockchain technology and how its implementation can potentially disrupt impact investment sector. The paper provides several possible use-cases for impact investors and a practical implementation in a chilean NGO. The thesis is structured as follows. Chapter 2 discusses the basics of blockchain technology, analyzing its main characteristics as cryptography, consensus model and smart contract. Chapter 3 gives a personal interpretation of blockchain trilemma and presents a possible way to break it. Chapter 4 presents a model aimed to analyze how a rational user chooses between different blockchain technologies. For instance, Proof-of-Work or Proof-of-stake consensus model, according to which is more suitable for its project. There are use-cases where decentralization and security is a critical factor with respect to cost and time efficiency. This chapter also analyses how different rational users change the network choice by varying the main characteristics of the blockchain, as the magnitude of noise over the technology's quality, the transactions' efficiency and the influence of network externalities. Chapter 5 analyzes the main initiatives dedicated toward impact investment sector and also evaluates different design solutions in order to understand the correct trade-off between blockchain features. In chapter 6, there is a practical application of the blockchain technology in an NGO organization located in Chile. It will be analysed how a organization operating in the impact investment sector can implement a blockchain network in order to overcome its main problems: transparency, traceability and accountability. In order to have an overview of the impact investment sector, an investigation was carried out on the possible consequences due to blockchain network design and the possible use-cases of this technology in this sector. Finally, chapter 7 presents conclusions.

Chapter 2

Blockchain technology

Blockchain is a digital decentralized distributed ledger acting as an open, trusted and shared record of transactions among different unknown parties. All nodes have identical ledgers and they are responsible of validation and authentication of the transactions depending on the consensus model. The accepted transactions are stored in "blocks" and are linked sequentially where each block depends on the previous one. This chain-structure allows to create an historical record of transactions not allowing the tampering of past data.

This technology is also based on two fundamental tools that allow its operations: Cryptography and Smart Contracts. Cryptography is composed by hash algorithms and public/private keys and it is applied to keep transactions secure and to enhance privacy. Smart contract is a program code, recorded in the blockchain as a transaction, that is execute when specific conditions are met."This is potentially a very powerful tool not only to automate contractual transactions but also to automate legal supervision and enforcement"(OECD 2018).

Blockchain can be customized with respect to the degree of decentralization, scalability, participation, write permissions and data access. "Hence, making intentional, ethical decisions in blockchain design and implementation into an overall system is crucial to ensuring the technology's potential for transformative change"(Lapointe and Fishbane 2018). The right blockchain characteristics depend on the industry and corporation's goal, it involves a series of tradeoffs based on its key attributes that are highly interdependent.

2.1 Blockchain types

There are two main types of blockchain 's architectures: private and public. They differ mainly in terms of read/write permissions.

In a strictly private blockchain, only a single centralized entity has the write permission, so there is only one writer. In this model the writer is disciplined only by the readers. Readers could punish an incorrect action of the writer, as the rise of the fees or a change in the ledger's rules, by migrate in an other ledger. In a general private blockchain, called also "permissioned blockchain", the write privilege belongs to different entities, so there are different writers. In this model the writers are disciplined by both other writers and readers. The process of adding blocks by the writers is done by following a predefined algorithm, usually achieved through the selective endorsement process (Laura Gargolinski 2018). The read permission may be granted to some privileged readers or to the public. In a public blockchain, called also "permissionless blockchain", both the write and read permissions are completely unrestricted. It could be readable and potentially writable by everyone. In this model the most common processes used for adding new blocks are the Proof-of-Work or the Proof-of-Stake. The two types of blockchain diverge in 5 key areas: consensus, performance, permissions, security and scalability.

Concerning the permission, in a public blockchain everyone can participate to the network without the need to meet predetermined criteria, without revealing their identity and using also pseudonym. In this blockchain's architecture all the transactions are public and every participants could have the privilege of writing. These features make this technology not particularly suitable for private companies that need to guarantee privacy over user's data and need to transact with known parties; this technology also limits the level of throughput. So companies are investigating how private blockchain could bring efficiency, trust and transparency in their organizations. Private blockchain networks, as Ibm blockchain, have been created in which private channel could be established between parties in order to not reveal sensible data to competitors.

Concerning the consensus, in both blockchains the transactions are validated and verified following an algorithm called consensus model. Differently form private blockchain, the mostly used by the public networks are time-consuming and computationally intensive. The most famous consensus model used by public blockchain is the Proof-of-Work. This way of adding blocks to the network is the most time-cost intensive but also is the one that should ensure the higher decentralized decision-making.[1] Due to its costly[2] and slow transaction speed , this consensus mechanism

[1] Nouriel Roubini(2018) thinks that “the massive centralisation of power among cryptocurrency miners, exchanges, developers and wealth holders [in the public blockchain] is not about decentralisation and democracy; it is about greed." He has computed that the Gini coefficient of Bitcoin, 0.88, is higher that the one of North Korea, 0.86.“ Where a Gini coefficient of 1.0 means that a single person controls 100% of a country's income/wealth"

[2] a OECD (2018) report states that in the “early March 2018, Bitcoin's estimated annual electricity consumption amounted to 58 Tetra Watthours (TWh) and growing rapidly. This is the

is not suitable for private companies that need high level of throughput and developers are looking for different consensus model. “In a private blockchain, like the IBM blockchain, consensus is usually achieved through a process called selective endorsement "(Laura Gargolinski 2018). In this consensus model the endorsement policy is set by operators and writers when the chaincode is instantiated. The advantages of this blockchain are greater transactions volume, faster speed and lower costs, but a some level of trust between members is necessary.

Concerning the security, in both types of blockchain, its chain-like structure and cryptography ensure immutability and tamper-evident features. A difference between the two is the degree of decentralisation. Higher level of centralization lead to higher risk to hacking and cyber attacks, so in private blockchain, where the level of decentralization is lower, trust is important among the members of the network.

Concerning performance and scalability, as mentioned above Public blockchain tends to have slower transactions speed and lower volumes than private blockchain. This is related to the consensus model applied and the number of users who join the network. The more transactions are requested, the longer it takes. According to blockgeeks, “paypal manages 193 transactions per second and visa manages 1667 transactions per second, Ethereum does only 20 transactions per second while Bitcoin manages a whopping 7 transactions per second". For the mass adoption of public blockchain, the improvement of performance and scalability of this technology is a crucial step.

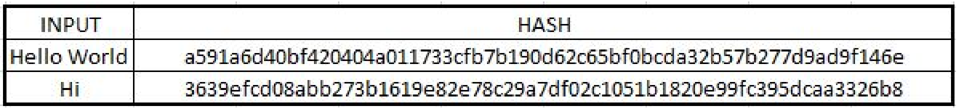
2.2 Cryptography

Cryptography is a technique for secure communication. It is essentially a process that converts a string of information into unintelligible text and vice-versa. It is also a process to store and transmit data where only the desired user can read and process it. In blockchain system it is used to preserve and enhance privacy and transparency in order to permit the exchange of data and ownership in a secure way. The cryptography techniques used by blockchain technology are: hash algorithms and Private/Public keys.

2.2.1 Hash algorithm

Hashing is a cryptographic function that taking an input string of any length, generates a unique fixed-length hash code.The same input will always produce the same

equivalent of over 5 million American homes, and roughly the same energy consumption as countries such as Kuwait. This represents 26% of the world’s annual consumption" hash code as output. Below there is an example of how hashing algorithm works, using SHA-256 technique as Bitcoin protocol.



INPUT	HASH
Hello World	a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e
Hi	3639efcd08abb273b1619e82e78c29a7df02c1051b1820e99fc395dcaa3326b8

Figure 2.1. Hash Function

Figure 2.1 shows how no matter the length of the input, the output is always a fix 256-bits length. This is so important when dealing with a huge amount of transactions. This powerful tool allows that with the output of the hash function it is unfeasible to determine the original input. The only way to obtain the original input from an hashing function's output is the brute force method.

In blockchain, the hash functions allow also to interconnect blocks together in a chain-like structure. Each block contains its own hashed data, called hash of the Merkle Root, and the hash pointer[3] of its previous block, hence creating the chain. Any attempt of altering the content of a block would leads to the change of the hash code generated, altering also all the following blocks, so it would be easily discovered.

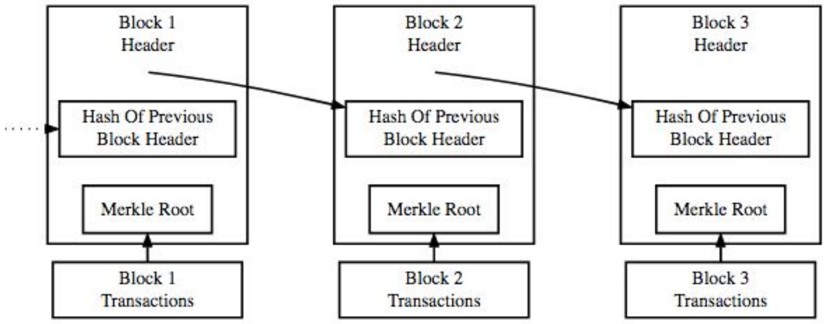


Figure 2.2. Hash Function In Blockchain [30]

Storing one transaction for a block would be time and cost inefficient, so Bitcoin protocol use the binary Merkle tree algorithm. In this way a huge amount of transactions are stored in a block. "Andreas M. Antonopoulos define it as a data structure used for efficiently summarizing and verifying the integrity of large sets of

[3] a pointer is a variable who stores the address of another variable, so a hash pointer store the address's hash function of another variable

data" (Medium). It is basically a tree where every leaf node is the hash of the data block and every non-leaf node is the hash of the concatenation of its two child nodes

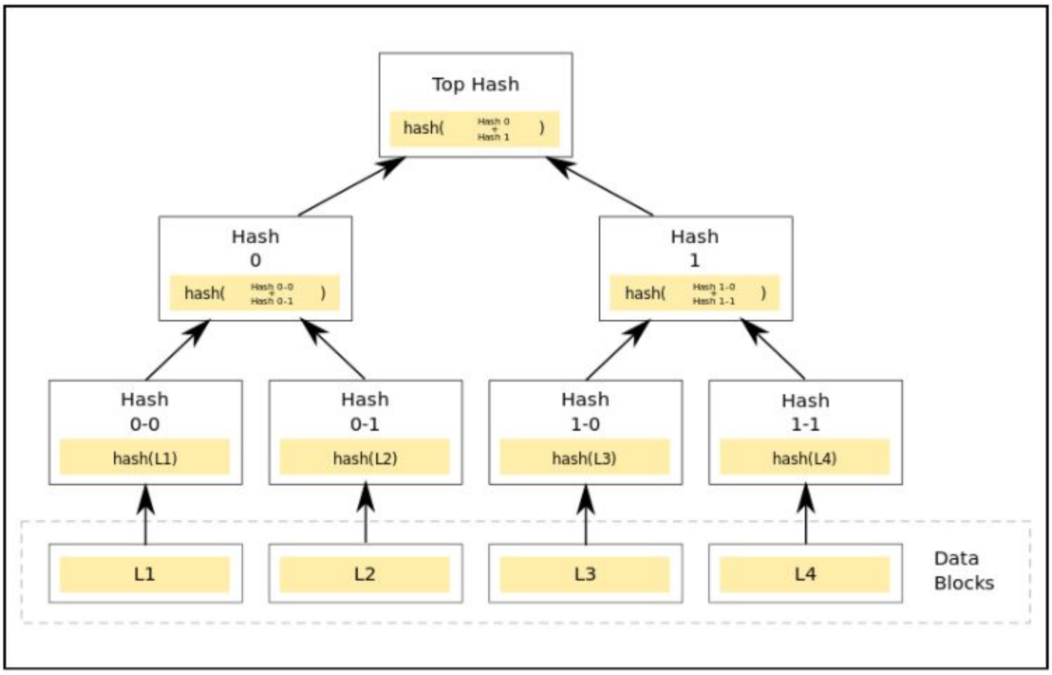


Figure 2.3. Hash Function And Merkle Tree [30]

When N data are stored and hashed in a merkle tree, to prove that a specific transaction is present in a block is very efficient. A node needs only (2*log 2 (N)) calculations for constituting an authentication path (Check the info and put the reference). This feature is very important as the number of transaction increases, because the base-2 logarithm of (N) is a function that increases much slower than N.

In the blockchain network, the application of the Merkle tree provides: high performance and scalability, efficient way to verify whether a transaction is included in a block, lightweight clients and Simplified Payment Verification (SPV). SPV and lightweight clients mean that to verify the presence of a transaction in a block is not needed to download the entire block.

2.2.2 Public/Private key

Public/Private keys is a powerful encryption tool in order to verify and authenticate the transfer of ownerships or data and to sign agreements. In many countries the digital signature already has legal evidence. The public key is a public address useful to interact with other people on the network and it is generated from the private key. The private key is used to confirm that a particular instruction comes from the sender and to read a transaction received by the correspondent public address. It is easy to generate the public key from the private one, but it is extremely difficult to calculate the private key knowing the public one.

In the Bitcoin network, the sender generates a signature that is composed by its private key and the message. This cryptographic tool permits to verify that the signature has been created by the private key associated with the sender address without knowing the private key. Since the signature is generated from the private key and the message, no transaction could re-uses the past signature. In a Bitcoin transaction, the sender uses its signature and the recipient's public key. The recipient instead utilises its own private key to read it.

This powerful tool guarantees a secure and private way for transact ownership and data. One weakness of this system is the way of storing the private keys. Nowadays a lot of private keys are stored in centralized exchanges that are vulnerable to hacking attacks. Although the blockchain is a very secure network, the vulnerability of this centralized exchanges and so of the stored private keys led to theft of many private keys. Losing a private key means the losing of data or asset like cryptocurrencies.

2.3 Consensus models

The consensus model is the process who is responsible of adding new blocks. It is basically an algorithm that is in charge of validating and authenticating the transactions and broadcasting them between nodes. This method enables the establishment of secure and transparent networks without a central trusted intermediary.

The first consensus model was the Proof-of-Work (PoW). This model was implemented for the first time in the Bitcoin network. This is a power-intensive process where nodes, called miners, compete in order to solve a "mathematical puzzle" to earn the right of adding a new block to the network. This expensive calculation effort ensures good behaviour by all nodes, making hacking economically non-viable. This consensus model should lead to a high decentralization environment but it has many drawbacks as: scalability, latency, transaction throughput and high costs.

In order to solve these downsides, different types of consensus models have been developed as: Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), Proof-of-Authority (PoA)etc. In the PoS protocol, the node who has the right of adding a new block is chosen in a semi-deterministic way according mainly to the stakes and other random variables. In the PoA model instead, the process is not competitive. Authorized validator are in charge of adding new blocks. Essentially its consensus model is not so different from traditional databases.

In private blockchain where the transaction throughput and knowing the nodes are fundamental, the consensus policy is set by operations that configure the blockchain in such a way as to match the needs of the company.

2.3.1 Proof-of-Work

Proof-of-Work (PoW) is the consensus model of the Bitcoin's and Ethereum's protocol. PoW is an expensive competitive process where nodes, called miners, try to solve a "mathematical puzzle" in order to gain the privilege of adding a block to the network and earn the reward. In Bitcoin network, the validator's reward is composed by transaction fees and new Bitcoins. The probability of winning the right of adding the block is proportionate to the validator's computational efforts. In the Bitcoin network, it takes an average of ten minutes to find the solution of the "puzzle"[7]. After it has been found, it is broadcasted in the blockchain waiting for confirmation from other nodes. The operation is considered approved after six confirmations[3], because different solutions for the same block can be found and different branch of the blockchain could be formed. This process is applied in order to avoid the double-spending risk.

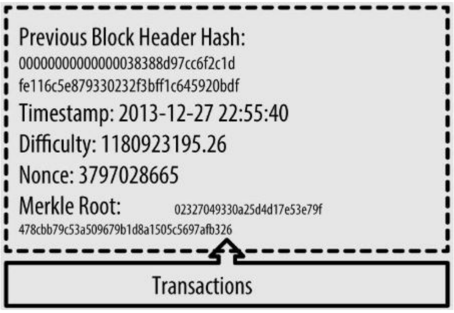
Bitcoin's safety mechanism has two interesting features. First, in the Bitcoin protocol only one miner get the reward, so there is only one "winner". The other validators basically had only wasted computational power. This wasted power is a crucial element. The more computational power is deployed in the network, the more difficult the puzzle becomes. Increasing the difficulty of solving the puzzle leads to an increment of the security.

Second, when the price of Bitcoin increases means a more valuable mining reward, thus miners are willing to invest in more computational power. These features of the Bitcoin's blockchain lead to increase security by discouraging misconduct by hackers. The greater the computational power involved, the smaller the proportion of the attacker which decreases the chances of attackers success.

Another Bitcoin's feature that increase the network security is how the block are composed. A Block is composed by:

- The previous block header hash: it is the hash pointer of its previous block header hash.
- The timestamp: it is basically the time when the block is created.
- The difficulty target: it sets the computational difficulty of the "cryptographic puzzle".
- The nonce: it is an arbitrary number used to vary the input of the hash function. It represents the solution of the "puzzle".

- The merkle root: it is the hashed data contained in the block.



Previous Block Header Hash:
000000000000000038388d97cc6f2c1d
fe116c5e879330232f3bff1c645920bdf
Timestamp: 2013-12-27 22:55:40
Difficulty: 1180923195.26
Nonce: 3797028665
Merkle Root: 02327049330a25d4d17e53e79f
478cbb79c53a509679b1d8a1505c5697afb326
Transactions

Figure 2.4. Bitcoin's Block

The mathematical puzzle that miners actually solve is to find the hashed function of the concatenation of the previous block header hash with the timestamp, the nonce and the merkle root that satisfies the difficulty condition. This solution is found in a brute-force way and by varying the nonce.

During the formation of the chain, it can happens that there are two or more different branches of the blockchain. This is an inevitable phenomena, called accidental fork, which is due to the latency on the internet. Some miners can receive a block before an another and vice versa. In this case, the consensus protocol establishes that the miners have to focus over the longest chain. It is considered the "honest" one because it has the greatest computational effort invested in it. Modifying a past block means to spend computational power for that block and all the block after. Dishonest chains will grow slower than the honest one, if the majority of the nodes work honestly.

The "loser" chains will became orphaned. Transactions that appear in the orphaned chain are not lost. They are still in the pool of transactions that have to be processed.

Due to the exponential increase of the hash rate in the last years, solving a block is very expensive for a single person, so mining pool companies have been founded. A mining pool is a group of entities that put together their hash rates to increase the chances of finding the solution of a block and then to split the reward proportionate to the amount of computational effort shared with the mining pool. This way of mining has compromised the desired decentralization that was the basis of the Bitcoin philosophy.

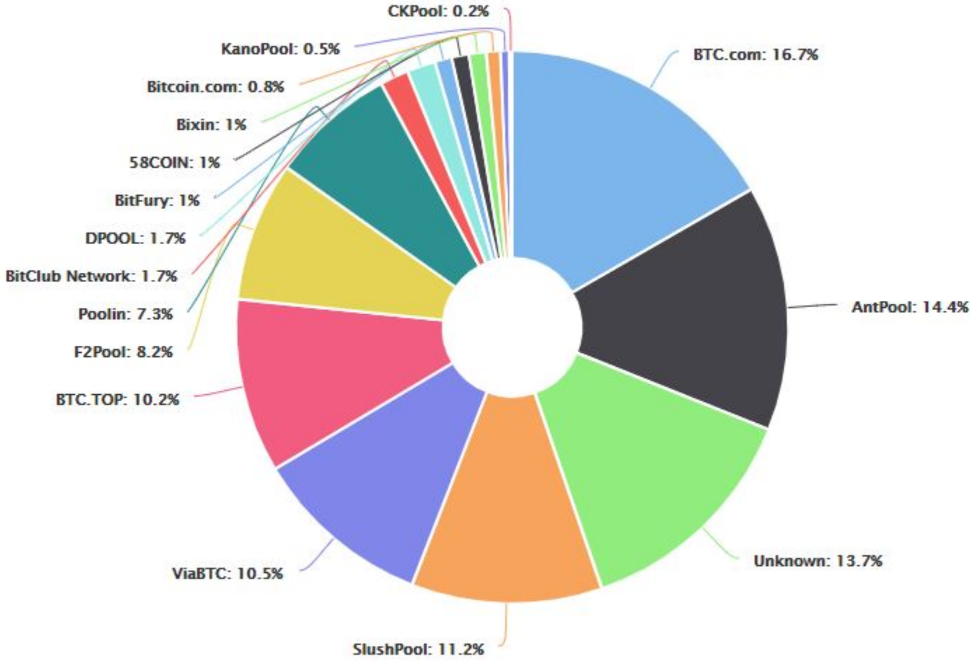


Figure 2.5. Bitcoin's Mining Pools [34]

The graph data (at 23/10/2018) above shows how the major four Bitcoin's mining pools have more than 51% of the total hash rates[33] and they are located in China. Decentralization is compromised by the Chinese mining "monopoly". The centralization of the hashrate in the Ethereum blockchain is even more evident as shown in the graph below.

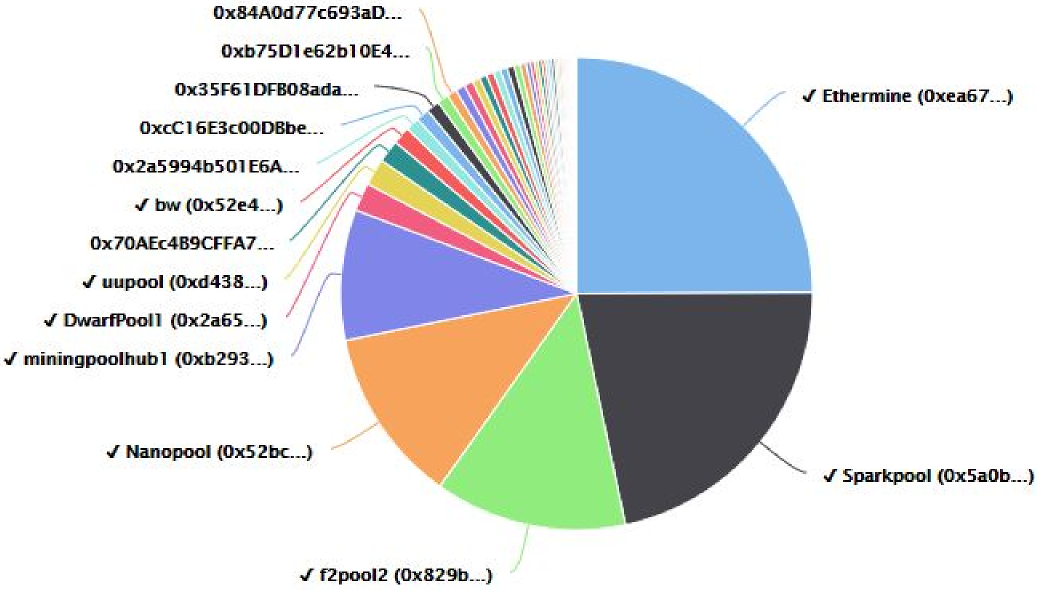


Figure 2.6. Ethereum's Mining Pools [35]

PoW's protocol is facing many issues, but there are several blockchain projects that are attempting to overcome the weaknesses of this consensus model even sacrificing decentralization.

2.3.2 Proof-of-Stake

Proof-of-Stake (PoS) is a consensus model used by several cryptocurrencies. This model has been developed to overcome the main problem of the PoW: low transaction throughput, huge amount of computational power consumed and the consequent birth of mining pools that threaten decentralization. Differently from PoW where the validator is the one who wins the competition against the others miners, wasting computational power. In PoS algorithms, a validator, called forger is chosen in a semi-random two-step process.

In the first step, it is considered the user's stake. The user is required to lock an amount of its stakes, as tokens, to ensure that it does not act maliciously; the stakes are deposited in the "network". The assumption is that users with a high stake in the network are more inclined to act with good behavior for the success of the platform.

The second step includes a degree of randomness in the selection of the validators. The most widely used approaches are random block selection and age selection of coins. These methods are used to avoid the scenario in which the rich get richer.

Random block selection chooses users based on a combination of the lowest hash value and the highest stakes. In the coin age selection users are selected by looking for the older tokens that have been staked. The age of a token is reset to "0", once a creation of a block. This are not the only two methods implemented in PoS. Some algorithms use the combination of the aforementioned methods.

Validators reward is composed by: transaction fee and a pay-out proportionate to their deposited stake [4](usually from 1% to 10%)[53].

In the absence of mining process no new cryptocurrencies are created. In this networks typically there are a fixed supply of pre-mined tokens.

The main problem that this consensus model faces is the Nothing-at-Stake problem.

> “In the event of a fork, whether the fork is accidental or a malicious attempt to rewrite history and reverse a transaction, the optimal strategy for any miner is to mine on every chain, so that the miner gets their reward no matter which fork wins" (James Ray).

For a validator is not expensive, differently from PoW, support different extending branches of the chain. Conversely in the PoW mining in different chain branches is extremely expensive. The protocol developed by Ethereum, called casper, is developed to overcome this problem. If a validator behaves maliciously trying to do a "nothing at stake", all their stakes will be slashed.

2.3.3 Centralization in PoW and PoS

PoS is a consensus model created to address the main problems of PoW algorithm: exorbitant energy inefficiencies and centralization tendencies. Surely PoS solves the energy inefficiency problem that affects PoW, but does it solves the centralization tendencies?

In PoW consensus model, called mining, the probability of solving a "cryptographic puzzle" is proportionate to the percentage of hashing power owned. Higher is the investment in the "hardware", higher is the probability of winning the competition among the miners and get the reward. Contrary in PoS consensus model, called forging, the probability of gaining the right of appending a new block to the blockchain is proportioned to the amount of stake owned. In this model the stake, i.e. the cryptocurrency, have to be locked in an online wallet. The cost of an online wallet is constant and it does not depend with the amount of stake hold.

[4] In some cryprocurrency to have a staking reward you must have a minimum amount of stake[53]

In both protocols, economy of scale occurs, so "Join forces" as participating in a mining pool or joining a single online wallet lead to lower average cost. In both network, economy of scale fosters centralization .

In PoW, fixed cost increase with the hash rate [5]. By putting more computational power in the network leads to increase the difficulty of the "mathematical puzzle". Joining a mining pool does not increase your reward, but allow to distribute your reward during the time. Due to the difficulty of solving a "mathematical puzzle", a miner who holds a little percentage of hash power will probably gain the privilege of adding a block once in a year, but by joining a mining pool he can gain the reward many times in a year but by distributing it. The benefit due to join a mining pool is lowering cost structure.

Conversely, in PoS, fixed cost[6] for maintaining an online wallet does not grow in relation with the stakes hold.

PoW and PoS present economies of scale, so for both protocols there is a tendency toward centralization.

Focusing over the Geographical location of nodes, it will be analyzed PoW in cryptocurrency as Bitcoin and Ethereum and PoS in cryptocurrency as Stratis(https://stratisplatform.com/) and PIVX(https://pivx.org/).

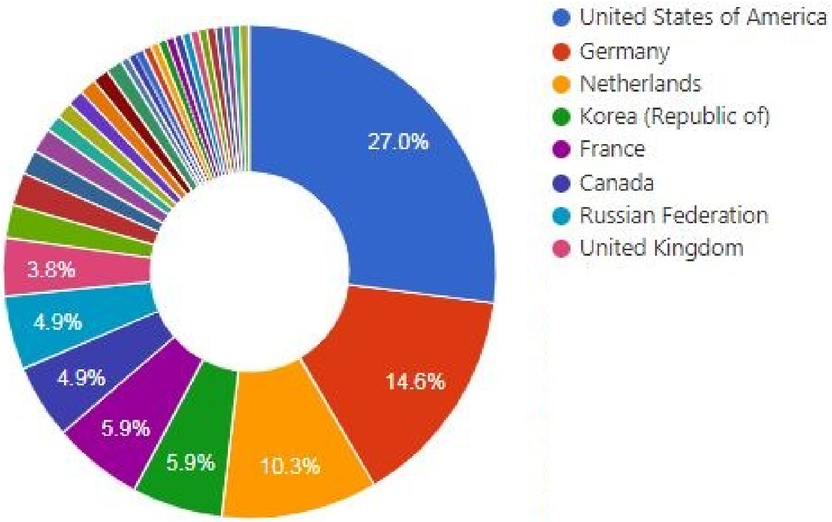


Figure 2.7. Stratis Mining Pools (data refers at 19/12/2018) [79]

[5] without taking into account cost structure, fixed cost refers to the investment done in order to increase computational power

[6] Fixed cost in PoS refers to the cost of locked stakes in an online wallet and the investment to increase the stakes in a blockchain network

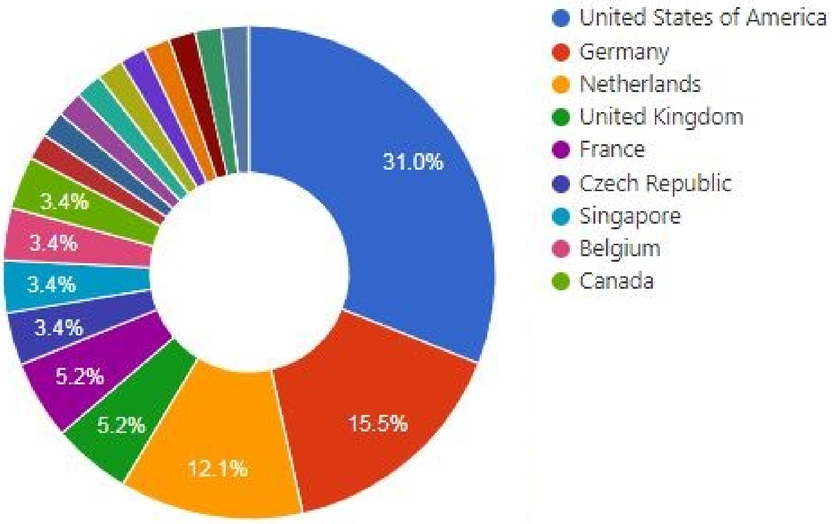


Figure 2.8. PIVX Mining Pools (data refers at 19/12/2018) [80]

The first thing that can be pointed out is that in PoS, forgers are distributed across more countries than PoW. Both PIVX and Stratis are more concentrated in the US, where around a quarter of all the wallets is holds. However other countries as Germany, Lithuania, Canada and others are involved in the validation processes. On the other hand, PoW mining process is concentrated in China where electricity is cheaper. So in a geographical point of view, the research points out that PoW is more centralized than PoS.

Concerning security and vulnerability of a consensus algorithm, according to Robert Greenfield IV (2017) must be analyzed how:

- a user who discovered a block should be encouraged to broadcast it
- a user should be discouraged from discovering blocks on top of intermediate chains
- consensus rules should be constructed in a way that results in resolving blockchain forks

This section will be focused over the possible attacks that can occur in a PoS-based consensus model. The majority of vulnerabilities arise from the fact that in PoS there is no computational power involved in the validation process. it will be discussed the main problems that affect PoS:

First, nothing at stake problem occurs in the case of a fork, accidental or deliberate. In this case the rational user is incentivized to validate blocks on both branches. In PoW, such behavior is irrational. A Miner who spits its computational resources in multiple branches, diminishes the probability of gaining the competition among the other users. The optimal strategy is always to mine on the longest branch. Conversely in PoS, the attempt of validating on multiple blockchain forks does not decrease the likelihood of adding a block. So it is easy to perform double-spending, called also bribe attack. In PoW algorithm, a similar attack would require a prohibitively high computational power.

Another problem that could affect the PoS network is called initial distribution problem. The consensus model does not incentivise the initial holders of coins to release them to third parties. This occurs because more are the stake locked in the network, more are the probability of validating a block. So purchasing when the system was just launched gives an advantage. On the other hand, in PoW the initial coin holders have not an advantage over the new users. In order to validate blocks, they need to invest in order to improve their hardware performance.

For addressing both issues, several improvement of PoS consensus have been realized.

To sum up, it can be stated that both blockchain systems suffer almost of the same problems, but in the PoW the huge amount of computational power required to attack the system, makes it in fact unfeasible. The optimal strategy for a rational miner is not to cheat.

The last consideration that can be made is about what happens when a validator tries to cheat. In PoS validators lock their stake in an online wallet, so in case of misconduct the user loses all his cryptocurrency. On the other hand, if this happen in a PoW network, the cheaters can still sell their hardware to another person. They may also migrate in another networks and reuse the same hardware.

It should be pointed out that comparisons between PoW and PoS tend to be difficult to make. Both consensus model have downsides. There are many debates among experts to attribute which technology is more decentralized, but surely a dominant design have still to be implemented. In this paper, PoW will be considered the more decentralized. This decision has been taken to highlight the importance of the computation efforts done by miners in order to enhance the security of the system and to orient miners good behavior.

2.3.4 Delegated Proof-of-Stake

The delegated proof-of-stake(DPoS) is a variant of the PoS. It provides a high level of scalability sacrificing the degree of decentralization by limiting the number of block producers. One of the main DPoS network is EOS network(https://eos.io/), it is a free to use platform. It is basically an online, representative democracy. This algorithm present two different figures: the block validators and the block producers. The block producers are voted by the users of the network. The weight of the vote of each user is proportional to the stake owned in the blockchain. User can also delegate their stake to another user, who will vote in their behalf.

A block producer is responsible for creating blocks and broadcasting into the network. They are a limited number[7]. In EOS network producer's reward consists on new tokens every time a block is produced. On the other hand, block validators are unlimited and are responsible for checking and verifying that block producers follow the rules agreed with the network community. Any users can be a block validator.

A block is considered valid if the validators verify that the block follows the consensus rules. Block producers take turns in the production of a block. In the EOS software a block is produced every 0.5 seconds.[41] A block is confirmed when it is voted by (2/3)+1 of block producers. In the case of fork, the "honest" chain will be always the longest. "Furthermore, no block producer should be producing blocks on two forks at the same time. A block producer caught doing this will likely be voted out. Cryptographic evidence of such double-production may also be used to automatically remove abusers"(Github)

This consensus model is attempting to create centralization in a decentralized environment in order to increase transaction throughput. The consensus methodology is a democracy with token holder suffrage. Powerful users, who has more stakes in the network, have an indirect role in the production of the block, because they only have influence in elections.

Some experts believe that this attempt of centralization is not totally secure and suitable for a network that transfer financial values. It can be suitable for platforms that require high throughput and does not need a full decentralized network as social network or gaming platform.

2.4 Smart contract

Smart contracts are auto enforceable computer programs that are stored on a blockchain. They are self-executing contracts that are performed when predetermined conditions are met and verified. Like other blockchain transactions, once verified, they are broadcast across all nodes in the network. The main benefits of smart contracts are:

- Automatic, reliable and impartial execution of contracts.
- Taking out the intermediaries for the construction, execution and enforcement of contracts.

[7] EOS:21,BitShares: 101,Steemit: 21

This trustless execution leads to different drawbacks. Stipulating a complex contract without a middle man is very difficult to secure. “With smart contracts, security means handling every possible way in which a contract could get executed and making sure that the contract does what the authors intend"[42]. Furthermore in a smart contract, as in all computer program, “testing [with manual verification and the classic testing-based approach] can only identify when bugs are present, and never certify their absence"[43]. A smart contract bug happened in 2016 in the Ethereum blockchain saw 3.6 million ether stolen (15% of all ether in circulation)[43]. The only possibility to save the lost funds was a hard fork solution.

To deal with the smart contract bug, several companies have been founded. There are two different approaches to face this problem:

- a labor-intensive approach where specifications are verified with off-chain computation written manually by human experts as Quantstamp platform (https://quantstamp.com/).
- an engineering approach that mathematically proves that any codes are bugs-free and hacker-resistant as CertiK’s platform (https://certik.org/).

Another problem to deal with is the link between the tokenized world, or digital world, and the "real" world. How can smart contracts ensure that the ownership of an asset corresponds to its possession?. This problem is called "Oracle problem". There could be different ways to face this issue but all will have the same problem, the involvement of a third party who verifies the events in the "real" world.

Smart contracts are certainly a very powerful tools but to be mass adopted they needs to be improved both in terms of technology and bureaucracy.

Chapter 3

Blockchain trilemma

Traditionally, data and transactions were stored in centralized ledgers that were managed by trusted entities. The technology had allowed the achievement of cost efficiency and data accuracy. However data centralization have lead to expose traditional ledger as a single point of failure, lowering records security, and to the monopolization of user's data.

Blockchain technology has provided an alternative way of record-keeping, thanks to its decentralized methods of storing and maintaining information.

> "Ideally, a ledger should record all information correctly and do so in a cost efficient and fully decentralized manner to avoid any concentration of power"(Abadi and Brunnermeier 2018).

In traditional ledgers, a single trusted and centralized entity is in charge of ensuring the correctness of data. The only incentive for writers to report honestly is related to their own profit, maintaining customer loyalty and exploiting their data. High stake in a traditional database lead to increase the inertia of an user to switch to a competitor. Network externality amplifies the anchorage of the users towards incumbent ledger, leading even those with low stakes unwilling to switch. Traditional ledger achieves cost efficiency guaranteeing high level of throughput and scalability.

In contrast, a decentralized environment enhances record security and privacy but leads to inefficiencies. Decentralization and the inefficiencies of a blockchain are related mainly to its consensus model and write permission.

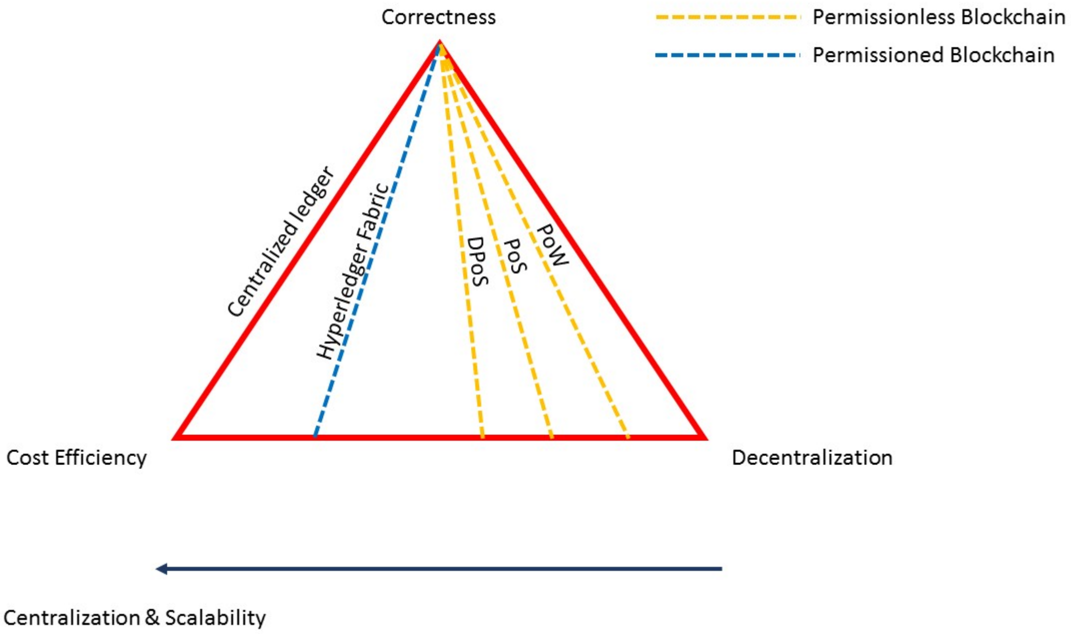


Figure 3.1. Qualitative Blockchain Trilemma

The graph above shows a blockchain trilemma. A ledger cannot ensure simultaneously the correctly record of all information in a cost efficient way and in a fully decentralized environment; Decentralization has a cost. Figure 3.1 shows in a qualitative way how the different consensus models reach a different degree of decentralization and so cost efficiency.

Differently from the previous interpretation of Abadi and Brunnermeier (2018), that has analyzed only the difference between a traditional ledger and a Proof-of-Work (PoW) blockchain, I have analyzed the differences between permissioned and permissionless blockchain and also the differences between PoW, Proof-of-stake (PoS) and Delegated Proof-of Stake (DPoS).

PoW, theoretically, can be considered the consensus model most decentralized. In this protocol there are two forms of competition that result in distinct inefficiencies. First, the write permission is unrestricted. Anybody could join the network and gain the right of writing. To ensure that writers do not behave unfairly and subvert the democratic nature of the network, they have to perform expensive computational tasks. This competitive and expensive mining procedures enhance the security between untrusted parties. Second, The fork competition, in case of hard fork, allows the portability of information in a competing branch of the chain.

Portability of information means no having higher stake in a particular ledger. This feature leads readers to not be anchored with the incumbent branch, eroding the rents of a monopolist ledger. Many competing blockchains can coexist. The splitting of the community into several competing ledgers leads to failure in the exploitation of the positive network externalities, considered a true efficiency loss.

PoS, differently from PoW, limits the waste of computational power by the writers. The probability of having the write privilege is proportionate to the stake owned in network and other random variables. The lack of competition between the writers lead to enhance cost efficiency but at cost of decreasing the degree of decentralization.

DPoS is considered the most centralized of the three public blockchain. In this consensus model the write permission is elected by the user and the number of block producers is limited. Then writers take turns in the block production. The weight of the vote of each user is proportional to the stake owned in the network. This attempt to create centralised democratic representative in a decentralised environment leads to a sharp increase in the volume and speed of transactions.

In addition to the case of permissionless blockchain, the permissioned one shows promises in many applications. It enables fork competition but lowering the wasted of computational power roughly as a any other distributed system [45]. Clearly the lack of free entry condition of writers weaken fork competition. Collusion between the nodes can prevent the survival of competing forks.

Another possible interpretation of a blockchain trilemma is the one thought by Vitalik Buterin. This trilemma is called scalability trilemma. In this interpretation, it takes into account three different features of a blockchain as scalability, security and decentralization. Differently from my interpretation, it separates the concept of security and decentralization. For example, in this trilemma PoW and PoS are considered equally decentralized, but PoW more secure instead PoS more scalable .

I have taken into account the trilemma developed by Abadi and Brunnermeier because it allows to better analyze quantitatively different consensus models, as PoW or PoS, instead the scalability trilemma is more suitable to analyze different protocols that also used the same consensus model, as Bitcoin PoW and Ethereum PoW.

3.1 Conclusions

To sum up, what most influence the decentralization of a network and consequently its cost efficiency are the write permission and the competition among the writers. Concerning the write permission, in a permissioned blockchain the number of the writers is restricted so for this reason it is considered a more centralized network with respect to a permissionless blockchain. Concerning the competition between the writers, only in the PoW blockchain it is present. Every writers spend computational power and compete in order to resolve a "mathematical puzzle", but only one gain the reward. In a PoW network the best strategy for a writer is not cheat; cheating is very expensive. For this reason PoW is considered the most decentralized consensus model. Instead in PoS the selection of the writer is a semi-random two step process. In these networks, cheating is not expensive as in a PoW blockchain, so for this reason is considered less decentralized than PoW.

The possibility of using different blockchain types in terms of degree of decentralization and cost efficiency allows this technology to be suitable in different contexts. Platform that enables exchange of ownership should require an high level of decentralization also by sacrificing cost efficiency. Instead other kind of networks that need high level of transaction throughput should increase the level of centralization.

However the creation of interchain blockchains, as Cosmos (https://cosmos.network/), allow to different blockchain to communicate each other and trade different asset.

Implementing interchain blockchains, applications can take advantage of both consensus model, PoW where security and decentralization is needed and PoS where an higher efficiency is a crucial factor.

Chapter 4

Model

This model was inspired by a work done by Abadi and Brunnermeier (2018). This paper analyzes how rational users choose between two different branch of the same blockchain in case of hard fork. An hard fork happens when the rules of a blockchain change, as writer reward or consensus model, and the community of a blockchain is split.

My interpretation instead analyzes how rational users choose between a Proof-of-Work (PoW) and a Proof-of-Stake (PoS) blockchain implementation depending on its use-case. The purpose of this model is to investigate the different behaviours of rational users choosing between two different blockchain, highlighting the decentralization-cost efficiency tradeoff postulated in the trilemma.

The set of agents is given by $I = [0{,}1]$. There are two options A or B, and τ is a common value affecting preferences for A. The proportion of agent who chooses A is ϕ.

Let us characterize an agent $i \in I$

1. $x_i \in \{A, B\}$ option taken by agent i, where x_i^* denotes an optimal choice
2. $\theta_i \in \mathbb{R}$ heteregeneous private value for $x_i = A$, denote $\theta_{-i} = (\theta_\iota)_{\iota \neq i}$
   - $F : \mathbb{R} \to [0{,}1]$ distribution function of θ iid
3. $v(\theta_i, \tau, \phi)$ preferences of i
   - $v(\theta_i, \tau, \phi) > 0$ (resp. < 0) implies $x_i^*(\theta_i, \tau, \phi) = A$ (resp. $= B$)
4. s_i is the personalized signal of i
   - Given $\sigma > 0$ and noise η_i iid with distribution $H : [-0.5{,}0.5] \to [0{,}1]$, we define
     $$s_i = \tau + \sigma\eta_i$$
   - Denote the signal profile by $s = (s_i)_{i \in I}$

4.1 Assumptions

(B.1)

1. $v(\theta_i, t, \phi)$ is increasing in θ_i
2. $v(\theta_i, \tau, \phi)$ is increasing in τ
3. $v(0{,}0, \phi) = -v(0{,}0{,}1 - \phi)$

Let us fix the ideas with the following example.

Example 1 *Consider $v(\theta, s, \phi) = \theta + s + k\phi$, recall that if $v(\theta_i, s, \phi) > 0$, then type θ_i plays optimally the option A. This implies the following:*

$$\theta_i + s_i + k\phi > 0 \Rightarrow s_i > -(\theta_i + k\phi)$$

Define $\lambda(\theta_i) = -(\theta_i + k\phi)$. Thus, for each type θ, there is a signal $\lambda(\theta)$ such that θ plays A if $s_i > \lambda(\theta)$ and plays B if $s_i < \lambda(\theta)$

This game is supermodular (see Abadi et ali (2018) or Milgrom and Roberts (1990)). Thus, by applying Theorem 5 in Milgom and Roberts (1990) for a signal profile s, there are largest and smallest rationalizable strategy profiles $\overline{\lambda}(s)$ and $\underline{\lambda}(s)$ where $\underline{\lambda}(s) \leq \lambda(s) \leq \overline{\lambda}(s)$.

The purpose of this model is to evaluate how a rational user chooses between two different blockchain technology with different consensus model,PoW or PoS. As mentioned above the main difference between the two kind of consensus model are: PoW enhances decentralization by sacrificing cost and time efficiency in the transaction process instead PoS allows an higher level of throughput but by providing a more centralized environment.

In this model, the parameter x_i, that is the agent choice, will be A if the agent will choose a blockchain technology with a PoS consensus model, otherwise will be B, so choosing a network based on a PoW consensus model. The parameters that influence the agent choice are θ, s and k. θ will represent the personal benefit delivered to an agent due to the cost efficiency of the network for its use-case. θ means how much efficiency is important for the user in its application. s instead is a technical characteristic perceived by an agent, it represents the cost efficiency of the blockchain technology. s is composed by two parameter τ and η. τ is the parameter that effectively represents the technical characteristic of the blockchain, in terms of cost efficiency. η instead is the noise that determined how different agents perceived differently the same blockchain characteristic. Finally k is the parameter that evaluates the magnitud of the network externality.

In order to find the Nash equilibrium solutions, the model have to satisfy the following conditions:

$$\forall i, x_i : v_i(x_i^*, x_{-i}^*) \geq v_i(x_i, x_{-i}^*).$$

where $x_i^*(\theta_i, \tau, \phi)$ is optimal when :

- $v(\theta_i, \tau, \phi) > 0 \to x_i^*(\theta_i, \tau, \phi) = A$
- $v(\theta_i, \tau, \phi) < 0 \to x_i^*(\theta_i, \tau, \phi) = B$

To find the equilibrium, an algorithm has been developed in order to:

1. set up data
2. guess the initial $\tilde{\phi}$
3. compute the optimal $v^*(\theta_i, \tau, \phi)$
4. compute the optimal $x^*(\theta_i, \tau, \phi)$
5. compute the optimal ϕ^*
6. if $\tilde{\phi} = \phi^*$, the equilibrium has been founded. Otherwise go back to step 2 changing the $\tilde{\phi}$

Refer to Appendix A for the full algorithm.

4.2 Computations

For the computational part and to understand how the variables are interconnected, different values have been assigned:

- $\theta_i \in [-1,1]$ where:
  - $\theta_1 = -1$
  - $\theta_2 = -0.5$
  - $\theta_3 = +0.5$
  - $\theta_4 = +1$
- $F : \mathbb{R} \to [0,1]$ where:
  - $F_1 = 0.6$
  - $F_2 = 0.7$
  - $F_3 = 0.8$

  - $F_4 = 1$

- $\tau = 1$
- k=0.1
- $\eta \in [-0.5,0.5] \rightarrow \eta = -0.1$
- $\sigma > 0 \rightarrow \sigma = 1.5$
- $\phi \in [0,1] \rightarrow \phi = 0.4$

This iterative process was carried out to seek out the equilibrium points, varying first σ and successively k and τ. The results found have been plot, in order to understand how the variation of this variables affect the population of the PoS blockchain.

The graph below (Figure 4.1) shows the relation between the percentage of population that choose ledger A(PoS), ϕ , and the magnitud of the noise (σ). since the noise was set negative, the perception of the technology used by the ledger A is worse than the reality. So increasing σ lead to a decrease of ϕ.

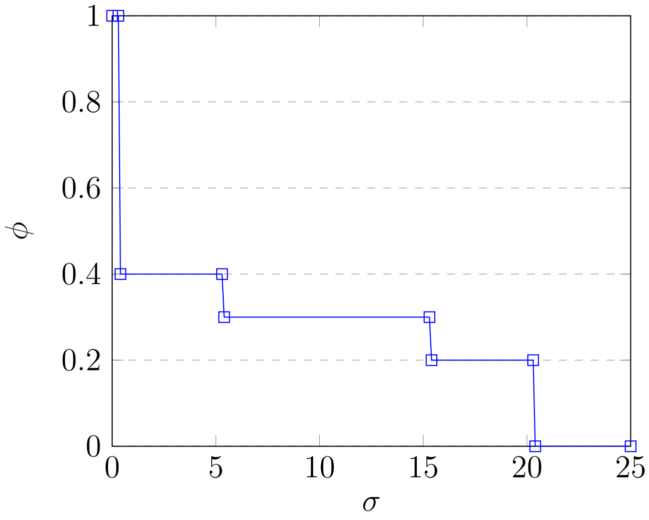


Figure 4.1. ϕ variation with respect of σ

Instead, the next graph (Figure 4.2) shows the variation of the percentage of population that choose ledger A(PoS),ϕ , with respect to the variation of the magnitud of the expected value of $\phi(k)$. By incresing k, as espected, also ϕ increases. The explaination of this phenomenon is that in a network, network externality greatly influences the choice of the users.

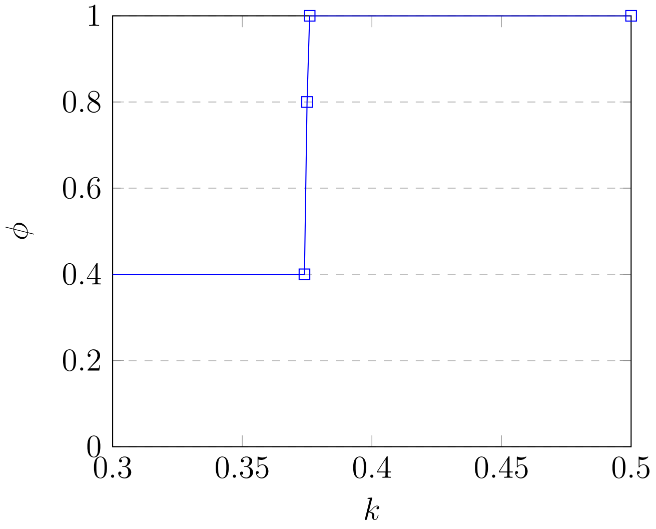


Figure 4.2. ϕ variation with respect of k

Finally, the graph below (Figure 4.3) shows how by improving the technical characteristic of the blockchain A in terms of efficiency (τ), the percentage of population that choose ledger A(PoS) will increase.

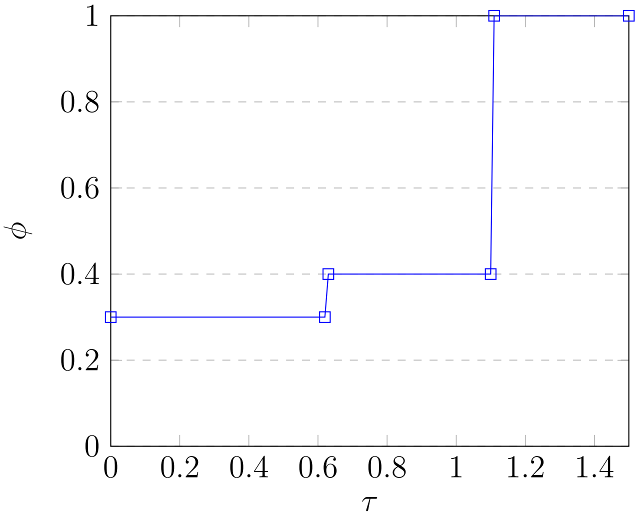


Figure 4.3. ϕ variation with respect of τ

The creation of this model was usefull to understand how different parameters, objective or subjective, influence the users choice. An other usefull result is that every different use-cases need different blockchain characteristics. There are use-cases where the time and cost efficiency of transaction is more important that a more decentralized environment. Instead there are other use-cases, as financial transactions, where decentralization and security is the most important feature.

This model points out the same results of the trilemma: each application needs different tradeoff between efficiency and decentralization. Use-cases, as the financial one, where security is a key factor, need an high degree of decentralization; high decentralization can only be reached by scarifying cost efficiency and vice versa. As mentioned in the previous chapter, the implementation of interchain blockchain can help to break the trilemma and take advantage of both blockchain characteristics in the same application.

Chapter 5

Blockchain use-cases for impact investment

The main blockchain characteristics enable to generate a measurable environmental and social impact alongside a financial return. The main benefit engendered by this technology is the establishment of a platform that enhances simultaneously transparency, privacy, trust and even efficiency. Different blockchain-based solution has been implemented in sectors such as energy, philanthropy, agriculture, finance, government and more. It can be said that blockchain could be a suitable solution as a business model if:

- Disintermediation is economically and technically feasible
- Multiple parties need to share and access the same data
- Business processes need trust and transparency, sharing and exchanging untampered data
- Data and transaction verification is required
- Certainty in the success of transactions is required

"Blockchain initiatives dedicated toward social impact are still in the early days, 34% were started in 2017 or later, and 74% are still in the pilot or idea stage. But, 55% of social-good blockchain initiatives are estimated to impact their beneficiaries by early 2019"(Galen and El-baz 2018). The main sectors that have attracted more initiatives for impact investment are health (25%), financial inclusion (13%), energy, climate and environment (12%) and philanthropy, aid, and donors (11%), (see figure 5.1)

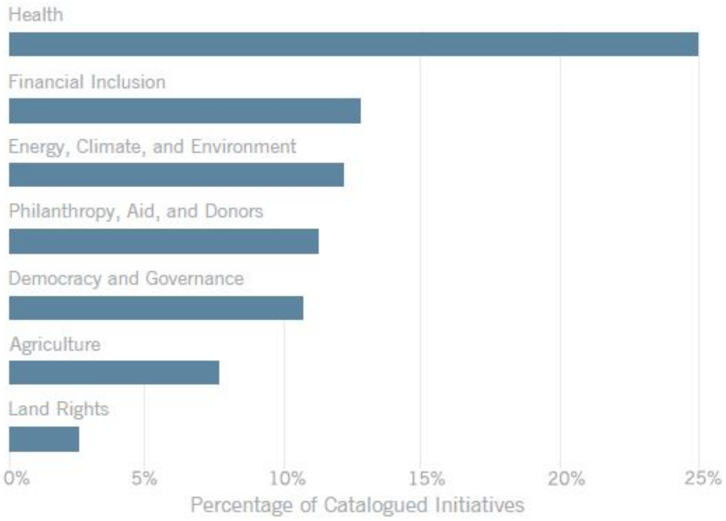


Figure 5.1. Blockchain Initiatives For Impact Investment [17]

Initiatives in the democracy and governance sector are the most developed, it is expected that 62% of them will have an impact in the next six months[17]. Furthermore, there are other sectors that still need more researches and testing and it is estimated that they will not have an impact within the next two years, as the 63% of energy initiatives[17].

The main use-cases for blockchain implementation are for facilitating records and verification (26%) and also payments and money transfers (25%). On the other hand initiatives toward the implementation for smart contracting are the less spread (1%). Other common use-cases initiatives are the establishment of platforms and marketplaces (19%), supply chain management (12%) and digital identity (8%)

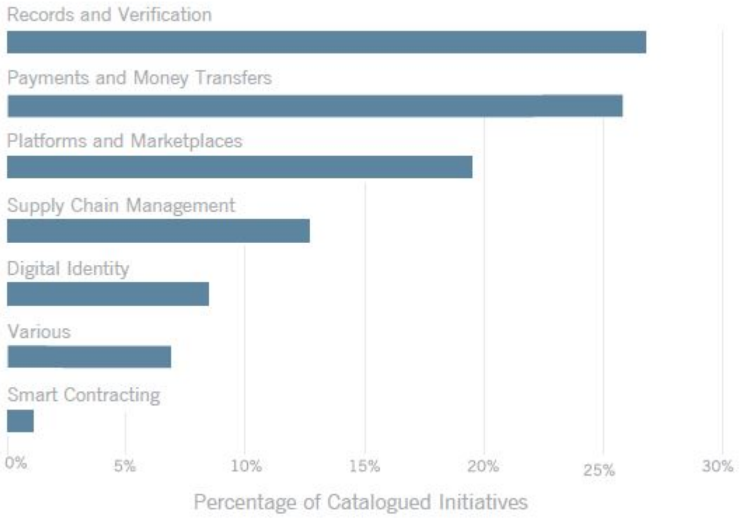


Figure 5.2. Blockchain Initiatives Use-Cases [17]

Concerning the main benefits observed due to blockchain implementation are : reduction of risk and fraud by increasing in integrity and transparency (38%) and increased efficiency (24%)

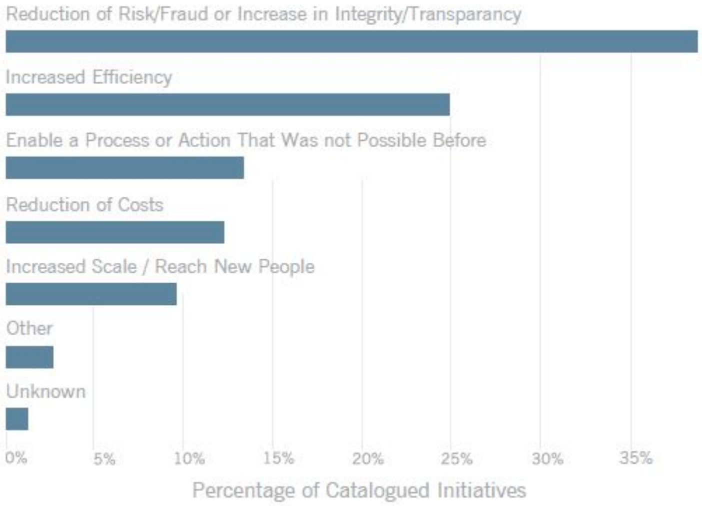


Figure 5.3. Blockchain Initiatives Benefits [17]

Overall, the majority of organizations that are developing a blockchain-base solutions are for-profit activity.

The research and investment in democracy and governance have figured out how this technology has a great potential for delivering benefits especially to public sector and citizens. Several government, as Estonia and Canada, are implementing several pilot projects that should already achieve impact in 2019. One of the biggest issue that government are facing is the establishment of a stable democracy. According to Freedom House, the 2017 has faced the most serious crisis in decades for democratic governance[59]. Blockchain-like network can address many security problem by enhancing transparency and privacy. This technology can prevent data tampering, ensuring immutability of data thanks to its chain-like structure. Data and information of citizens can be shared in a secure way among multiple agencies eliminating redundancy and paper-intensive processes. With the adoption of a distributed ledger technology, governments eliminate the single point of failure due to a centralized database. This way of storing and sharing information allow to enhance security and even lower maintenance and transaction costs. Sensitive data can be authenticated and verified without being transmitted and even seen by government employee. Blockchain technology, thanks to identity management functionalities, allows read-/write permissions only to specific entities. This functionality increase control and accountability in governmental processes. The main initiatives that are developing in this sector range from voting, digital identity, crowdfunding and citizen participation. The analysis of this projects shows that more than half of initiatives(53%) would be impossible without a decentralized and distributed ledger technology[17]. The most advanced blockchain initiative is E-Estonia(https://e-estonia.com/). It manages the 99% of country's governmental services[60]. Citizens can track and control government transactions that employ their personal information. Citizen information itself are stored off-chain but for every transaction, there is a proof registered on the blockchain. Estonia has a policy called "once only". It implies that once any government braches ask for a information, it will never be asked again. It is estimated that E-Estonia platform let the nation to save 820 working years and 2% of GDP[61].

Concerning identity issue, the world bank estimates that 1 billion people cannot prove their identity[62]; this problem affects mainly people come from underdeveloped country. Several organizations, as AID:tech (https://aid.technology/) and BanQu (https://banqu.co/), are attempting to provide digital identities and aid tracking to underserved regions thanks to a blockchain-based solution. People without a provable identity are not able to access to social benefits, as pensions,cash transfer, healthcare benefits, as vaccinations, insurance and maternal care, and political and legal rights, such as owning property, voting. Blockchain technology can deliver several solutions in order to provide a digital identity. It, with its chain-like structure, enhances immutability and transparency of data and contemporary includes reduction in cost and fraud. It enables people to use an user-centric ledger that allows users to have a complete control over their data, also by knowing who accesses and uses their data. Half of initiative in this sector would not be possible without the implementation of a distributed and decentralized ledger[17]. "Blockchain-based digital identity is a high-impact, global scale application. Half of projects documented are expected to impact over one million users"[17]. The main challenge that this sector have to face is how identity data deal with right-to-be-forgotten laws. Blockchain ensure the immutability of data, but what happens when people have the right to delete their information?.

Concerning financial inclusion, in the world there are more than 2 billion unbanked people[17]. According to World Bank , 18% of the unbanked people are unable of access to financial services because of their inability to proof their identity [63]. Blockchain solutions for financial inclusion can mainly benefit especially unbanked people and people come from underdeveloped countries. A distributed and decentralized ledger technology can lower transaction settlement costs and time, remove useless intermediaries and provide digital and economic identity. The major application of this technology is for cross-border payments. Without the implementation of a distributed ledger technology cross border payments include: involving many third-party intermediary and being exposed to the settlment and foreign exchange risks. All this processes and risks involved in a cross-border lead to high transaction fees. The main project developed in this sector are Mojaloop (`http://mojaloop.io/`) and WeTrust(`https://www.wetrust.io/`). Blockchain-based solutions for financial inclusion is a high-impact and global scale application. 68% of the initiative in this sector aim to reach more than a million people[17]. Despite its benefits, the usage of this technology is still not largely adopted. The delay in blockchain implementation is due to the presence of several obstacles as : the lack of a formal regulation framework, the complexity of the technology and the powerful presence of incumbents that take advantage of the current financial situation. Another factor that limits its adoption is that it is not mature enough; "While blockchain transaction speed is superior to available options in the developing world, its current speed is still limited compared to settlements in developed countries" [17].

Concerning healthcare, 25% of blockchain initiatives are focused to address issues in this sector[17]. The main problems that affect this industry include pharmaceutical supply chain management and digital health record exchange. With respect to health information exchange, there are already many but the main issue is the interoperability among them; each database has custom data standard, so it is not easy to exchange data among different database. To illustrate the challenge, the city of Boston there are more than 26 different medical record system[64]; so patients have records scattered across different databases. It is difficult for doctors access to the full medical history of a patient. With respect to pharmaceutical supply chain, the way medicines and vaccines are transported, from the manufacturer to the end user, is crucial to their correct working. There are parameters that should be respected like temperature, pressure and more. Hence, verifying and tracking the environmental condition of medicines along the supply chain allows to identify which one should be discarded. In the emerging countries another big problem exist: the presence of counterfeit drugs. According to WHO "About 100,000 deaths a year in Africa are linked to the counterfeit drug trade [and it is also estimated that] 700,000 deaths a year are caused by fake malaria and tuberculosis drugs" (Jocelyne Sambira). Distributed and decentralized ledger solutions in this sector can be useful to track and verify supply chain condition,as Modum (https://modum.io/), and to establish a unique set of data shared among different medical institute. Modum is a company founded in 2017 that offers digital supply chain monitoring solutions. It is composed by hardware sensors that share data with a blockchain system. Sensors collect data about temperature conditions during medicine shipment, instead blockchain stores sensors' data in order to ensure that they are not tampered. The majority of Blockchain initiative (80%) in this sector are for-profit company and are operating in Europe and U.S.[17]. This occurs because there are high healthcare expenditure in this countries. In the U.S., healthcare expenditure reach $3 trillion annually and around 20% of GDP [17].

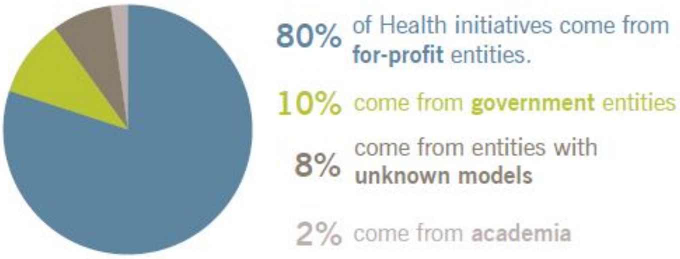


Figure 5.4. Types of Organizations Implementing Health Blockchain Initiatives [17]

Concerning philanthropy and aid, according to Sustainable Development Goals(SDGs) there are 836 million people who live in extreme poverty[66]. Furthermore United Nations conference on Trade and Development(UNCTAD) estimates that developing countries needs a range from $3.3 trillion to $4.5 trillion per year in order to achieve food security, basic infrastructure, health, education and climate change mitigation and adaption. nowadays there is a annual investment gap of $2.5 trillion[67].

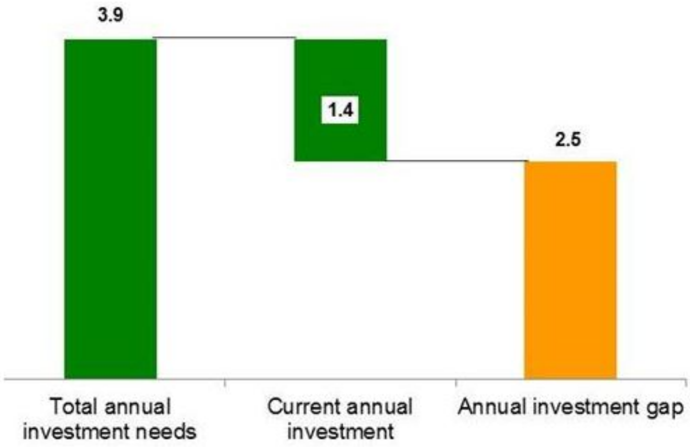


Figure 5.5. Estimated Annual Investment Needs in key SDG Sectors, 2015-2030 [67]

The main issues that impede the grow of investment in this sector are: the lack of transparency and the lack of trust that the funds donated will be used effectively. Currently, there are non-profit organizations that manage the funds donated. "Once the money leaves the account of the donor, there is limited tracking or transparency available to determine exactly how the funds were used and who ultimately benefited. Donors are also becoming more results - and impact - focused, and trust in the recipient organization is crucial to their giving decision-making"(Galen and El-Baz). According to Fidelity Charitable survey, 41% of donors believe that an increase in knowledge and transparency about non-profit effectiveness will produce a change in donors donations[68]. Intermediation in this sectors leads to inefficiency; approximately from 3% up to 10% of the donated funds are spent in transaction fees[17]. This phenomenon is critical especially for international aid organizations dealing with huge transfer of money in underdeveloped countries. Blockchain enables instant payments, lowers transaction fees and mitigates risk of fraud and loss thought funds tracking. Blockchain has the potential to disrupt the philanthropy sector by addressing the key issues: enhancing transparency, reducing transaction cost through disintermediation and enabling new system in order to monitor and track impact. Furthermore, smart contracts can enable that funds are disbursed when specific conditional milestones are met, so incentivizing organizations to run projects in a transparent way. This project management allows donors to track and verify the impact of their donations. A humanitarian organization that has implemented the blockchain for aid distribution is UN World Food Program (WFP) (http://www1.wfp.org/). It delivers food assistance in emergencies countries. Instead of receiving funds via intermediaries, such as bank, it has implemented a blockchain platform facilitating cash transfers for over 10,000 Syrian refugees[69]. In this pilot project, it was a able to save 98% of bank transaction fees. If blockchain solutions will be implemented in the entire organizations, that spends $66 billion annually, it will leads to save tens of millions that could be allocated to donations and aid[70]. Blockchain has also enabled a new sources of fundraising such as tokenized giving and crowdfunding. Donations through the use of cryptocurrencies are increasing. Fidelity Charitable, the largest donor-advised fund in the US, received nearly $70 million in 2017 in cryptocurrency donations, ten times what was raised in the previous year[71]. Decentralized and distributed ledger technology has the potential to disrupt the aid and philanthropy sector nonetheless has to face two issues that may prevent its application in the short term. First, nonprofits organizations and government are typically risk-averse so this attitude could slow down blockchain adoption; even if a successfully pilot project, the process of scaling the implementation of blockchain across the entire organization is often complex. Another important barrier to large-scale adoption is the presence of local political and economic forces that often impede the increase of transparency and effectiveness of philanthropy initiatives. Even if blockchain is facing barriers for a wide-scale adoption in the shot term, surely it has the potential to disrupt this sector in the long term. One of the main blockchain initiatives in this sector is ixo Foundation (https://ixo.foundation/). It is a Swiss-based nonprofit that has established an opensource blockchain system for the impact investment. “ixo solves the current issues in impact investing, results-based finance, and sustainable development by enabling projects to cost-effectively collect, verify and share their impact data"(Ixo Foundation). The first pilot project, Project Amply, has been funded by UNICEF and Innovation Edge and is being implemented with the collaboration of Western Cape Department of Social Development in South Africa. It enables to verify and record pre-school attendance of children using a mobile application. Based on children attendance, schools will receive government subsidies, bringing greater transparency and accountability. Amply has already digitized more than 55,000 children’s school attendance records[17]. ixo’s long-term vision is "enabling anyone to become the creators of their own impact projects and a stake-holder in the projects they believe in"(ixo Foundation). Its protocol will enable to self-certify the finance and social impact thanks to verified impact data that are universally accessible and untampered in the blockchain.

5.1 Blockchain design for impact investment

Blockchain technology surely have great potential to disrupt different industries but several consideration regarding its design must be taken into account. "What makes blockchain so relevant is also its greatest challenge: the interdependence of its attributes"(Lapointe and Fishbane 2018). Organizations cannot focus only over the desired features without taking into account the interaction of all its attributes. The design phase is about understand the correct trade-off that will be suitable according to the organizations' goals. Different design choices lead to different consequences in terms of social and ethical aims. Blockchain implementation can be an instrument to enhance democracy, nonetheless it can be a way to consolidate power over people and information. Its anonymity can be used for criminal activity and its records immutability can remove the right to be forgotten. There are many consequences to take into account in the evaluation of the right trade-off made during the blockchain design.

"One potential consequence for end users of blockchain technology is the codification and exacerbation of existing negative social dynamics"(Lapointe and Fishbane 2018). Blockchain can be used to establish secret agreement which circumvent regulations and laws or to strengthen control over people. It may increase the risk of creating a status quo or exacerbating inequalities or codifying community prejudices.

The immutability and transparency of personal data is another risk that may be faced. "Transparency of personally identifiable information could put someone at risk of exploitation, while transparency of ethnic or religious background, sexual orientation, or other identifiers could put a person at risk for persecution" (Lapointe and Fishbane 2018). Concerning the immutability, blockchain eliminates the ability to be forgotten. People who need to change their identity, as political refugee or people who are subject to a protection protocol, should be able to disassociate from their old digital identity. Hence is it essential to include every personal identifiable information?

Beyond personal identity, the immutability of blockchain address another issue called "zero state problem". It is about the veracity of records initially entered into the blockchain. What could be the consequence of entering an incorrect data into an immutable Ledger?. Falsification of data recorded could worsen the effects on disenfranchised owners.

In a blockchain, privacy and security are established thanks to cryptographic tools as public/private keys. These powerful instruments act respectively as email address and its password. The benefit of these tools is that users use them without knowing them. Often private keys are stored in centralized databases that are vulnerable to hack attack and there is no way to retrieve a lost private key. Considering a blockchain platform to record personal ownership, does losing a private key means the lose of real ownership?. For a mass adoption is important to establish a method to retrieve a lost private key.

Finally, another consequence to take into account is the environmental impact. In decentralized platform, the lack of a central trusted authority is compensated by a consensus model. Considering the Proof-of-Work (PoW), nowadays the most utilized protocol, it involves a significant waste of environmental energy. To address the environmental impact, alternative way to create consensus have been implemented but increasing the degree of centralization.

Blockchain technology has the potential to disrupt actual business model, but all the consequences related to its implementation should be considered, attempting to highlight the positive characteristics without forgetting the negative consequences that they can bring.

The right way to approach the design of blockchain in order to achieve social and environmental impact is to include these goals into the project requirements. The first step, even before deciding if this technology is suitable to the organization is to clearly identify the problems that want to be addressed.

> The overarching goals of the Framework are to give decision makers an outcome-focused and user-centric tool to assess the context-specific consequences and ethical implications of their blockchain design choices; and to enable them to use this understanding to make the appropriate values-based design choices to achieve better social outcomes. (Lapointe and Fishbane 2018)

The framework should be evaluate in a collaborative way involving different communities of expert from different sectors as government, private and non-profit organizations. The cooperation between different stakeholders allows to take into consideration different points of view and approach to the same problem and elaborate a framework suitable for the different use-case; for this reason different collaborative associations, as Hyperledger, have been established.

Once blockchain is considered the appropriate technology to achieve the goals predetermined, the main considerations that should be take into account are :

- governance
- identity
- verification and authentication
- access
- ownership of data
- security

Governance concerns the rules that govern the blockchain network. Since rules are a code, it is fundamental to evaluate that the governance does what the designers intended. "In the social sector, it is critical to ensure that a sound human governance structure is driving the technology" (Lapointe and Fishbane 2018).

Concerning identity, significant considerations should be done about how identity information is used, protected and accessed. The establishment of a digital identity linked permanently to a unique individual can allow people to use it in a different context and circumstances. Another challenge developers are facing is understanding what kind of information should be entered, taking into account the immutability of data once inserted into the blockchain.

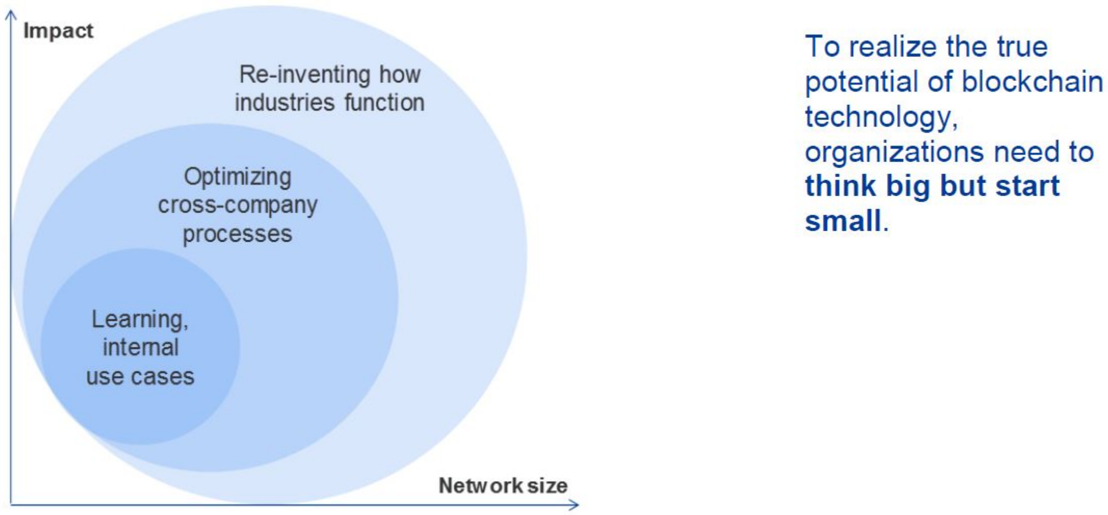
Verification and authentication of the information into a blockchain is critical in a decentralized and open platform. The verification process for digital assets is more simple and it refers to control if the user who request a transaction has control over that asset. However for nondigital assets, as ownership, this process is more complicated because it involves human interaction. The ownership of the tokenization of a real asset does not ensure its possession in the "real" world.

Defining who has the permission and the right to access to data is a crucial task in the blockchain system. "the scope of access to individuals' personal information on a blockchain may result in serious implications for those individuals if that information is exploited" (Lapointe and Fishbane 2018). Read/write permissions in a network must be evaluated carefully in order to take advantage of the full potential of this technology.

Concerning ownership of data is important to define who exercises control over the data and how they are stored. An appealing blockchain feature is its ability to shift the power from institution to customers.

Regarding security, the decentralized nature of blockchain permits to eliminate the single point of failure present in traditional ledgers. Furthermore cryptographic tools enhance the security of the network. The hash function allows to create a chain like a structure that is unfeasible to tamper. Additionally public/private keys allow a secure transfer of data and ownership.

Blockchain is considered a breakthrough technology that could have a huge social and environmental impact. It is receiving increasing attention by several companies in different industry. However a dominant design has not yet been established. Companies are trying to patent different blockchain design solutions by varying the interaction of all its attributes. In order to achieve the right design and to speed up the mass adoption, companies are establishing different consortium, as Hyperledger, involving many stakeholders of different industries in the decision making. The right way to approach the Blockchain design is to clearly understand the problems that want to be addressed. As a new technology, companies should begin to gain experience by applying it in small contexts.


Impact
Re-inventing how industries function
Optimizing cross-company processes
Learning, internal use cases
Network size

To realize the true potential of blockchain technology, organizations need to **think big but start small.**

Figure 5.6. How To Approach Blockchain Implementation [50]

Organizations "will need to think big but start small. Realizing the full potential of blockchain-based networks will take time - the winners will be those who start working with the technology today and, through first-hand experience, learn to make the most of blockchain-based networks" (Forrester 2018).

The design of blockchain in order to achieve social and environmental impact is a crucial phase. First of all, organizations should clearly identify the problems that want to be addressed and analyze all the possible consequences due to the blockchain design.

5.2 Conclusions

It cannot be predicted if blockchain solution for impact investment will disrupt the actual industries in the short term, but blockchain application are already emerging. The lack of a clear regulation, the complexity of the technology and the powerful presence of incumbents, that take advantage of the actual inefficient economy, are slowing down the wide-scale adoption. In order to have an effective implementation of blockchain technology for impact investment, organizations have to: clearly understand the problems that want address and how blockchain could fit it and become familiar with the technology by starting to build small applications.

Chapter 6

Blockchain implementation in SocialxChange

I have collaborate with a Chilean NGO, SocialxChange(SxC), that is focused in the impact investment sector where i was the blockchain expert. My tasks in the foundation were:

- Analyze the blockchain technology and the interdependence of its attributes
- Investigate the possible applications of the blockchain technology in the impact investment sector and its potential economic impact.
- Establish the design that best suit the use-case of the foundation and choose between the different blockchain available in the market.

As mentioned before, blockchain could be a suitable solution as a business model if:

- Disintermediation is economically and technically feasible
- Multiple parties need to share and access the same data
- Business processes need trust and transparency, sharing and exchanging untampered data
- Data and transaction verification is required
- Certainty in the success of transactions is required

The main sectors that have implemented a blockchain-based solutions for their initiatives are health, philanthropy, agriculture, financial inclusion, democracy and government. All this sectors have in common the need of enhancing simultaneously transparency, privacy, trust and even efficiency. The main use-cases implemented are for facilitating records, verification, payments and money transfers, establishing platform and marketplace, improving supply chain management and digital identity.

In order to estimate the potential economic impact of the technology, potential revenues, savings and costs have been taken into account.

Concerning the potential revenues, blockchain enables to charge fees, as onboarding, annual and transaction fee, to the member who uses your blockchain platform. For big companies that interact with a high amount of clients and suppliers, charging fees for its blockchain users could lead to earn around $60 M [50] after 5 years.

Concerning the potential savings, streamlined documentation and the reduction of legacy system have been taken into account. These factors lead to reduce number of employees and redundant processes. Taking into account these parameters, a big company could potentially save around $6 M [50] after 5 years.

Concerning the potential costs that may be incurred, different phases should been taken into account in the blockchain implementation, as pilot phase, commercialization phase and ongoing phase. According to Forrester(2018), the total costs a company can potentially bear are approximately $8 M in 5 years. The costs can vary due mainly to the complexity of the blockchain implementation, numbers of employees involved and project duration. Refer to Appendix C for the full calculation framework.

Regarding the design phase, it is about understand the correct trade-off that will be suitable according to the organizations' goals. Blockchain attributes as immutability and transparency can also have negative consequences; so understanding which attribute is fundamental for your goals is a key aspect in the blockchain implementation. The best way to approach blockchain design is to involve different experts from different sectors in order to take into account different points of view and different approaches to the same problem. As a new technology, company should familiarise with blockchain first by applying it in small context and learn to make the most of blockchain-based networks.

6.1 SocialxChange Goals

SocialxChange (SxC) is a Chilean non-profit organization operating in the impact investment sector. The main issues that SxC wants to address are the lack of transparency, the absence of trust that the fund donated will be effectively used and the limited possibility of tracking how the funds are used and who is benefited. Donors are becoming more and more focused on impact and an increase in the transparency about the effectiveness will lead a change in the donors attitude. The main goal of SxC is to increase the donation in Chile by implementing a blockchain-base solution that will guarantee traceability, transparency and accountability in this sector.

In Chile, according to IMTrust, the sector is highly concentrated, where the 80% of the total donations is managed by 25 organizations. Comparing the US and Chilean donation market is easly to see how in the US the largest part of the donators are individual people(74%) instead in Chile individual people count only 10% of the total amount.

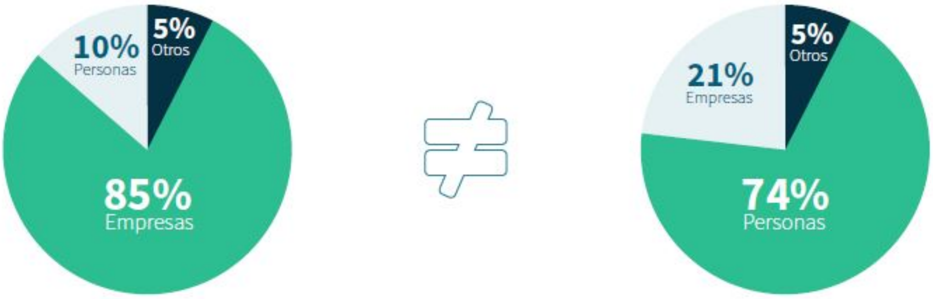


Figure 6.1. Donations in Chile and US

This is due mainly to the lack of trust of People about how the organizations manage the fund donated. SxC does not just want to increase donations in Chile but also redistribute where the funds come from. SxC have understood that impact investors need high-quality and verified impact data. Until now, investors needed to trust centralized organizations that manage the fund, but this business model lead to high inefficiency especially for project that want to impact underdeveloped country. Nonetheless thanks to the blockchain technology is possible to create decentralized platform where anyone can participate in an impact project in ways that is cost-effective and impact-focused.

The blockchain that have been analyzed are Hyperledger Fabrik and ixo network(https://ixo.world/). Hyperledger Fabrik is a open source permissioned blockchain platform designed by the Linux Foundation; refer to Appendix B for the full analysis of this blockchain. As every permissioned blockchain all the participants must be identified. The low number of writers guarantees high transaction throughput performance and low latency of transaction confirmation. This blockchain has been discarded for two main reasons: high degree of centralization and high costs to install a node.

SxC has selected ixo network as the most suitable for its purpose. Ixo network is a decentralized platform where different type of users can collaborate in order to achieve an impact, social or environmental. This network allows to be a project creator, a project investor, a project evaluator or a service provider. The objective of SxC is to create several impact project in its platform and share its projects with

Ixo network, becoming a Project creator, called project sponsor in the ixo network, in order to take advantage of the ixo network userbase and ixo technology.

6.2 ixo Network

SocialxChange(SxC) to addresses its goals has chosen to implement a blockchain-based platform in order to enhance transparency and efficiency in the impact investment sector. The most developed blockchain platform suitable for impact investment is the one developed by Ixo Foundation (`https://ixo.foundation/`).

SxC, thanks to ixo network, wants to break the trilemma and attempts to take advantage of both blockchain consensus model. In ixo network, a PoS blockchain is used as interaction layer between the users, instead a PoW blockchain is used as payment settlement layer.

"Ixo enables anyone to collect, measure, evaluate, value and trade verified impact data, with Proof of Impact" (Ixo Foundation 2017). There are four different kind of users in this protocol:

- Project sponsor
- Investment Agent
- Service Agent
- Evaluation Agent

Investment agents are organizations, institutions or individuals who contribute through all kind of financing mechanisms the different impact investment projects. Service agents are individuals, organizations or devices that delivers services and goods to achieve impact. Finally, Evaluation agents are individuals, organizations or software algorithms that evaluates the impact of the projects, establishing a proof of impact, by processing the impact claim. An impact claim is a certification of the service provided by the service provider. All the agents must at least be identified with their own universal decentralized identifier (DID) and have the necessary credentials.

All of these agents or anyone third party can create a new project. The agent who establishes a project is called project sponsor who is in charge of elaborate the project documentation and defines the impact claim.

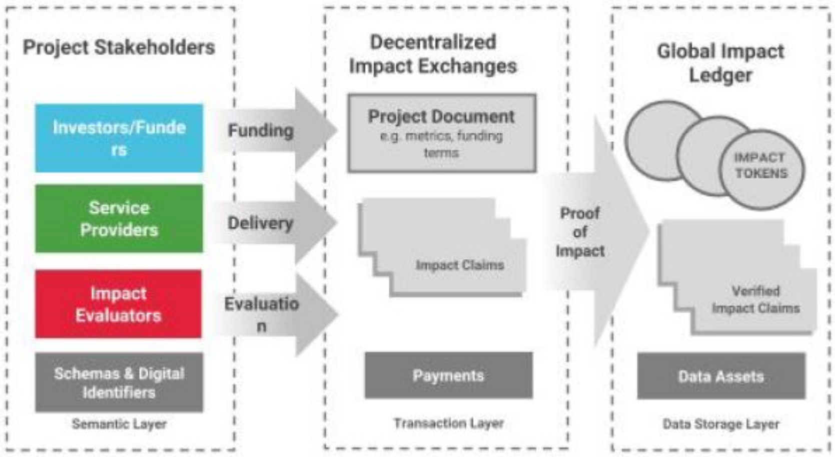


Figure 6.2. Components of the Ixo Operating System [76]

Decentralized Impact Exchange(DIX), based on the Ethereum public network, represents the transaction layer of the operating system. It is used to incentivize and coordinate evaluators, services providers and investors to work together on a specific impact project. Each DIX is a system of smart contracts and it is set up by the project sponsor who defines which impact claim schema will be used, who is authorized to participate and the value transfers between the participants in order to incentivize good behaviours. DIX also manages all the payments between the participants, it can be made using cryptocurrency (IXO Token) or conventional payment methods, with a record of these transactions in the distributed ledger.

The Global Impact Ledger, called ixo network, is a Proof-of-Stake(PoS) decentralized layer for the ixo protocol. It allows to service agents of submitting impact claims in order to be evaluated and validate by authorized evaluation agents. Once a claim has been evaluated, evaluators issue a signed attestation as Proof of impact that collects the result of the evaluation. "Verified impact claims and the associated Proof of Impact are recorded as digital assets in the ledger, in the form of cryptographic Impact Tokens"(Ixo Foundation 2017). This public ledger collects all the impact data that can be shared and used for several valuable applications.

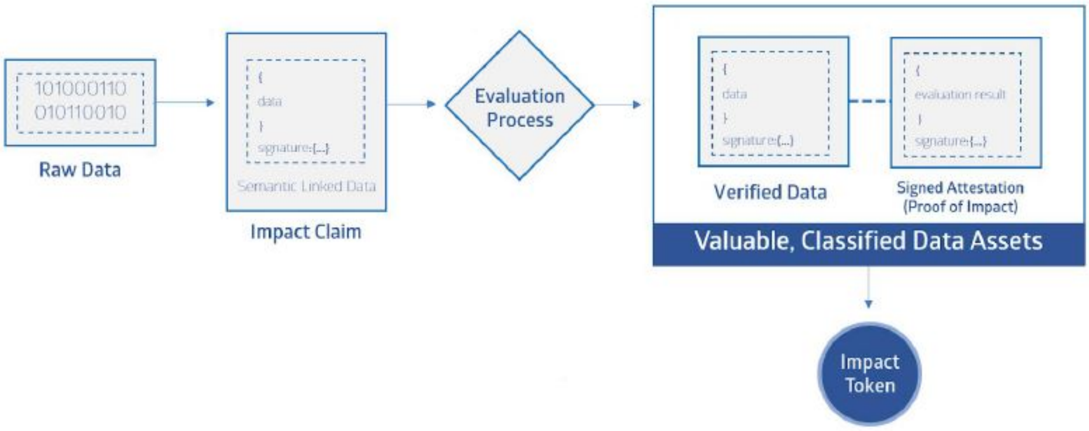


Figure 6.3. The Process for Evaluating an Impact Claim [76]

The evaluation process should include information about where, when, why, how and how much impact occurred. In order to guarantee accountability and prove attribution, data on who delivers, receives, witnesses, measures, evaluates and finances the impact have also to be included.

Analysing step-by-step the coordination of a new project, since the creation of the project until the generation of the impact token, eight different steps can be recognised.

- A project sponsor create the project by setting up a Decentralized Impact Exchange(DIX). Typically the project sponsor is an investment agent but could also be an evaluation agent or a service agent. "They define the project description, participants - including any capabilities the participants must demonstrate, and the impact claims schemas to be used" (Ixo FOundation 2017). The Merkle Root for the Ethereum blockchain is derived from the Project Document.

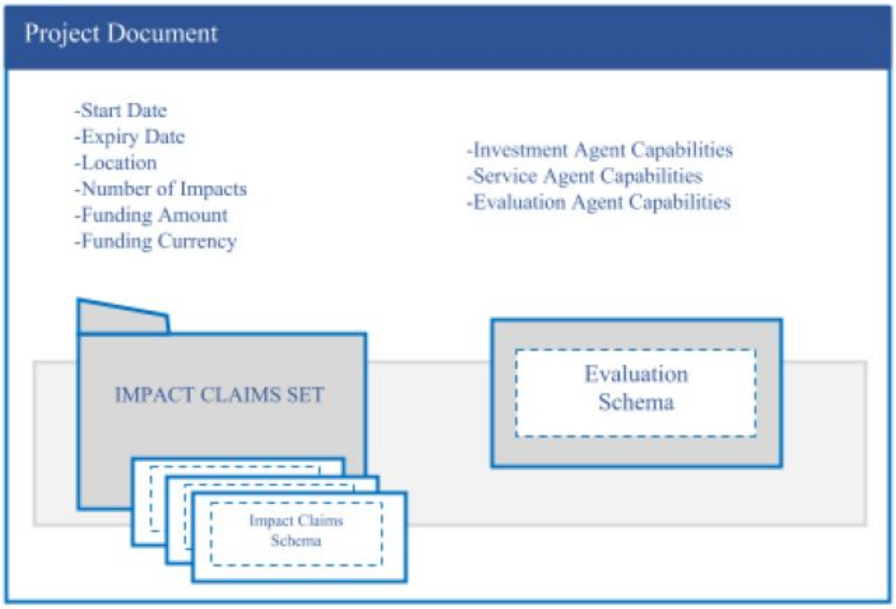


Figure 6.4. The Structure of a Project Document [76]

- In order to start the project, the project sponsor have to deposit a certain amount of IXO token from its IXO wallet to the project's DIX address. When this transaction is finalised, an equivalent amount of ixo-native tokens, called Cosmos Coins, are minted in the ixo network and are associated with the project account. Cosmos coins are used mainly for the fee as claims are processed. When the project owner request a payout, Cosmos Coins are burnt on the ixo network and the payout is made by ERC20 IXO token, where ERC20 is a technical standard utilized in Ethereum blockchain for smart contracts. This process is validated by ixo validator nodes.

- Service agents communicate with the project sponsor through a mobile application developed for the specific use-case. They accept the condition of the project and receive the project impact claim schemas. They will utilise the application in order to digitally record their service and to submit their impact claims into the ixo Network.

- Evaluation agents connected with the DIX accept the condition of the project and evaluate the claim using an agent software. The agent verifies if the evaluation criteria have been successfully met. Then it produces a signed Proof of Impact for the specific claim. For each claim they process, they will gain a specific amount of IXO token, as a payment from the project sponsor.

- The verified impact claim and its related Proof of Impact is recorded digitally in the Global Impact Ledger and an Impact Token is created.

- The service agent is paid by the investment agent when the impact claim have successfully met all the predetermined goals. "At periodic intervals, or after a prescribed number of transactions, the ixo Nodes send signed messages to the DIX smart contract. This produces a state change in the DIX, once a threshold number of signatures has been reached. The state change updates the numbers of IXO Tokens that are allocated to each of the participants in the DIX. In this way, participants receive payments for their services"(Ixo FOundation 2017). This payment can be made off-chain, with a digital record in the DIX, or on-chain. Once the payment is done, a Proof of Payment is generated and this triggers a transfer of ownership of the impact token to the project sponsor.

- A small fixed amount of transaction fee is automatically paid in IXO to the ixo foundation, to fund ongoing operation.

- If the project is evaluated as a good quality impact claim type, new IXO tokens are generated and sent to the project sponsor.

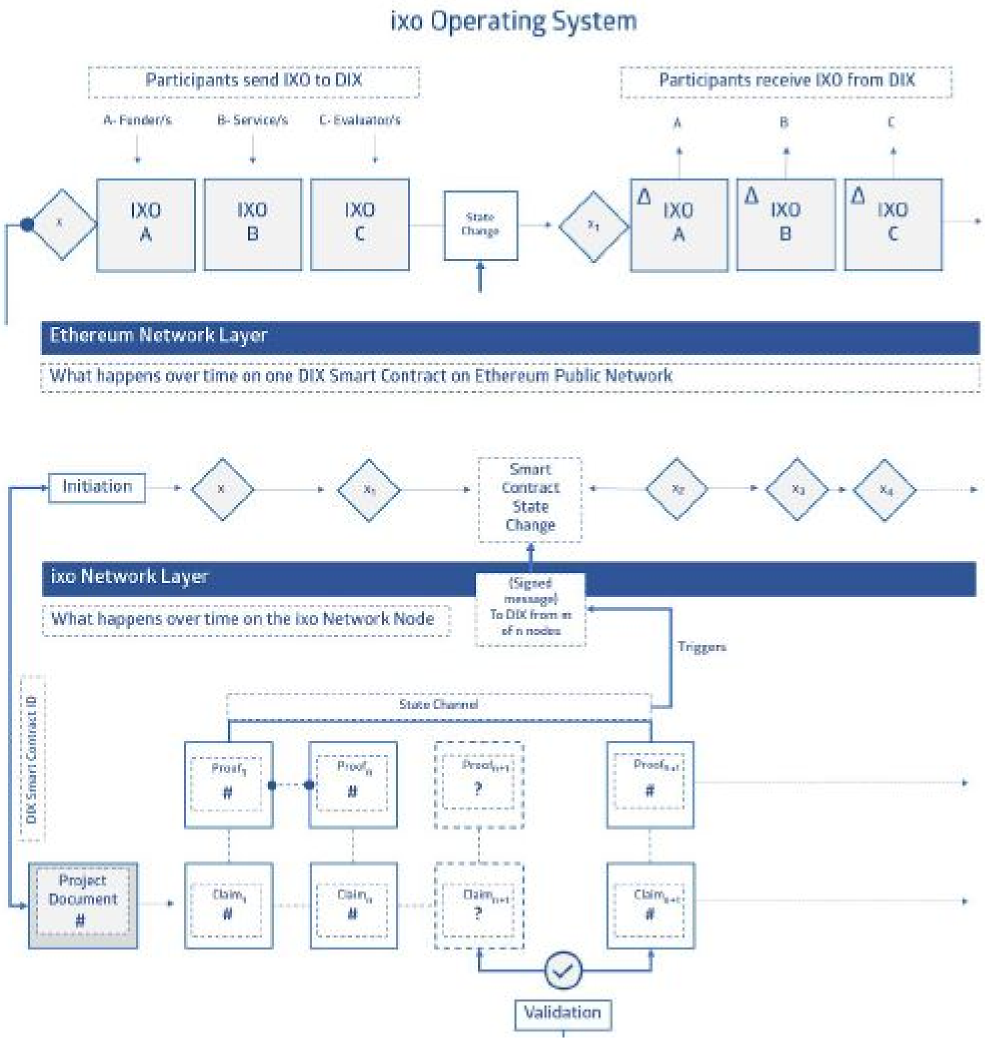


Figure 6.5. Ixo Operating System [76]

Ixo Foundation has created a network were tokens,IXO token and Impact Token, play an important role. "Impact Tokens are generated for a project by a smart contract that algorithmically determines the price on issuance or repurchase of the project's impact tokens, based on a transparent mechanism that statistically measures the probability of the project succeeding"(Ixo Foundation). Impact token is a form of value that can be used in all kind of innovating financial mechanism. In the past, costs to the people, economy and environment, as for example pollution, were qualified as externalities. They were considered non-financial results so they did not been included into the traditional ledger of economic activities. Hence "intangible externalities have not been properly valued, or priced into the real economy" (Dr Shaun Conway (2018)). Impact tokens have the purpose of valuing and pricing "what impacts our economic activities are having in a period" (Dr Shaun Conway (2018)). Each project has its impact token as, education token, carbon token etc; It depends on the impact that is generated. So if an individual or a company wants to help for example a project that reduce carbon emission, by buying carbon token, it generates capital for those project that are creating carbon token. So the idea is to create a new marketplace where the impact is being traded. Actually buying an impact token means buying an information; this market already exists and is called data monetization. For many companies, this market represents one of the biggest profitable business in which they are involved.

IXO is an ERC20 utility token that enables the participants of the ixo network to transact among each others."Token holders have a vested interest to increase the utility of the network and to grow the value of the ixo ecosystem, as they will both directly and indirectly benefit"(Ixo Foundation 2017). Using IXO between participants of the network will enable frictionless transacting across geographic territories. It also provides a more price-stable medium of exchange with respect to Bitcoin or Ether that face unpredictable fluctuation due to excessive market speculation. Ixo network does not hold stocks of tokens. "Pricing of the tokens at the transaction interface is linked to the market price of tokens"(Ixo Foundation 2017).

Ixo foundation has implement a crypto-economic mechanism to protect the users and the network called staking. Stakeholders have to locking up value in the network, this ensure the good behaviour of the participants. "The benefits of increased security and trust make it economically much less costly to defend the network, than to protect the interests of all participants"(Ixo Foundation 2017).

Different staking mechanisms have been implemented:

- Network node stakes a long-term security deposits in order to assure the security, performance and integrity of the network. Attempting of cheating lead to lose the deposit staked. This" Proof-of-Stake" mechanism is managed by using self-executing Ethereum smart contract.

- Project sponsor have to stake in each DIX when they set up a new project. The stake covers the transaction fee and the payment for the evaluation agent. Any residual deposit left at the end of the project is returned to the project sponsor.

- Evaluation agents stake performance deposit if requested by the project sponsor, in order to guarantee a quality service.

- The community can stake in order to give the priority to a specific impact claims for sustainable development impacts.

- The decentralized governance of the network is achieved by a PoS consensus model, where users have a proportional number of votes related to the size of stakes.

Tokens that are lost due to penalty mechanism will be automatically burned. "Staking also has the effect of increasing the long-term non-speculative value of the network, which grows as more people become vested in the network and its ecosystem. Total IXO token supply staked at any point in time will therefore become a proxy measure of how well the network achieving its intended purpose"(Ixo Foundation).

Hence, The two layer structure due to the implementation of both PoS and PoW, powered by Ethereum blockchain, consensus model allows to take advantage of the security of Ethereum blockchain, used for the payment between the participants, for staking and for holding the project documentation. Instead the PoS layer, ixo blockchain, is used to establish the Proof of Impact for each project and to transact with Impact Token; here the capacity for high-throughput volumes and low-cost transaction costs is needed. The ixo network will provide inputs to trigger state-changes in Ethereum blockchain.

How do Ethereum blockchain and ixo network communicate? The communication between these two blockchains, having different consensus models and tokens, is possible thanks to to Cosmos network (https://cosmos.network/). Cosmos is defined has internet of blockchain. The benefit of implementing Cosmos network is to create an ecosystem made by different type of blockchains that exchange data and value. In this way it is possible to take advantage of blockchains that leverage on efficiency for several application and blockchain that leverage on decentralization and security. This solution allows to scale up blockchain ,as Ethereum and Bitcoin, that guarantee a decentralized decision-making but scarifying cost and time efficiency.

Cosmos Ecosystem

Essentially, "Cosmos is designed around the concept of standardizing communication between various blockchains that are part of its broader ecosystem to facilitate interoperability"(Brian Curran (2018)). Cosmos' ecosystem is composed by several independent blockchain called "zone", that are interconnected to a central blockchain called "hub".

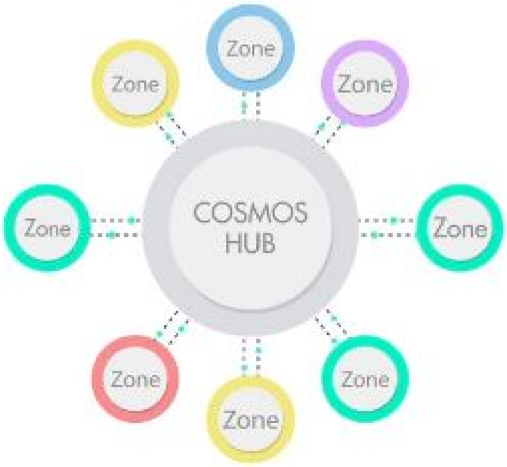


Figure 6.6. Cosmos' ecosystem [85]

The zones can communicate each other through the Hub via Inter-Blockchain Communication (IBC) protocol. Cosmos blockchain is built on the Tendermint engine (https://tendermint.com/ that is composed of two main parts: Tendermint Core, the BFT Proof-of-Stake Consensus Engine and Application Blockchain Interface (ABCI), the BFT replication of dapps in multiple programming languages.

> "Tendermint core underlies the consensus of the Cosmos Hub, and subsequently the broader network for managing a standardized exchange of tokens between zones. It is important to note that blockchains plugged into Cosmos retain their consensus sovereignty, and do not forfeit it to the larger Cosmos PoS consensus"(Brian Curran (2018)).

Concerning Application Blockchain Interface (ABCI), it is a critical component in the Cosmos ecosystem flexibility. It allows applications written in any programming languages to run on top of the Tendermint consensus engine. So Cosmos can support a wide variety of currencies and programming languages like those found in Bitcoin, Ethereum and more.

As mentioned above, the communication between the zones works via IBC protocol. It is natively supported by Tendermint-based zones, so for this reason ABCI is a critical component .It is a stardardized communication protocol across the network and between blockchains with independent consensus model; It enables users to transfer asset across the network.

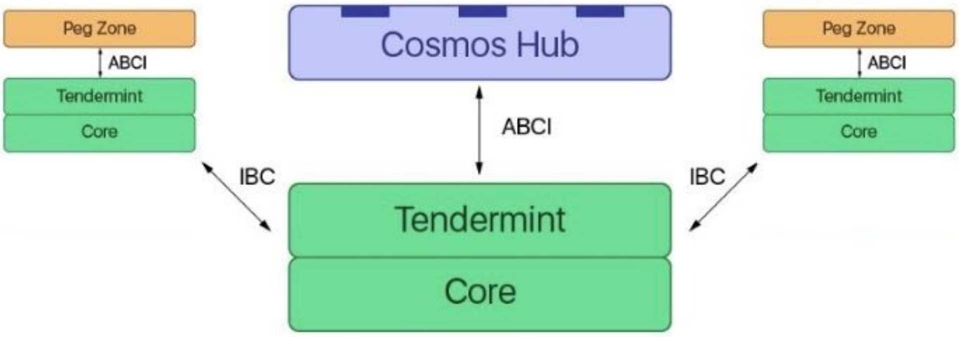


Figure 6.7. Cosmos Hub and Zones[84]

Ixo world needs to standardize the communication between Ethereum, running on a PoW consensus model, and the Cosmos ecosystems, running on a PoS consensus model. Terdermint has developed two different kind of implementations of the Ethereum blockchain that runs on top of Tendermint consensus: Ethermint(https://ethermint.zone/) and Ethereum Peg Zone.

Ethermint's goal is to provide to the developers the capabilities of writing and executing Ethereum's smart contracts plus the added performance benefits of Tendermint's consensus protocol. Thanks to Tendermint's ABCI application, anybody can take the Ethereum code and run it on Proof-of-Stake consensus engine. "Tendermint can process up to 20 times the number of transactions as the Ethereum Virtual Machine, so executing a smart contract in Ethermint equates to something on the order of 20 to 50 times the savings in transaction fees. (EVM)"(Interchain Foundation). This implementation strips of PoW mining, but does not enable the movement of ERC20 tokens.

Ethereum Peg Zone instead enables the transaction of the ERC20 tokens even if they run on a PoW consensus engine. In this operation five different elements are involved: Ethereum smart contracts, a witness, the peg zone, a signer and a relayer:

- Ethereum smart contracts act as asset custodians, they are capable of taking custody of Ethereum ERC20 native tokens and issuing Cosmos native tokens.
- The witness is in charge of attests events that happen in Ethereum . "It runs a fully validating Ethereum node in order to attest to state changes within Ethereum by submitting a WitnessTX to the peg zone"(Chjango Unchained(2018)).
- The peg zone is a blockchain powered by Tendermint consensus model that

allows users to query and perform transactions and enables the communication between Cosmos and Ethereum

- "The signer component generates secp256k1 signatures via the SignTx message and posts it to the peg zone for relaying transactions for validation in the smart contract down the pipeline"(Chjango Unchained(2018)).
- "The relayer component relays a batched list of transactions, signed by the Signer component, and posts them to the Ethereum smart contract"(Chjango Unchained(2018)).

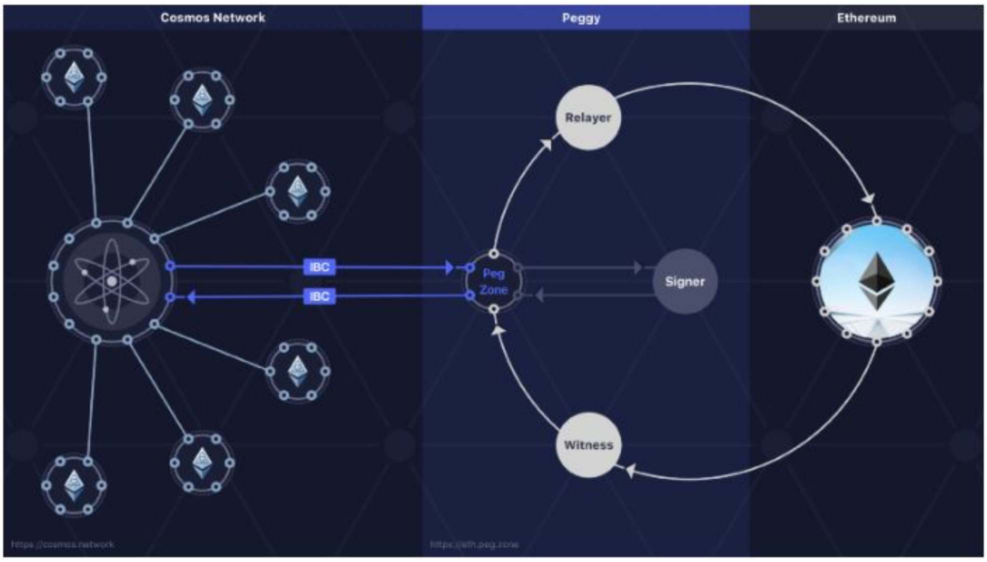


Figure 6.8. Ethereum Peg Zone [87]

In order to move some quantity of Cosmos native tokens and convert them in Ether, four different steps have been recognised:

1. Cosmos Hub transfers via IBC, through a message containing the transaction, Cosmos native coins to the peg zone. Then "Signers monitoring the peg zone then sign those IBC transactions, effectively converting the signature scheme to Ethereum-understandable private keys"(Chjango Unchained (2018)). In this operation the transaction has been signed on the peg zone.
2. Relayers wait that more than 2/3 of signers have signed the transaction and then batch that into a list with other transactions sent via IBC. Finally they sent the list to the EVM where Ethereum smart contracts live.

3. after checking that the transitions are valid, the smart contract generates an ERC20 version of the Cosmos native coin. finally it sends the ERC20 tokens to your destination address in Ethereum.

4. At this point, ERC20 tokens are converted in ETH by using a decentralized exchange.

Ixo world has implemented an Ethereum peg zone, because the exchange of data and tokens is critical for its goal.

use-case

The first use-case where SxC will be involved is the standardisation of 100 form of social donations of a subset of foundations and NGOs in Chile. The goal of this project is to record all this forms into an immutable ledger as the blockchain. This project was also carried out to familiarise with the ixo protocol and understand better how the users interact each other and how the incentive system works.

Analysing step-by-step the coordination of a new project, since the creation of the project until the generation of the impact token, six different steps can be recognised:

- The project sponsor, SxC in this case, create the project by setting up a Decentralized Impact Exchange(DIX), by defining the project description, participants and the impact claims schemas to be used.

- to start the project, SxC have to deposit a certain amount of IXO token from its IXO wallet to the project's DIX address. When this transaction is finalised, an equivalent amount of ixo-native tokens, called Cosmos Coins, are minted in the ixo network. Cosmos coins are used mainly for the fee as claims are processed.

- Service agents accept the condition of the project and receive the project claim schemas as in (Table 6.1).

- Evaluator agents accept the condition of the project and evaluate the claim by verifying if the evaluation criteria have been successfully met. At the end of the evaluation, a signed proof of impact is produced and the evaluator gains a specific amount of IXO token , set in the project creation. Evaluators are paid by SxC.

- The verified impact claim and its related Proof of Impact is recorded digitally in the Global Impact Ledger and an Impact Token is created.

- The service agent is paid by the investment agent when the impact claim have successfully met all the predetermined goals. Once the payment is done, a Proof of Payment is generated and this triggers a transfer of ownership of the impact token to the SxC.

To setting up a new project, a form must be fill out and the following information are required:

- The main information of the project: Name, Duration and Location.
- Where is possible to see more information about the project as ,Facebook, Twitter, Instagram, Web site.
- Project description and which impact is the project measuring.
- Which SDG (sustainable goals development) is your project helping to reach.
- How many claim would make successful the project.
- What kind of knowledge and expertise are required for the service provider.
- what kind of proof have to be submitted in order for the project claim to be approved as photos, receipt and more.
- What kind of knowledge and expertise are required for the evaluation agent. (Data specialist)

In order to incentivize the good behavior of the user and the good quality of the work, the project sponsor have to set up also the incentive system. The project sponsor is in charge to pay the fee of the network, that is based on how many transactions are required in the project, in this case 346, and the evaluator agents. The transaction fees that should be taken into account are the Ethereum fees : 0.0716$ for transaction [88] (at 21/01/2019). So based on this amount, project sponsor have to "lock" in the Ethereum wallet of the project a certain amount of Ixo tokens. Instead, the service providers are paid by the investment agents.

SxC should lock in the project's Ethereum wallet:

- fees: 0.0716$ $\times 346 = 24.77\$ \Rightarrow 24.81$€.
- evaluation agents reward: 1.5€$\times$ 346= 519€.

So the total amount of the project's Ethereum wallet is 544€.

Instead, concerning the Service providers, the reward is set up at 5€each filled out project claim. So investment agents should collect 5€$\times$346= 1384€.

finally, the project claim schema to be used by the services provider is set as following:

Table 6.1. Project Claim schema

JSON Document			
Data N	Variable	Details	Answer Choices
1	ID	Identifier code	
2	Year of publication	Year in which the form was published	
3	Reporting period	Year of report	
4	Organization name		
5	Legal organization structure	Legal form of the organisation	Foundation, Corporation, NGO, Other
6	Location headquarters	Legal address of the organization	
7	Website	Organization's web domain	
8	Mission	Statement of the organization's purposes and goals	
9	Sector	Sector or area in which the organization focuses and seeks to influence	Agriculture, Handicrafts, Environment, Culture, Education, Energy, Health, Housing and community development, Infrastructure, Other
10	Target beneficiaries	Type of people who will receive the benefits created by the organization	
11	N of employees	Total number of employees working at the foundation	
12	N of volunteers		
13	Total income [M$]		
14	Donated income [M$]	Amount of private donation	
15	Member dues income [M$]	Amount paid by the partners of the foundation	
16	Subsidy income [M$]	Amount subsidized by the State	
17	Total private income [M$]	Sum of all income from private sources (donations, projects, sale of services and products, membership fees, etc.)	
18	Total state revenue [M$]	Sum of all income earned from the state (grants, projects, sale of products and services, others)	
19	Equity [M$]		
20	Net result (surplus/deficit) [M$]	Surplus or deficit for the year	
21	N of beneficiaries	Number of people benefited by the projects generated by the organization	
22	N of indirect beneficiaries		
23	Year of foundation	Year the organization was founded	
24	Customer model	Type of business model used by the organization	B2B, B2C, B2G, Otros
25	Operational model	Type of operational model of the organization	Production or Manufacturing, Research, Service, Distribution, Other
26	Target socio-economic stratum	Socio-economic level(s) to which the target beneficiaries belong	
27	Number of projects		
28	Number of communes served		
29	List of certifications (processes and practices)	List of certifications of processes and practices of the organization granted by third parties	
30	Income with restriction [M$]	Amount of income that is restricted in its use	
31	Current assets [M$]	Short-term assets	
32	Fixed assets [M$]	Long-term asset	
33	Current liabilities [M$]	Short-term liabilities	
34	Total assets [M$]		
35	Total liabilities [M$]		
36	Loans payable [M$]		
37	Remunerations [M$]	Wages, bonuses and fees of the organization's employees	
38	Program expenses [M$]		
39	General expenses		
40	Administrative expenses [M$]		
41	Fundraising expenses [M$]		
42	Total expenditure [M$]		
43	Audit	Indicate if the balance sheet was audited	

Chapter 7

Conclusion

The thesis presents an overview of the blockchain technology, an analysis over its different settings and its possible implementation for impact investment. The analysis of the trade off between decentralized recordkeeping and cost efficiency is guided by the blockchain trilemma. A surprising result, arises from the study of ixo network, is that the employment of a interchain network allows multiple parallel independent blockchain to interoperate while preserving their own property. In this way an application on the one hand can take advantage of the efficiency of a network for some transactions and on the other hand can take advantage of the security assured by a more decentralized environment. This cross-chain communication can also solve the problem of the portability of information that is present in every network.

This dissertation examined the differences between the inefficiency of the actual investment impact sector and the potential improvements due to a blockchain implementation. A distributed ledger technology can improve effectiveness, reduce friction between agencies, reduce bureaucratic barriers, foster automation through smart contracts and enhance accountability and transparency. Blockchain implementation can have an impact on millions of people thanks to its key attributes.

The mass adoption of this technology will take time because of there are different barriers that are slowing down the implementation. The main issues companies are facing concern : market regulation and technological limits.

Beyond technological limits, blockchain faces another problem related to the human interaction. who can guarantee that what happen in the blockchain is enforced in the real world?. A validator, as in ixo network, or the integration of artificial intelligent, it depends on use-cases, is fundamental to ensure the proper functionality.

Concerning future improvements of this thesis, different consensus model can be taken into account and analyzed in order to enhance both the model and the trilemma.

Blockchain for several use-cases will disrupt many industries, the financial one overall, but for some use-cases this technology is overhyped. Even if the application of a distributed ledger technology is sometimes useless, this revolution will pave the way for markets always less centralized, reducing increasingly the inefficiencies of the current economy.

Bibliography

[1] Chiu, J. and T. Koeppl (2018): “Blockchain-based Settlement for Asset Trading" *Review of Financial Studies*.

[2] Chiu, J. and T. Koeppl (2017): “The Economics of Cryptocurrencies - Bitcoin and Beyond" *SSRN Working paper*, DOI 10.2139/ssrn.3048124.

[3] Böhme,Christin, Edelman and Moore (2015): “Bitcoin: Economics, Technology, and Governance" https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.29.2.213.

[4] Chiu and Koeppl: “Incentive compatibility in the Blockchain" https://www.bankofcanada.ca/wp-content/uploads/2018/07/swp2018-34.pdf.

[5] Jamie Berryhill, Théo Bourgery and Angela Hanson (2018): “Guide to blockchain technology and its use in the public sector " http://www.oecd.org/innovation/innovative-government/oecd-guide-to-blockchain-technology-and-its-use-in-the-public-sector.htm.

[6] David Lehr and Paul Lamb(2018): “Digital currencies and blockchain in the social sector" https://ssir.org/articles/entry/digital_currencies_and_blockchain_in_the_social_sector1?utm_source=Enews&utm_medium=Email&utm_campaign=SSIR_Now&utm_content=Title#.

[7] Hanna Halaburda (2018): “Blockchain Revolution Without the Blockchain" https://works.bepress.com/halaburda/33/.

[8] Haeringer and Halaburda (2018): “Bitcoin: A Revolution?" .

[9] OECD Secretariat (2018): “Blockchain Technology and Competition Policy " http://www.oecd.org/daf/competition/blockchain-and-competition-policy.htm.

[10] Greg Medcraft Presentation OECD : “The OECD and the Blockchain Revolution".

[11] Vedat Akgiray (2018): “Blockchain Technology and Corporate Governance OECD Report".

[12] John Barrdear and Michael Kumhof (2016): “The macroeconomics of central bank issued digital currencies" https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2016/

the-macroeconomics-of-central-bank-issued-digital-currencies.pdf?la=en&hash=341B602838707E5D6FC26884588C912A721B1DC1.

[13] Jamsheed Shorish (2017): “Blockchain State Machine Representation " https://osf.io/preprints/socarxiv/eusxg/.

[14] Gatteschi,Lamberti,Demartini,Pranteda,SantamarÃa (2018): “To Blockchain or Not to Blockchain: That Is the Question" https://osf.io/preprints/socarxiv/eusxg/.

[15] Gatteschi,Lamberti,Demartini,Pranteda,SantamarÃa (2018): “Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?"

[16] Lapointe and Fishbane (2018): “The blockchain ethical design framework "

[17] Galen,El-Baz,Brand,Kimura,Boucherle,Wharton,Davis,Lee and Do (2018): “Blockchain for social impact, moving beyond the hype "

[18] Taylor, Michael Bedford (2013): “Bitcoin and the Age of Bespoke Silicon." http://cseweb.ucsd.edu/~mbtaylor/papers/Bitcoin_taylor_cases_2013.pdf

[19] Möser and Böhme (2014): “Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees." http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2530843

[20] Zervas, G., Proserpio, D., Byers, J. W. (2017): “The Rise of the Sharing Economy: Estimating the Impact of Airbnb on the Hotel Industry. " http://journals.ama.org/doi/abs/10.1509/jmr.15.0204

[21] Broadridge (2015): “Charting a Path to a Post-Trade Utility. How Mutualized Trade Processing can Reduce Costs and Help Rebuild Global Bank ROE."

[22] Ponemon Institute Research Report, October (2016) : “2016 Cost of Cyber Crime Study & the Risk of Business Innovation"

[23] Mckinsey (2017): “Fueling-growth-through-data-monetization" https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/fueling-growth-through-data-monetization

[24] Fortune (2018): “Facebook Cambridge Analytica Scandal: 10 Questions Answered" http://fortune.com/2018/04/10/facebook-cambridge-analytica-what-happened/

[25] PWC (2018): “PwC’s Global Blockchain Survey 2018"

[26] Deloitte (2018): “Breaking blockchain open Deloitte’s 2018 global blockchain survey"

[27] Laura Gargolinski (2018): “Public versus private: What to know before getting started with blockchain" https://www.ibm.com/blogs/blockchain/2018/10/public-versus-private-what-to-know-before-getting-started-with-blockchain/

[28] Nouriel Roubini (2018): “Blockchain isn’t about democracy and decentralisation - it’s about greed"

https://www.theguardian.com/technology/2018/oct/15/blockchain-democracy-decentralisation-Bitcoin-price-cryptocurrencies

[29] blockgeeks: “Blockchain Scalability: When, Where, How?" https://blockgeeks.com/guides/blockchain-scalability/

[30] blockgeeks: “What Is Hashing? Under The Hood Of Blockchain" https://blockgeeks.com/guides/what-is-hashing/

[31] Medium: “Blockchain Fundamentals #1: What is a Merkle Tree?" https://medium.com/byzantine-studio/blockchain-fundamentals-what-is-a-merkle-tree-d44c529391d7

[32] Bitcoinbook: “Blockchain"https://github.com/Bitcoinbook/Bitcoinbook/blob/develop/ch09.asciidoc

[33] Mattia Franzoni: “Analysis on main Bitcoin mining-pools" https://medium.com/novamining/analysis-on-main-Bitcoin-mining-pools-2d14c5d73b10

[34] Blockchain.com: https://www.blockchain.com/it/pools

[35] etherchain.org https://www.etherchain.org/charts/topMiners

[36] Max Thake: “What is Proof of Stake" https://medium.com/nakamo-to/what-is-proof-of-stake-pos-479a04581f3a

[37] blockgeeks: “What is Ethereum Casper Protocol? Crash Course" https://blockgeeks.com/guides/Ethereum-casper/

[38] James Ray: “problems" https://github.com/Ethereum/wiki/wiki/Problems

[39] Georgios Konstantopoulos: “Understanding Blockchain Fundamentals, Part 3: Delegated Proof of Stake" https://medium.com/loom-network/understanding-blockchain-fundamentals-part-3-delegated-proof-of-stake-b385a

[40] steemit: “DPOS Consensus Algorithm - The Missing White Paper" https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper

[41] github: “EOS.IO Technical White Paper v2" https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md#free-usage

[42] Jimmy Song: “The truth about smart contracts" https://medium.com/@jimmysong/the-truth-about-smart-contracts-ae825271811f

[43] Sherman Lee: “Blockchain Smart Contracts: More Trouble Than They Are Worth?"https://www.forbes.com/sites/shermanlee/2018/07/10/blockchain-smart-contracts-more-trouble-than-they-are-worth/#2f58619f23a6

[44] Abadi and Brunnermeier (2018): “Blockchain Economics"

[45] Hyperledger 2018: “Introduction" https://hyperledger-fabric.readthedocs.io/en/release-1.3/whatis.html

[46] Hyperledger 2018: “Functionalities" https://hyperledger-fabric.readthedocs.io/en/release-1.3/functionalities.html

[47] Hyperledger 2018: “Ledger" https://hyperledger-fabric.readthedocs.io/en/release-1.3/ledger/ledger.html

[48] Muntasir Mamun: “How does Hyperledger Fabric works?" https://medium.com/coinmonks/how-does-hyperledger-fabric-works-cdb68e6066f5

[49] Hyperledger 2018: “Peers" https://hyperledger-fabric.readthedocs.io/en/release-1.3/peers/peers.html

[50] Forrester 2018: “Emerging Technology Projection: The Total Economic Impact Of IBM Blockchain"

[51] NovaMining: “Crypto Economy: a new era for the financial markets" https://medium.com/novamining/crypto-economy-a-new-era-for-the-financial-markets-573b99a8d17f

[52] Sudhir Khatwani: “9 Most Profitable Proof Of Stake (POS) Cryptocurrencies" https://coinsutra.com/proof-of-stake-cryptocurrencies/

[53] stakingrewards.comhttps://stakingrewards.com/

[54] Pool Of Stake: “PoW vs PoS showdown: which is more centralized?" https://medium.com/@poolofstake/pow-vs-pos-showdown-which-is-more-centralized-aaa01c8052b3

[55] Robert Greenfield IV (2017): “Vulnerability: Proof of Work vs. Proof of Stake" https://medium.com/@robertgreenfieldiv/vulnerability-proof-of-work-vs-proof-of-stake-f0c44807d18c

[56] Pool Of Stake: “Centralization in Proof of Stake" https://cryptocurrencyhub.io/centralization-in-proof-of-stake-96f6605c0c13

[57] Reddit: “Proof of Stake leads to centralization, with worse consequences than PoW" https://www.reddit.com/r/Ethereum/comments/6d1mca/proof_of_stake_leads_to_centralization_with_worse/

[58] Bitfury Group: “Proof of Stake versus Proof of Work"

[59] Freedom House: https://freedomhouse.org/report/freedom-world/freedom-world-2018

[60] e-Estonia:https://e-estonia.com/solutions/

[61] e-Estonia:https://e-estonia.com/wp-content/uploads/updated-facts-estonia.pdf

[62] World Bank: http://id4d.worldbank.org/global-dataset

[63] World Bank: “The Global Findex Database 2014" http://documents.worldbank.org/curated/en/187761468179367706/pdf/WPS7255.pdf#page=32

[64] Mike Orcutt: “Who Will Build the Health-Care Blockchain?" https://www.technologyreview.com/s/608821/who-will-build-the-health-care-blockchain/

[65] Jocelyne Sambira(2013): “Counterfeit drugs raise Africa’s temperature" https://www.un.org/africarenewal/magazine/may-2013/counterfeit-drugs-raise-africa%E2%80%99s-temperature

[66] Sustainable Development Goals: “About the Sustainable Development Goals" https://www.un.org/sustainabledevelopment/sustainable-development-goals/

[67] United Nations conference on Trade and Development: “Developing countries face $2.5 trillion annual investment gap in key sustainable development sectors, UNCTAD report estimates" https://unctad.org/en/pages/PressRelease.aspx?OriginalVersionID=194

[68] Fidelity Charitable: “The Future of Philanthropy" https://www.fidelitycharitable.org/docs/future-of-philanthropy.pdf

[69] World Food Program:(http://innovation.wfp.org/project/building-blocks)

[70] Paynter, Ben: “How Blockchain Could Transform The Way International Aid Is Distributed" https://www.fastcompany.com/40457354/how-blockchain-could-transform-the-way-international-aid-is-distributed

[71] Fidelity Charitable: “Fidelity CharitableÂ® donors drive a record-breaking year for charitable giving, $4.5 billion granted to charity through more than 1 million grants in 2017" https://www.fidelitycharitable.org/about-us/news/donors-drive-record-breaking-year-for-charitable-giving.shtml

[72] Ixo Foundation:https://ixo.foundation/

[73] Arena: “Improving Time to Market" https://www.arenasolutions.com/resources/articles/time-to-market/

[74] Report to the nations: “Global study on occupational fraud and abuse" https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf

[75] Social Impact Investment Taskforce (2014): “Measuring Impact" https://www.thinknpc.org/wp-content/uploads/2018/07/IMWG_Measuring-Impact1.pdf

[76] Ixo Foundation (2017): “Ixo the blockchain for impact" https://ixo.foundation/wp-content/uploads/2018/08/ixo-Technical-White-Paper-w-Cover-Version-3.0-8-December-2017-1.pdf

[77] Ixo Foundation :(https://ixo.foundation/faqs/)

[78] IMTrust and credicorp capital: "Fundaciones y FilantropÃa en Chile: Impacto y DesafÃos" http://comunidad-org.cl/wp-content/uploads/2016/11/Fundaciones-y-Filantrop%C3%ADa-Impacto-y-Desaf%C3%ADos-PRESENTACION-v3-_.pdf

[79] Crypto id:https://chainz.cryptoid.info/strat/#!network

[80] Crypto id:https://chainz.cryptoid.info/pivx/#!network

[81] Dr Shaun Conway (2018): “The ixo-Cosmos blockchain for sustainability" https://medium.com/ixo-blog/

the-ixo-cosmos-blockchain-for-sustainability-69c64bc5b505

[82] Dr Shaun Conway (2018): “ixo Bridging Cosmos into Ethereum" https://medium.com/ixo-blog/ixo-bridging-cosmos-into-Ethereum-2d4d1d3d1f62

[83] Brian Curran (2018): “Beginner’s Guide to Tendermint: Byzantine Fault Tolerant Blockchain Engine" https://blockonomi.com/tendermint-guide/

[84] Brian Curran (2018): “Beginner’s Guide to Cosmos: The Tendermint-Based Blockchain Ecosystem" https://blockonomi.com/cosmos-tendermint-based-blockchain-ecosystem/

[85] Blockgeeks: “What is Cosmos Blockchain? The Most Comprehensive Guide" https://blockgeeks.com/guides/cosmos-blockchain-2/

[86] Interchain Foundation: “A Beginner’s Guide to Ethermint" https://blog.cosmos.network/a-beginners-guide-to-ethermint-38ee15f8a6f4

[87] Chjango Unchained(2018): “The Technicals of Interoperability- Introducing the Ethereum Peg Zone" https://blog.cosmos.network/the-internet-of-blockchains-how-cosmos-does-interoperability-starting-with-the-Eth

[88] bitinfocharts: https://bitinfocharts.com/comparison/Ethereum-transactionfees.html

Appendix A

Code for calculation

θ=h
τ=t
σ=o
ϕ=p
$\eta = n$

A.1 Graph of $\phi(\sigma)$

```
h1=–1
h2=−0.5
h3=0.5
h4=1

F1=0.6
F2=0.7
F3=0.8
F4=1

t=1
k=0.1
t1=−0.1
p=0.4

o1=0.3
o2=0.4
o3=5.4
o4=15.4
```

```
o5=20.4

for i in range(1,6):
  j=0

  if i==1:

    while True:
      if j==1:
         p=0

      if j>1:
         p=p+0.01

      j=j+1

      o=o1

      v1=h1+(t+o*n1)+k*p
      v2=h2+(t+o*n1)+k*p
      v3=h3+(t+o*n1)+k*p
      v4=h4+(t+o*n1)+k*p

      if v1>0:
        x1='A'
        pA=F1
        pB=0
      if v1<0:
        x1='B'
        pB=F1
        pA=0

      if v2>0:
        x2='A'
        pA=pA+(F2-F1)
      if v2<0:
        x2='B'
        pB=pB+(F2-F1)

      if v3>0:
        x3='A'
```

```
            pA=pA+(F3-F2)
        if v3<0:
            x3='B'
            pB=pB+(F3-F2)

        if v4>0:
            x4='A'
            pA=pA+(F4-F3)
        if v4<0:
            x4='B'
            pB=pB+(F4-F3)

        p1=pA

        if (abs(p1-p)<0.001 or p>1 ):

            print('sigma=',o1,'equilibrium ',p1,p)
            break

j=1


if i==2:

    while True:
        if j==1:
              p=0

        if j>1:
              p=p+0.01

        j=j+1

        o=o2

        v1=h1+(t+o*n1)+k*p
        v2=h2+(t+o*n1)+k*p
        v3=h3+(t+o*n1)+k*p
        v4=h4+(t+o*n1)+k*p

        if v1>0:
            x1='A'
            pA=F1
            pB=0
        if v1<0:
            x1='B'
            pB=F1
            pA=0

        if v2>0:
            x2='A'
            pA=pA+(F2-F1)
        if v2<0:
            x2='B'
            pB=pB+(F2-F1)

        if v3>0:
            x3='A'
            pA=pA+(F3-F2)
        if v3<0:
            x3='B'
            pB=pB+(F3-F2)

        if v4>0:
            x4='A'
            pA=pA+(F4-F3)
        if v4<0:
            x4='B'
            pB=pB+(F4-F3)

        p2=pA

        if (abs(p2-p)<0.001 or p>1 ):

            print('sigma=',o2,'equilibrium ',p2,p)
            break

j=1

if i==3:

    while True:
```

```
if j==1:
    p=0

if j>1:
    p=p+0.01

j=j+1

o=o3

v1=h1+(t+o*n1)+k*p
v2=h2+(t+o*n1)+k*p
v3=h3+(t+o*n1)+k*p
v4=h4+(t+o*n1)+k*p

if v1>0:
   x1='A'
   pA=F1
   pB=0
if v1<0:
   x1='B'
   pB=F1
   pA=0

if v2>0:
   x2='A'
   pA=pA+(F2-F1)
if v2<0:
   x2='B'
   pB=pB+(F2-F1)

if v3>0:
   x3='A'
   pA=pA+(F3-F2)
if v3<0:
   x3='B'
   pB=pB+(F3-F2)

if v4>0:
   x4='A'
   pA=pA+(F4-F3)
```

```
            if v4<0:
                x4='B'
                pB=pB+(F4-F3)

            p3=pA

            if (abs(p3-p)<0.001 or p>1 ):

                print('sigma=',o3,'equilibrium',p3,p)
                break

    j=1

    if i==4:

        while True:
            if j==1:
                p=0

            if j>1:
                p=p+0.01

            j=j+1

            o=o4

            v1=h1+(t+o*n1)+k*p
            v2=h2+(t+o*n1)+k*p
            v3=h3+(t+o*n1)+k*p
            v4=h4+(t+o*n1)+k*p

            if v1>0:
                x1='A'
                pA=F1
                pB=0
            if v1<0:
                x1='B'
                pB=F1
                pA=0

            if v2>0:
```

```
            x2='A'
            pA=pA+(F2−F1)
          if v2<0:
            x2='B'
            pB=pB+(F2−F1)

          if v3>0:
            x3='A'
            pA=pA+(F3−F2)
          if v3<0:
            x3='B'
            pB=pB+(F3−F2)

          if v4>0:
            x4='A'
            pA=pA+(F4−F3)
          if v4<0:
            x4='B'
            pB=pB+(F4−F3)

          p4=pA

          if (abs(p4−p)<0.001 or p>1 ):

            print('sigma=',o4,'equilibrium',p4,p)
            break

    j=1
    if i==5:

        while True:
          if j==1:
              p=0

          if j>1:
              p=p+0.01

          j=j+1

          o=o5
```

```
v1=h1+(t+o*n1)+k*p
v2=h2+(t+o*n1)+k*p
v3=h3+(t+o*n1)+k*p
v4=h4+(t+o*n1)+k*p

if v1>0:
   x1='A'
   pA=F1
   pB=0
if v1<0:
   x1='B'
   pB=F1
   pA=0

if v2>0:
   x2='A'
   pA=pA+(F2-F1)
if v2<0:
   x2='B'
   pB=pB+(F2-F1)

if v3>0:
   x3='A'
   pA=pA+(F3-F2)
if v3<0:
   x3='B'
   pB=pB+(F3-F2)

if v4>0:
   x4='A'
   pA=pA+(F4-F3)
if v4<0:
   x4='B'
   pB=pB+(F4-F3)

p5=pA

if (abs(p5-p)<0.001 or p>1 ):

   print('sigma=',o5,'equilibrium',p5,p)
   break
```

A.2 Graph of $\phi(k)$

```
import matplotlib.pyplot as plt
import numpy as np


h1=-1
h2=-0.5
h3=0.5
h4=1

F1=0.6
F2=0.7
F3=0.8
F4=1

t=1
#k=0.1
n1=-0.1
o=1.5

p=0.4

k1=0.374
k2=0.375
k3=0.376

for i in range(1,4):
  j=0

  if i==1:

    while True:
      if j==1:
         p=0

      if j>1:
         p=p+0.01

      j=j+1
```

```
k=k1

v1=h1+(t+o*n1)+k*p
v2=h2+(t+o*n1)+k*p
v3=h3+(t+o*n1)+k*p
v4=h4+(t+o*n1)+k*p

if v1>0:
  x1='A'
  pA=F1
  pB=0
if v1<0:
  x1='B'
  pB=F1
  pA=0

if v2>0:
  x2='A'
  pA=pA+(F2-F1)
if v2<0:
  x2='B'
  pB=pB+(F2-F1)

if v3>0:
  x3='A'
  pA=pA+(F3-F2)
if v3<0:
  x3='B'
  pB=pB+(F3-F2)

if v4>0:
  x4='A'
  pA=pA+(F4-F3)
if v4<0:
  x4='B'
  pB=pB+(F4-F3)

p1=pA

if (abs(p1-p)<0.001 or p>1 ):
      print('kappa=',k1,'equilibrium',p1,p)
      break

j=1

if i==2:

  while True:
    if j==1:
       p=0

    if j>1:
       p=p+0.01

    j=j+1

    k=k2

    v1=h1+(t+o*n1)+k*p
    v2=h2+(t+o*n1)+k*p
    v3=h3+(t+o*n1)+k*p
    v4=h4+(t+o*n1)+k*p

    if v1>0:
      x1='A'
      pA=F1
      pB=0
    if v1<0:
      x1='B'
      pB=F1
      pA=0

    if v2>0:
      x2='A'
      pA=pA+(F2-F1)
    if v2<0:
      x2='B'
      pB=pB+(F2-F1)

    if v3>0:
            x3='A'
            pA=pA+(F3-F2)
        if v3<0:
            x3='B'
            pB=pB+(F3-F2)

        if v4>0:
            x4='A'
            pA=pA+(F4-F3)
        if v4<0:
            x4='B'
            pB=pB+(F4-F3)

        p2=pA

        if (abs(p2-p)<0.001 or p>1 ):

            print('kappa=',k2,'equilibrium',p2,p)
            break

j=1

if i==3:

    while True:
        if j==1:
              p=0

        if j>1:
              p=p+0.01

        j=j+1

        k=k3

        v1=h1+(t+o*n1)+k*p
        v2=h2+(t+o*n1)+k*p
        v3=h3+(t+o*n1)+k*p
        v4=h4+(t+o*n1)+k*p

        if v1>0:
```

```
        x1='A'
        pA=F1
        pB=0
      if v1<0:
        x1='B'
        pB=F1
        pA=0

      if v2>0:
        x2='A'
        pA=pA+(F2-F1)
      if v2<0:
        x2='B'
        pB=pB+(F2-F1)

      if v3>0:
        x3='A'
        pA=pA+(F3-F2)
      if v3<0:
        x3='B'
        pB=pB+(F3-F2)

      if v4>0:
        x4='A'
        pA=pA+(F4-F3)
      if v4<0:
        x4='B'
        pB=pB+(F4-F3)

      p3=pA

      if (abs(p3-p)<0.001 or p>1 ):

        print('kappa=',k3,'equilibrium',p3,p)
        break
```

A.3 Graph of $\phi(\tau)$

```
import matplotlib.pyplot as plt
import numpy as np
```

```
h1=–1
h2=−0.5
h3=0.5
h4=1

F1=0.6
F2=0.7
F3=0.8
F4=1

# t=1
k=0.1
n1=−0.1
o=1.5

p=0.4


t1=0
t2=0.63
t3=1.11

for i in range(1,4):
    j=0

    if i==1:

        while True:
            if j==1:
                p=0

            if j>1:
                p=p+0.01

            j=j+1

              t= t1

            v1=h1+(t+o∗n1)+k∗p
```

```
v2=h2+(t+o*n1)+k*p
v3=h3+(t+o*n1)+k*p
v4=h4+(t+o*n1)+k*p

if v1>0:
   x1='A'
   pA=F1
   pB=0
if v1<0:
   x1='B'
   pB=F1
   pA=0

if v2>0:
   x2='A'
   pA=pA+(F2-F1)
if v2<0:
   x2='B'
   pB=pB+(F2-F1)

if v3>0:
   x3='A'
   pA=pA+(F3-F2)
if v3<0:
   x3='B'
   pB=pB+(F3-F2)

if v4>0:
   x4='A'
   pA=pA+(F4-F3)
if v4<0:
   x4='B'
   pB=pB+(F4-F3)

p1=pA

if (abs(p1-p)<0.001 or p>1 ):

   print('tau=', t1,'equilibrium',p1,p)
   break
```

```
j=1

if i==2:

    while True:
        if j==1:
            p=0

        if j>1:
            p=p+0.01

        j=j+1

          t= t2

        v1=h1+(t+o*n1)+k*p
        v2=h2+(t+o*n1)+k*p
        v3=h3+(t+o*n1)+k*p
        v4=h4+(t+o*n1)+k*p

        if v1>0:
            x1='A'
            pA=F1
            pB=0
        if v1<0:
            x1='B'
            pB=F1
            pA=0

        if v2>0:
            x2='A'
            pA=pA+(F2-F1)
        if v2<0:
            x2='B'
            pB=pB+(F2-F1)

        if v3>0:
            x3='A'
            pA=pA+(F3-F2)
        if v3<0:
            x3='B'
            pB=pB+(F3-F2)

        if v4>0:
            x4='A'
            pA=pA+(F4-F3)
        if v4<0:
            x4='B'
            pB=pB+(F4-F3)

        p2=pA

        if (abs(p2-p)<0.001 or p>1 ):

            print('tau=', t2,'equilibrium ',p2,p)
            break

j=1

if i==3:

    while True:
        if j==1:
              p=0

        if j>1:
              p=p+0.01

        j=j+1

          t= t3

        v1=h1+(t+o*n1)+k*p
        v2=h2+(t+o*n1)+k*p
        v3=h3+(t+o*n1)+k*p
        v4=h4+(t+o*n1)+k*p

        if v1>0:
            x1='A'
            pA=F1
            pB=0
        if v1<0:
```

```
        x1='B'
        pB=F1
        pA=0

    if v2>0:
        x2='A'
        pA=pA+(F2-F1)
    if v2<0:
        x2='B'
        pB=pB+(F2-F1)

    if v3>0:
        x3='A'
        pA=pA+(F3-F2)
    if v3<0:
        x3='B'
        pB=pB+(F3-F2)

    if v4>0:
        x4='A'
        pA=pA+(F4-F3)
    if v4<0:
        x4='B'
        pB=pB+(F4-F3)

    p3=pA

    if (abs(p3-p)<0.001 or p>1 ):

        print('tau=', t3,'equilibrium ',p3,p)
        break
```

Appendix B

Hyperledger Fabric

B.1 Introduction

As mentioned above, current permissionless blockchain technologies are not able to match the performance requirements required for many business use-cases. For enterprise use, according to Hyperledger (2018)(https://www.hyperledger.org/) the following requirements should be considered :

- Participants must be identified/identifiable
- Networks need to be permissioned
- High transaction throughput performance
- Low latency of transaction confirmation
- Privacy and confidentiality of transactions and data pertaining to business transactions

It is a open source permissioned blockchain platform designed by the Linux Foundation. Its features can be configured in several way in order to address different use-cases and industries. Differently from the other blockchain protocols that are based on a order-execute architecture, Hyperledger Fabric approach is called execute-order-validate. According to Hyperledger (2018) this new architecture divides the transaction flow into three phases:

- execute a transaction and check its correctness, thereby endorsing it,
- order transactions via a (pluggable) consensus protocol, and
- validate transactions against an application-specific endorsement policy before committing them to the ledger

Another feature introduced by this open-platform is the absence of a native cryptocurrency, but several asset can be established.

The main functionalities delivered by this blockchain platform are:

- Identity management
- Privacy and confidentiality
- Efficient processing
- Chaincode functionality
- Modular design

Concerning identity management, Hyperledger Fabric has implemented a membership identity service that verifies and authenticates all user IDs that participate to the network. Identity management allows to assign different permissions and authorizations of specific network operations to different users. In a permissioned network trust among entities is a crucial feature.

In the Hyperledger Fabric, different competing businesses could coexist in the same permissioned network. This platform enables the establishment of private channels that are restricted messaging paths shared among specific subset of network members. These channels allow to communicate with private and confidential transactions that are not visible and accessible for any other members of the network.

Hyperledger Fabric architecture follows a new approach called execute-order-validate, where different node types are in charge of different network roles. Transaction validation is separated from transaction ordering and execution. This way of dividing the operations in the transaction flow allows to provide parallelism and concurrency into the blockchain operations, increasing processing efficiency. The division of labor speeds up the processing required for authentication and authorization; all ordering peers do not need to trust all peer nodes and vice versa.

Chaincode is the name assigned to Hyperledger Fabric smart contract. It is invoked by the client application for executing a specific type of transaction. It is the only tool that interacts with the ledger in reading or writing tasks.

Hyperledger fabric provides a modular architecture in such a way as to allow the network designer to customize it and adapt it to the organization use-case. This blockchain can plug several algorithms for identity, encryption and consensus.

The two main features of Hyperledger fabric that enables to speed up operations while preserving data security are the Blockchain ledger and the different types of nodes.

B.2 Blockchain Ledger

The blockchain ledger implemented by Hyperledger Fabric consists of two distinct parts: a blockchain and a world state.

The world state is a database that holds the current values of the network. It is useful for the platform to check the current value without calculating it by go through the entire blockchain. The blockchain communicates with the database for update its current state as a transaction is executed, validated and ordered. Every added transaction determine a change in the world state.

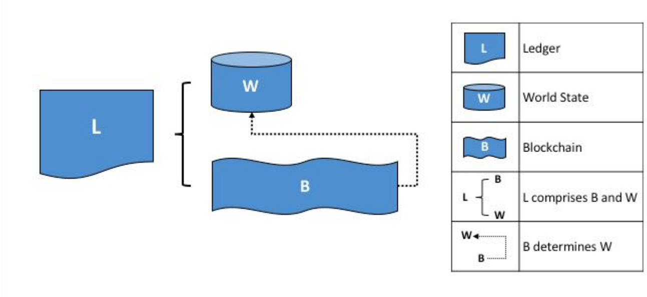


Figure B.1. Hyperledger Fabric Blockchain Ledger [47]

The way of storing transactions and data enables to take advantage of the speed and efficiency of a database and the security and transparency of the blockchain.

B.3 Peers

Hyperledger Fabric, as aforementioned, have a execute-order-validate approach; specific network operations are executed by different peer types.

The different types of peer node present in this blockchain network are:

- Endorser Peer
- Anchor Peer
- Orderer Peer
- Normal Peer

The Hyperledger Fabric workflow is composed by three phases. In the first phase, endorser peers are accountable for the execution of two tasks. First, they control that a transaction follow the endorsement policy and certificate details and roles of the requester. Second, they execute the chaincode, but they are not in charge of update the ledger. At the end of this operations the endorsers can approve or disapprove the transaction.

In the second phase orderer peer, differently from the endorsers, does not execute chaincode. They receive transactions from many applications and then they order them and package them into blocks. The created blocks will be sent to the Anchor peer that, it is configured when a channel is established. There should be at least one anchor peer for channel; usually there are one for each company that join the channel.

Lastly, in the third phase anchor peers are in charge of receiving updates from orderer peer and, if validated, broadcast the updates to the general peers. Every transaction within a block is authenticate and validate to ensure that it has been consistently endorsed by the network involved in the transaction.

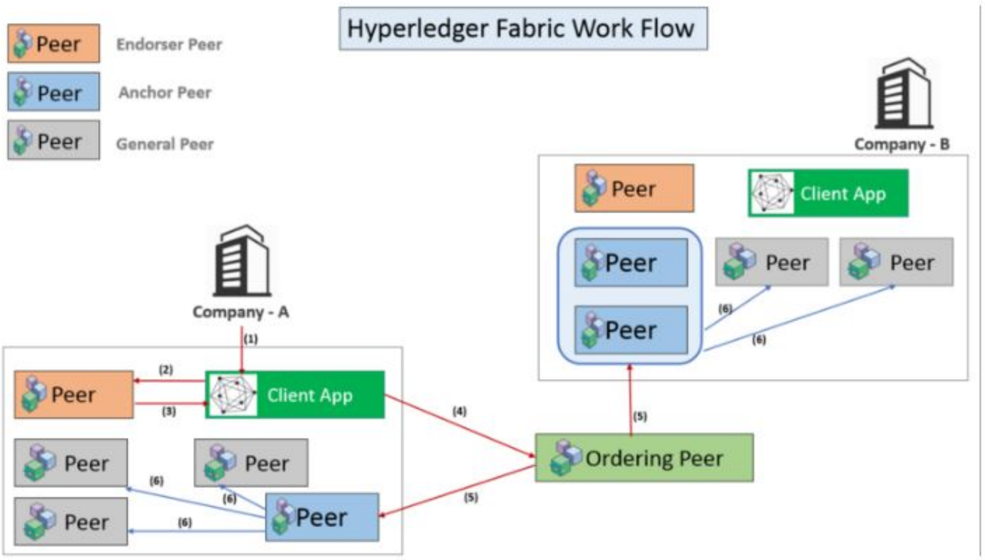


Figure B.2. Hyperledger Fabric workload [47]

This way of validate, broadcast and execute a transaction, done by different peers, allows to increase process efficiency respect other blockchain without a sizeable decrease of the level of security and privacy.

Appendix C

Economic impact of IBM blockchain implementation

This section is aimed of attempting to figure out the economic impact that IBM blockchain solution could have in a enterprise. This analysis have the purpose to examine and study the potential revenues, savings and costs that organizations may face by implementing a distributed ledger technology solution. Blockchain-based network, due to "its ability to support multiparty collaboration around shared, trusted data and process automation across organizational boundaries, brings benefits at many levels, starting with efficiency gains and culminating in reinventing how entire industry ecosystems operate" (Forrester 2018). So blockchain initiatives can be divided into two main categories:

- Establishing new business model
- Bringing efficiency in existing process flow

With respect to the opening of a new business model, most of this initiatives have not been rolled out yet. Nevertheless it can be seen how it establishes new markets or how it enables to rethink how different entities, as public authorities, corporations and business, interact and share data without compromising commercial confidentially and privacy. Enhancing transparency in process lead also to minimizing fraud risks.

With respect to the improvement of actual process flows, Blockchain-based network is a suitable solution in process that involves a waste of resources and time for the reconciliation of data among multiple parties; circumstances where there are fraud risks; and situations where efficiency and benefits can be achieved by increasing the transparency and visibility across an entire value or supply chain.

Obviously, as all digital revolution, blockchain initiatives need a long term strategic approach. It takes time for this technology to change the way of doing business, also putting at risk institutional figures and intermediaries who have always played an important role in the existing business model. Blockchain "business aspects are often a greater challenge than those posed by technology" (Forrester 2018).

The financial model framework is divided in benefits and costs. The benefits are subdivided in new revenues opportunity and solve existing pain points. Conversely, costs are categorized in pilot phase, commercialization phase and ongoing operation phase. The analysis takes into consideration risk factors, impact risk and implementation risk. Impact risks refer to the risk that the needs of an organization are not meet by the investment. Implementation risks refer to the risk that an investment could deviate from the original evaluation, leading to higher costs. The greater the risk, and so the uncertainty, the wider the possible range of outcomes for potential benefit evaluation or cost estimation. According to Forrester (2018), for benefits calculation, the risk is incorporated in the analysis by developing a wide range of projected outcomes: low, middle and high projection. The risk assessment is based on data acquired from IBM customer interviews. Organizations typically use discount rates between 8% and 16%[50]. Conversely, in the cost calculation, the assessment is less risky because IBM can accurately estimate the cost incurred in the different phases.

C.1 Benefits

Benefits are grouped in new revenues opportunity and solve existing pain point. Then new revenues opportunity are subdivided in membership revenue and transaction revenue. Instead, solve existing pain point is divided in cost avoidance and savings and efficiency

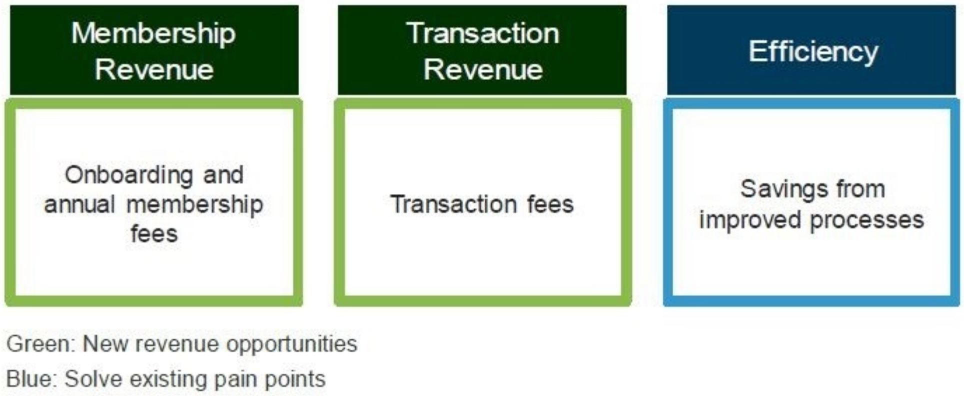

Membership Revenue
Transaction Revenue
Efficiency
Onboarding and annual membership fees
Transaction fees
Savings from improved processes
Green: New revenue opportunities
Blue: Solve existing pain points

Figure C.1. Framework For Projecting Benefits Associated With IBM Blockchain [50]

C.1.1 Membership Revenue

According to Forrester(2018) the factors that influence the magnitude of this benefit are:

- Number of new members onboarded onto the platform annually.
- Onboarding fee for new members.
- Annual membership fee.
- Annual membership churn.

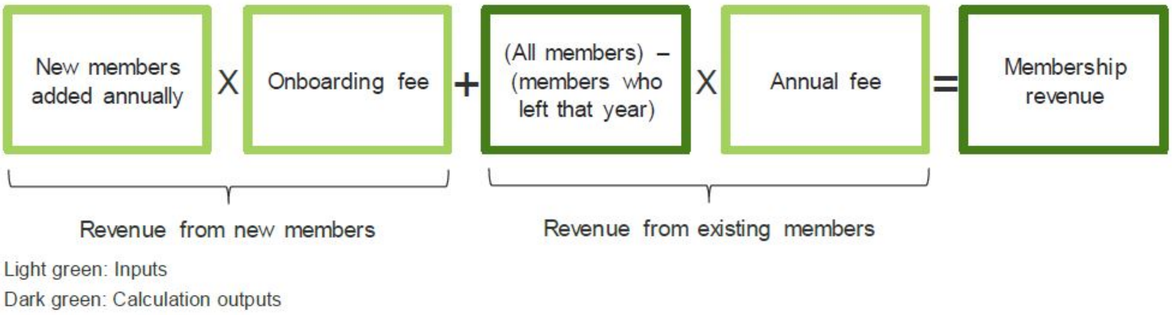
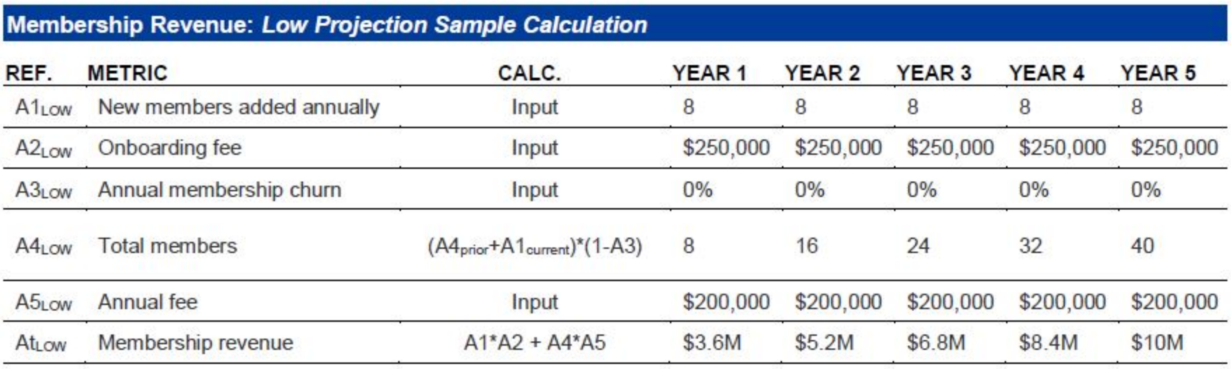

New members added annually
X
Onboarding fee
+
(All members) – (members who left that year)
X
Annual fee
=
Membership revenue
Revenue from new members
Revenue from existing members
Light green: Inputs
Dark green: Calculation outputs

Figure C.2. Membership Revenue Calculation [50]

The membership revenue calculation has been done by taking into account the three different projected outcomes. The differences between the three are in terms of new members added annually, onboarding fee and annual fee.

PROJECTION OUTCOME			
	LOW	MIDDLE	HIGH
New members added annually	8	12	16
Onboarding fee	$ 250,000	$ 300,000	$ 350,000
Annual fee	$ 200,000	$ 250,000	$ 300,000

The calculations for the low projection of membership revenues are the following:

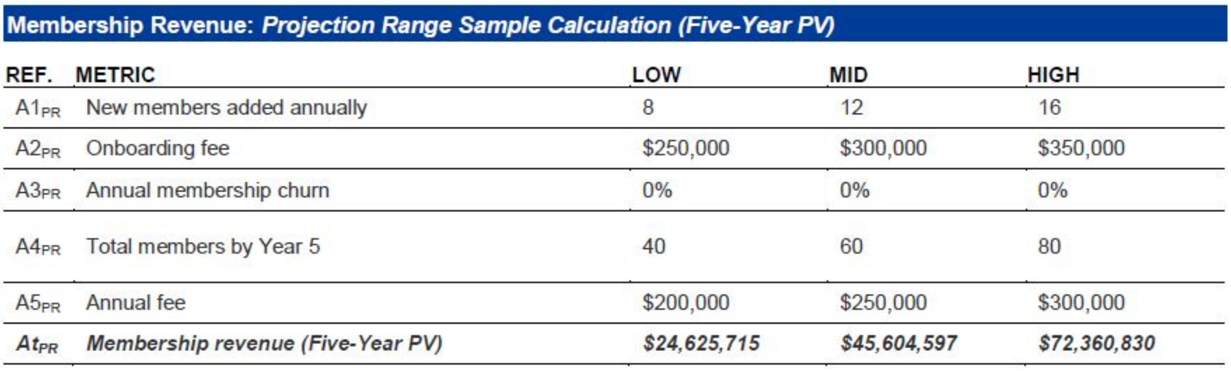


Membership Revenue: *Low Projection Sample Calculation*

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5
$A1_{LOW}$	New members added annually	Input	8	8	8	8	8
$A2_{LOW}$	Onboarding fee	Input	$250,000	$250,000	$250,000	$250,000	$250,000
$A3_{LOW}$	Annual membership churn	Input	0%	0%	0%	0%	0%
$A4_{LOW}$	Total members	$(A4_{prior}+A1_{current})*(1-A3)$	8	16	24	32	40
$A5_{LOW}$	Annual fee	Input	$200,000	$200,000	$200,000	$200,000	$200,000
At_{LOW}	Membership revenue	A1*A2 + A4*A5	$3.6M	$5.2M	$6.8M	$8.4M	$10M

Figure C.3. Membership Revenue: Low Projection Sample Calculation [50]

The Present Value(PV) of the three projection are:



Membership Revenue: *Projection Range Sample Calculation (Five-Year PV)*

REF.	METRIC	LOW	MID	HIGH
$A1_{PR}$	New members added annually	8	12	16
$A2_{PR}$	Onboarding fee	$250,000	$300,000	$350,000
$A3_{PR}$	Annual membership churn	0%	0%	0%
$A4_{PR}$	Total members by Year 5	40	60	80
$A5_{PR}$	Annual fee	$200,000	$250,000	$300,000
At_{PR}	***Membership revenue (Five-Year PV)***	***$24,625,715***	***$45,604,597***	***$72,360,830***

Figure C.4. Membership Revenue: Projection Range Sample Calculation (Five-Year PV) [50]

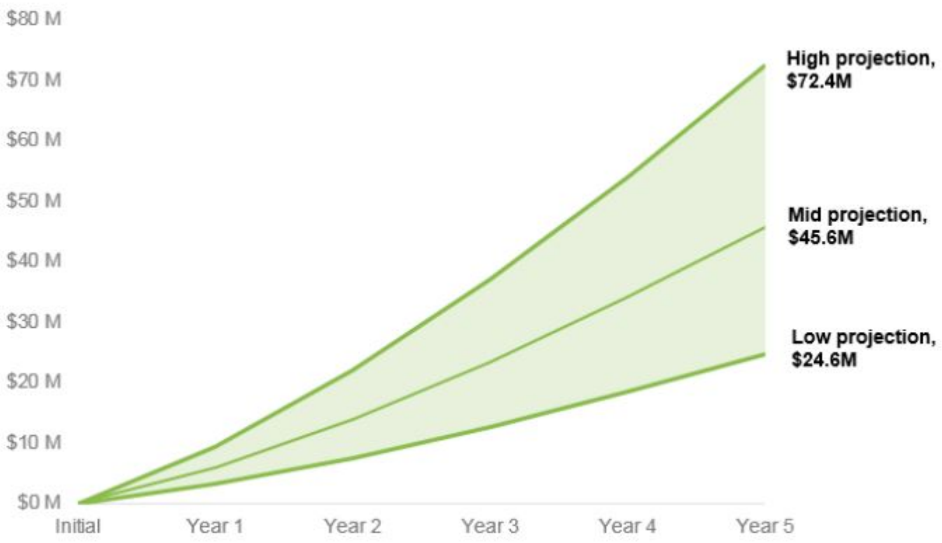


Figure C.5. Membership Benefit Module: Range Of 5-Years Cumulative Impact[50]

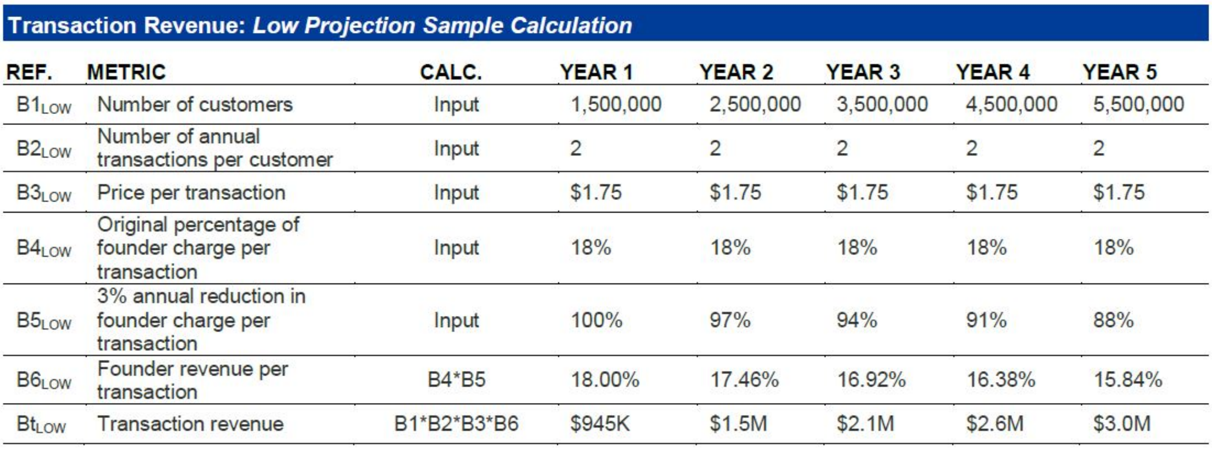
So according to Forrester(2018), the revenue generated due to membership benefit thanks blockchain implementation after 5 years is in the range from $24,6M to $72.4M.

C.1.2 Transaction Revenue

According to Forrester (2018) the factors that influence the magnitude of this benefit are:

- Number of customers using the blockchain platform annually.
- Number of transactions completed by each customer per year.
- Price per transaction.
- Percentage charged per transaction.
- Change in percentage of transaction price charged by blockchain founder as customer base grows.

For the calculations of the low projection of transaction revenues, Forrester(2018) has taken into account the parameters present in the graph below:

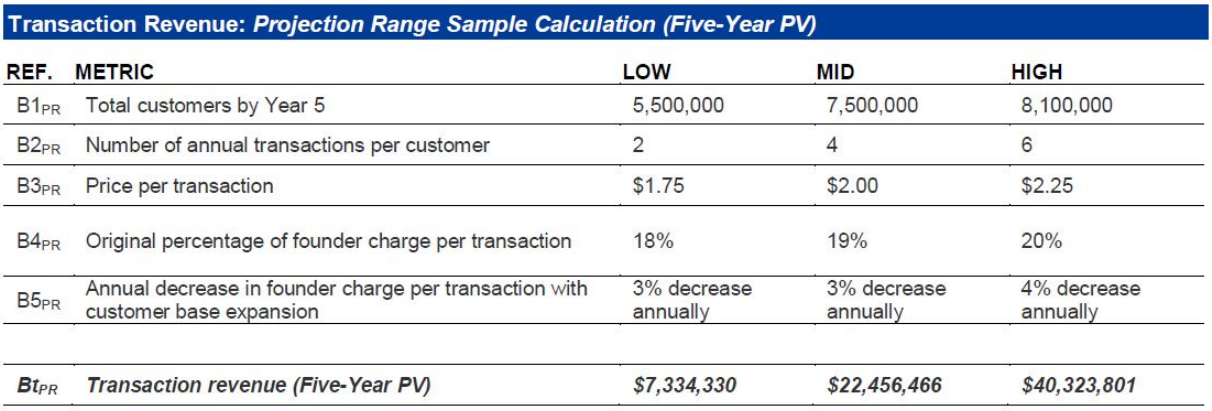


Transaction Revenue: *Low Projection Sample Calculation*

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5
$B1_{LOW}$	Number of customers	Input	1,500,000	2,500,000	3,500,000	4,500,000	5,500,000
$B2_{LOW}$	Number of annual transactions per customer	Input	2	2	2	2	2
$B3_{LOW}$	Price per transaction	Input	$1.75	$1.75	$1.75	$1.75	$1.75
$B4_{LOW}$	Original percentage of founder charge per transaction	Input	18%	18%	18%	18%	18%
$B5_{LOW}$	3% annual reduction in founder charge per transaction	Input	100%	97%	94%	91%	88%
$B6_{LOW}$	Founder revenue per transaction	B4*B5	18.00%	17.46%	16.92%	16.38%	15.84%
Bt_{LOW}	Transaction revenue	B1*B2*B3*B6	$945K	$1.5M	$2.1M	$2.6M	$3.0M

Figure C.6. Transaction Revenue: Low Projection Sample Calculation[50]

As the membership revenue calculation, transaction revenue calculation has been done by taking into account the three different projected outcomes. The three evaluations differ in term of: number of customers, number of annual transactions per customer, price per transaction, percentage of annual reduction in founder charge per transaction. So the Present Value(PV) estimated of the three projection are:



Transaction Revenue: *Projection Range Sample Calculation (Five-Year PV)*

REF.	METRIC	LOW	MID	HIGH
$B1_{PR}$	Total customers by Year 5	5,500,000	7,500,000	8,100,000
$B2_{PR}$	Number of annual transactions per customer	2	4	6
$B3_{PR}$	Price per transaction	$1.75	$2.00	$2.25
$B4_{PR}$	Original percentage of founder charge per transaction	18%	19%	20%
$B5_{PR}$	Annual decrease in founder charge per transaction with customer base expansion	3% decrease annually	3% decrease annually	4% decrease annually
Bt_{PR}	***Transaction revenue (Five-Year PV)***	***$7,334,330***	***$22,456,466***	***$40,323,801***

Figure C.7. Transaction Revenue: Projection Range Sample Calculation (Five-Year PV)[50]

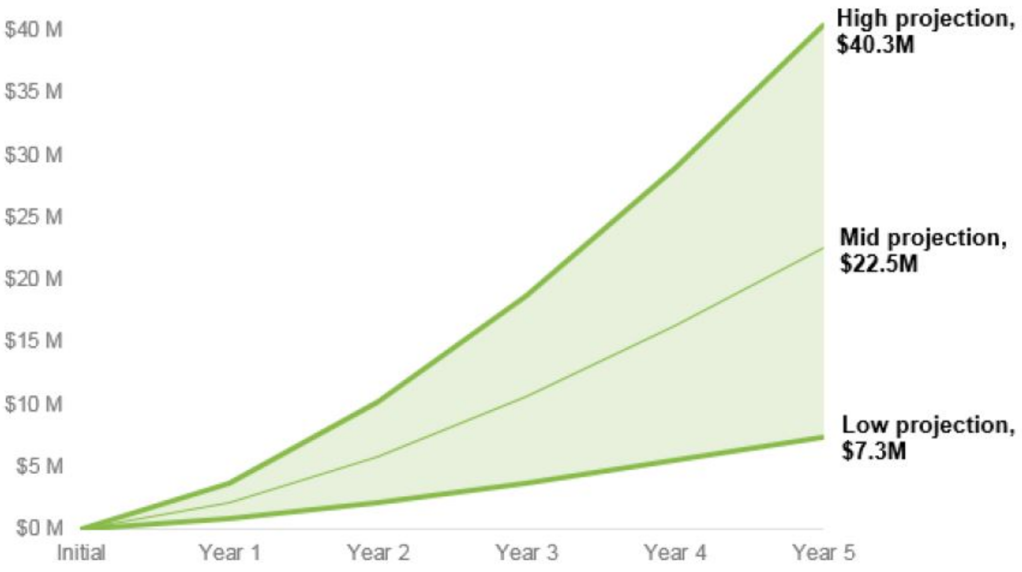


Figure C.8. Transaction Benefit Module: Range Of 5-Years Cumulative Impact[50]

So according to Forrester (2018), the revenue generated due to transaction benefit thanks blockchain implementation after 5 years is in the range from $7.3M to $40.3M.

C.1.3 Efficiency Savings

According to Forrester (2018) the implementation of a blockchain-based solution includes streamlined billing and documentation, eliminated disputes stemming from inconsistent documentation and replacing legacy systems; these benefits lead to a reduction of employees and redundancy processes for reconciling data among multiple parties. Forrester (2018) explored several components to measuring internal efficiency improvements:

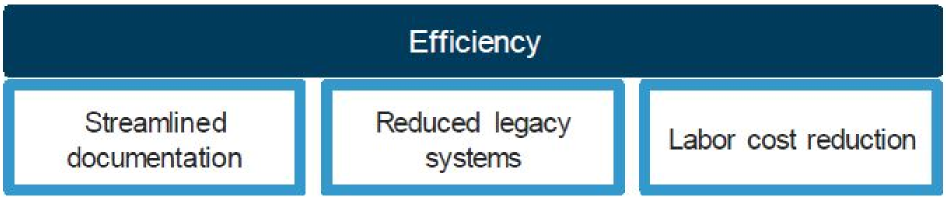


Figure C.9. Efficiency Savings Calculation[50]

As reported by Forrester(2018) the factors that influence the magnitude of this benefit are:

- Number of records (i.e., invoice, shipping document) handled by an organization, average cost to process a record, percentage of records conflicting in the customer's (and their counterpart's) systems, and average cost to resolve a dispute over a record.

- License cost of legacy systems and organization's approach to replacing them with a solution built with IBM Blockchain Platform and Services.

- Number of employees re-assigned from using a solution built with IBM Blockchain Platform and Services and their annual compensations.

On the other hand, the framework used for calculating the efficiency delivered to the organization due to a streamlined documentation is:

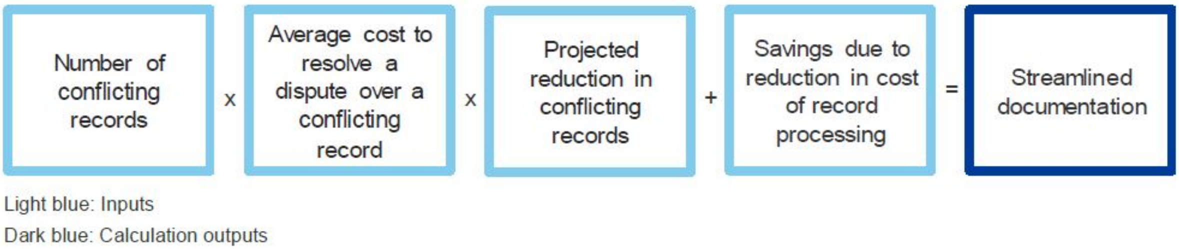
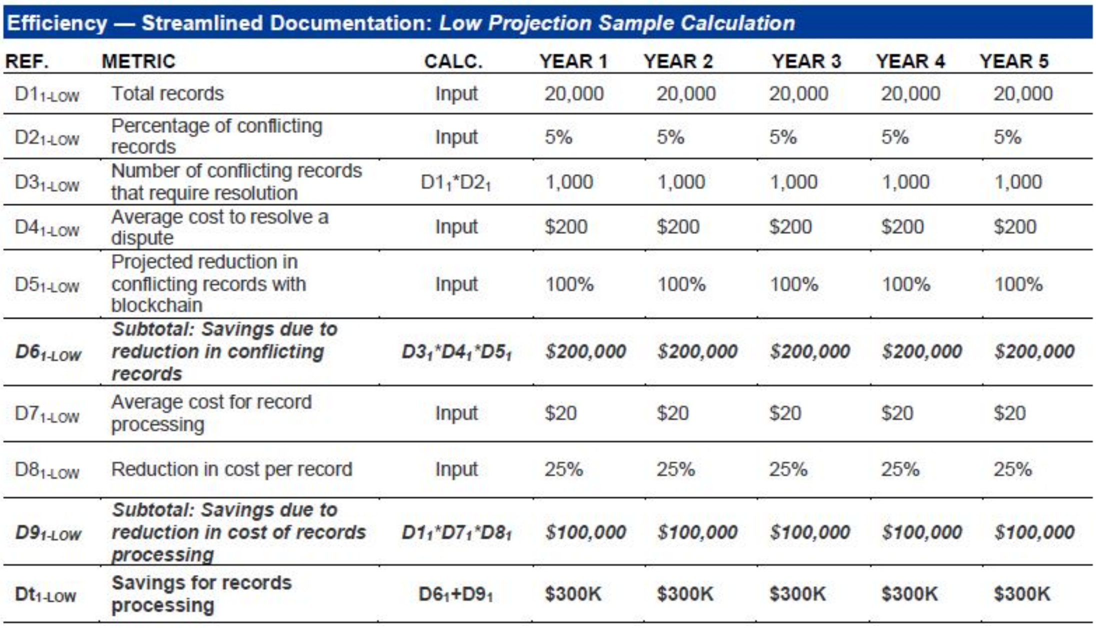

Number of conflicting records
x
Average cost to resolve a dispute over a conflicting record
x
Projected reduction in conflicting records
+
Savings due to reduction in cost of record processing
=
Streamlined documentation
Light blue: Inputs
Dark blue: Calculation outputs

Figure C.10. Efficiency-Streamlined Documentation Calculation[50]

The calculations for the low projection of efficiency improvement due to streamlined documentation are the following:

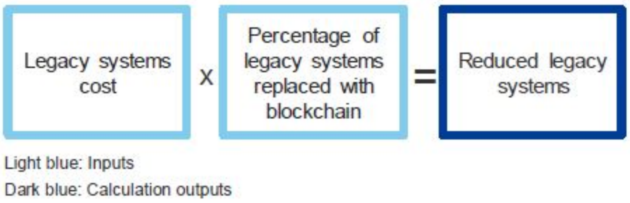


Efficiency — Streamlined Documentation: ***Low Projection Sample Calculation***

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5
$D1_{1\text{-}LOW}$	Total records	Input	20,000	20,000	20,000	20,000	20,000
$D2_{1\text{-}LOW}$	Percentage of conflicting records	Input	5%	5%	5%	5%	5%
$D3_{1\text{-}LOW}$	Number of conflicting records that require resolution	$D1_1{*}D2_1$	1,000	1,000	1,000	1,000	1,000
$D4_{1\text{-}LOW}$	Average cost to resolve a dispute	Input	\$200	\$200	\$200	\$200	\$200
$D5_{1\text{-}LOW}$	Projected reduction in conflicting records with blockchain	Input	100%	100%	100%	100%	100%
$D6_{1\text{-}LOW}$	***Subtotal: Savings due to reduction in conflicting records***	***$D3_1{*}D4_1{*}D5_1$***	***\$200,000***	***\$200,000***	***\$200,000***	***\$200,000***	***\$200,000***
$D7_{1\text{-}LOW}$	Average cost for record processing	Input	\$20	\$20	\$20	\$20	\$20
$D8_{1\text{-}LOW}$	Reduction in cost per record	Input	25%	25%	25%	25%	25%
$D9_{1\text{-}LOW}$	***Subtotal: Savings due to reduction in cost of records processing***	***$D1_1{*}D7_1{*}D8_1$***	***\$100,000***	***\$100,000***	***\$100,000***	***\$100,000***	***\$100,000***
$Dt_{1\text{-}LOW}$	**Savings for records processing**	**$D6_1{+}D9_1$**	**\$300K**	**\$300K**	**\$300K**	**\$300K**	**\$300K**

Figure C.11. Efficiency-Streamlined Documentation: Low Projection Sample Calculation[50]

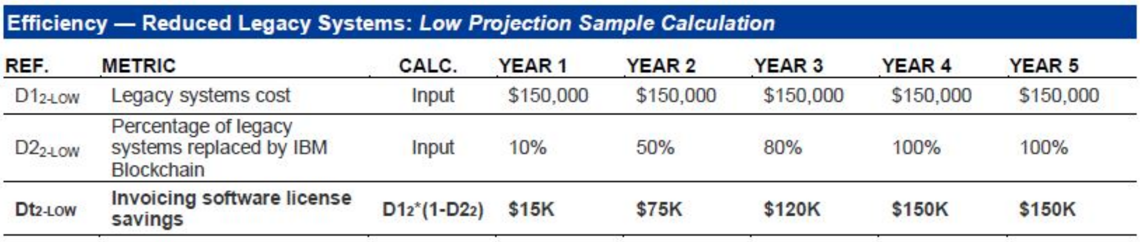
Finally, the framework used for calculating the efficiency delivered to the organization due to a reduction in the legacy system is:



Light blue: Inputs
Dark blue: Calculation outputs

Figure C.12. Efficiency-Reduced legacy systems Calculation[50]

The calculations for the low projection of efficiency improvement due to the reduction of legacy systems are the following:



Efficiency — Reduced Legacy Systems: ***Low Projection Sample Calculation***

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5
$D1_{2\text{-LOW}}$	Legacy systems cost	Input	$150,000	$150,000	$150,000	$150,000	$150,000
$D2_{2\text{-LOW}}$	Percentage of legacy systems replaced by IBM Blockchain	Input	10%	50%	80%	100%	100%
$Dt_{2\text{-LOW}}$	**Invoicing software license savings**	**$D1_{2}$*(1-$D2_{2}$)**	**$15K**	**$75K**	**$120K**	**$150K**	**$150K**

Figure C.13. Efficiency-Reduced Legacy Systems: Low Projection Sample Calculation[50]

The framework used for calculating the efficiency delivered to the organization due to a labor cost reduction is:

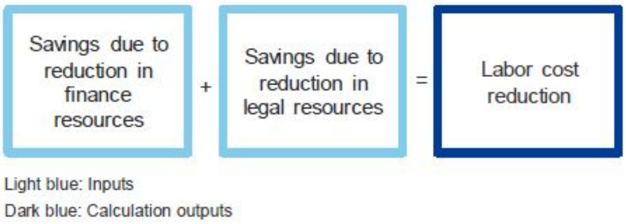
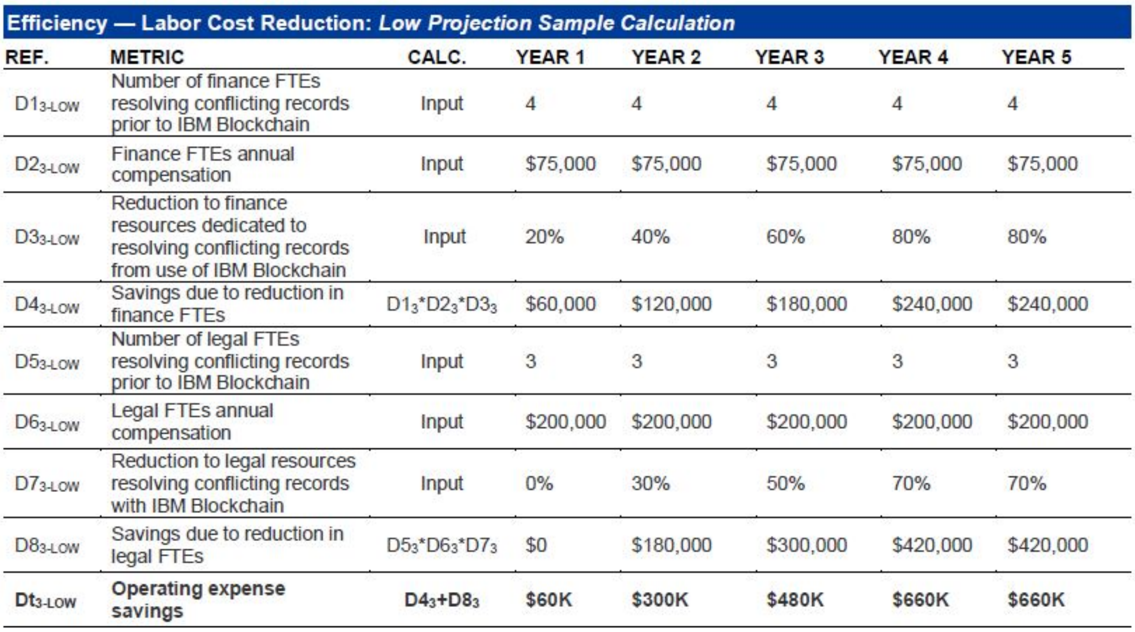

Savings due to reduction in finance resources
+
Savings due to reduction in legal resources
=
Labor cost reduction
Light blue: Inputs
Dark blue: Calculation outputs

Figure C.14. Efficiency-Labor Cost Reduction Calculation[50]

The calculations for the low projection of efficiency improvement due to the reduction of labor cost are the following:

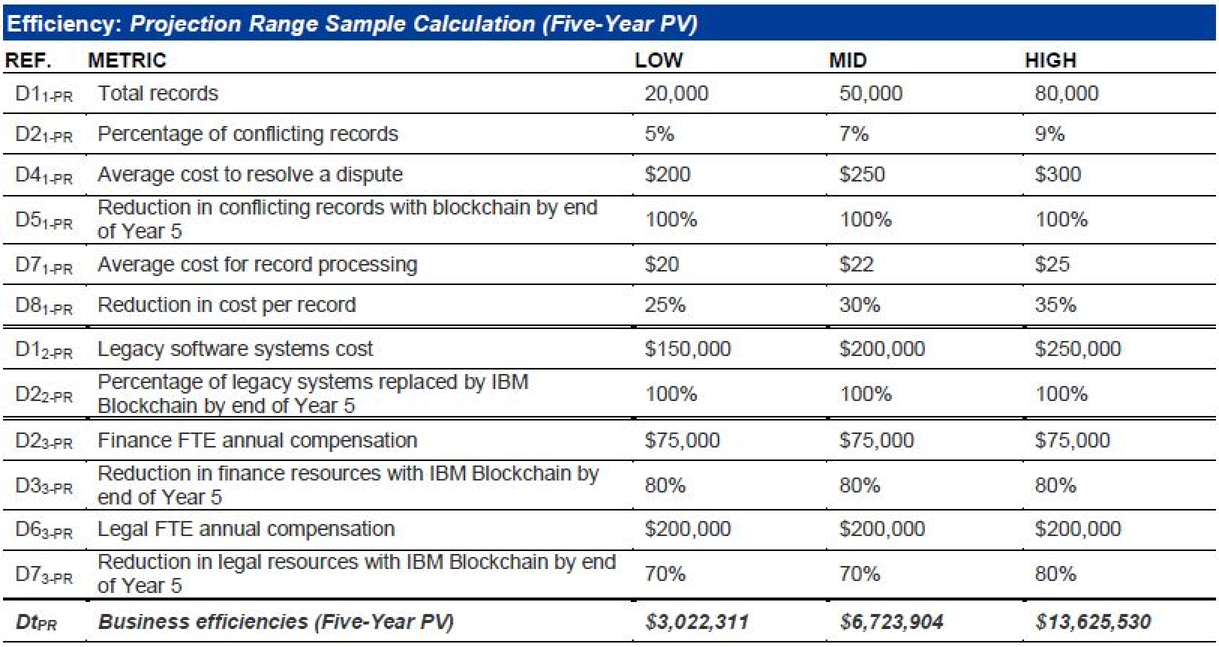


Efficiency — Labor Cost Reduction: *Low Projection Sample Calculation*

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5
$D1_{3\text{-LOW}}$	Number of finance FTEs resolving conflicting records prior to IBM Blockchain	Input	4	4	4	4	4
$D2_{3\text{-LOW}}$	Finance FTEs annual compensation	Input	$75,000	$75,000	$75,000	$75,000	$75,000
$D3_{3\text{-LOW}}$	Reduction to finance resources dedicated to resolving conflicting records from use of IBM Blockchain	Input	20%	40%	60%	80%	80%
$D4_{3\text{-LOW}}$	Savings due to reduction in finance FTEs	$D1_3*D2_3*D3_3$	$60,000	$120,000	$180,000	$240,000	$240,000
$D5_{3\text{-LOW}}$	Number of legal FTEs resolving conflicting records prior to IBM Blockchain	Input	3	3	3	3	3
$D6_{3\text{-LOW}}$	Legal FTEs annual compensation	Input	$200,000	$200,000	$200,000	$200,000	$200,000
$D7_{3\text{-LOW}}$	Reduction to legal resources resolving conflicting records with IBM Blockchain	Input	0%	30%	50%	70%	70%
$D8_{3\text{-LOW}}$	Savings due to reduction in legal FTEs	$D5_3*D6_3*D7_3$	$0	$180,000	$300,000	$420,000	$420,000
$Dt_{3\text{-LOW}}$	**Operating expense savings**	**$D4_3+D8_3$**	**$60K**	**$300K**	**$480K**	**$660K**	**$660K**

Figure C.15. Efficiency-Labor Cost Reduction: Low Projection Sample Calculation[50]

The efficiency calculation has been done by taking into account the three different projected outcomes. So the Present Value(PV) estimated of the three projection are:



Efficiency: *Projection Range Sample Calculation (Five-Year PV)*

REF.	METRIC	LOW	MID	HIGH
$D1_{1-PR}$	Total records	20,000	50,000	80,000
$D2_{1-PR}$	Percentage of conflicting records	5%	7%	9%
$D4_{1-PR}$	Average cost to resolve a dispute	$200	$250	$300
$D5_{1-PR}$	Reduction in conflicting records with blockchain by end of Year 5	100%	100%	100%
$D7_{1-PR}$	Average cost for record processing	$20	$22	$25
$D8_{1-PR}$	Reduction in cost per record	25%	30%	35%
$D1_{2-PR}$	Legacy software systems cost	$150,000	$200,000	$250,000
$D2_{2-PR}$	Percentage of legacy systems replaced by IBM Blockchain by end of Year 5	100%	100%	100%
$D2_{3-PR}$	Finance FTE annual compensation	$75,000	$75,000	$75,000
$D3_{3-PR}$	Reduction in finance resources with IBM Blockchain by end of Year 5	80%	80%	80%
$D6_{3-PR}$	Legal FTE annual compensation	$200,000	$200,000	$200,000
$D7_{3-PR}$	Reduction in legal resources with IBM Blockchain by end of Year 5	70%	70%	80%
Dt_{PR}	***Business efficiencies (Five-Year PV)***	***$3,022,311***	***$6,723,904***	***$13,625,530***

Figure C.16. Efficiency savings: Projection Range Sample Calculation (Five-Year PV)[50]

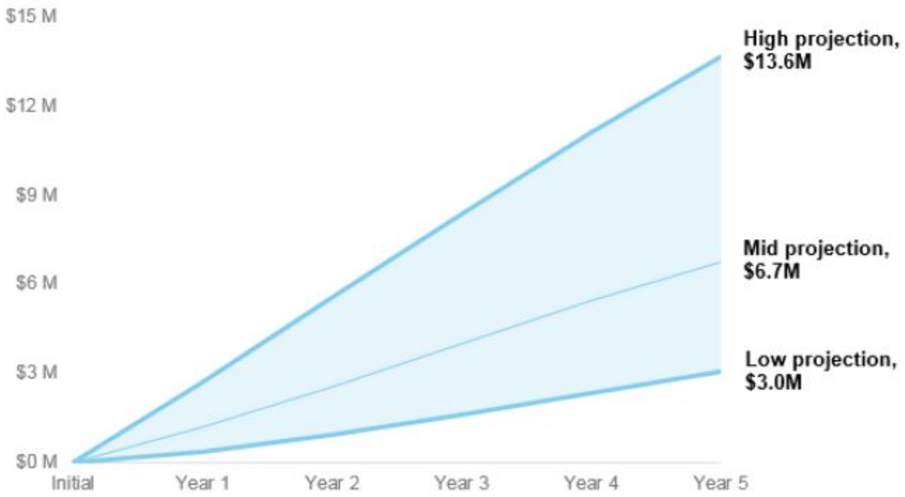


Figure C.17. Efficiency Benefit Module: Range Of 5-Years Cumulative Impact[50]

So according to Forrester(2018), the efficiency delivered by blockchain implementation after 5 years is in the range from $3M to $13.6M.

C.1.4 Other potential benefits

Other potential benefits associated with blockchain implementation are related to: time-to-market(TTM) reduction, fraud avoidance and Inventory loss avoidance. Process automation and sharing data across multiple parties in blockchain network lead to enhance efficiency across the supply and value chain. Especially in fast-moving industries where products are outmoded quickly, speeding up the TTM is a crucial factor for enhancing market share capture and for revenue acceleration.

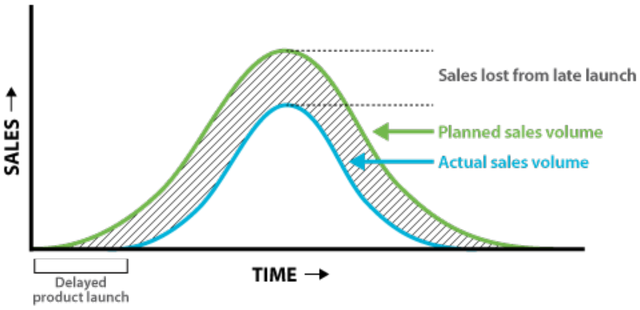


Figure C.18. Time-To-Market[74]

The tamper-resistant and distributed nature of blockchain networks has the potential to reduce fraud. According to Report To The Nations(2018) organizations lose 5% of their annual revenues to fraud, where internal control weaknesses were responsible for nearly half of frauds[75]. So, Blockchain could be a suitable solution in order to avoid fraud and by reducing investment in preventing strategies.

Inventory loss avoidance can be achieve by enhance efficiency and transparency across supply chain. Monitoring products condition in supply chain is crucial especially in food and beverage and pharmaceutical industries where during the shipment, particular temperature conditions should be respected.

These factors are very variable with respect to the industry that is taken into account. So doing a general quantitative analysis to measure the impact of blockchain considering these variables is almost impossible.

C.2 Costs

According to Forrester (2018) the costs involved in the blockchain implementation can be divided in : Pilot phase costs, commercialization cost and ongoing costs

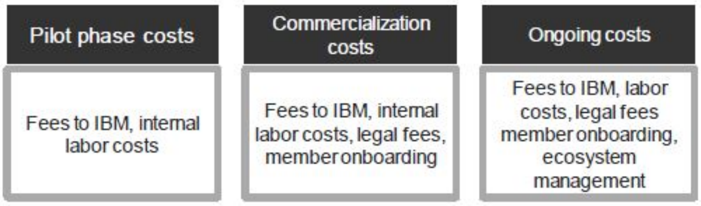

Pilot phase costs
Fees to IBM, internal labor costs
Commercialization costs
Fees to IBM, internal labor costs, legal fees, member onboarding
Ongoing costs
Fees to IBM, labor costs, legal fees member onboarding, ecosystem management

Figure C.19. costs in IBM blockchain implementation[50]

According to Forrester (2018), the pilot stage costs take into account :

- Fees to IBM
- Cost of internal IT and development resources
- Cost of internal legal and business resources

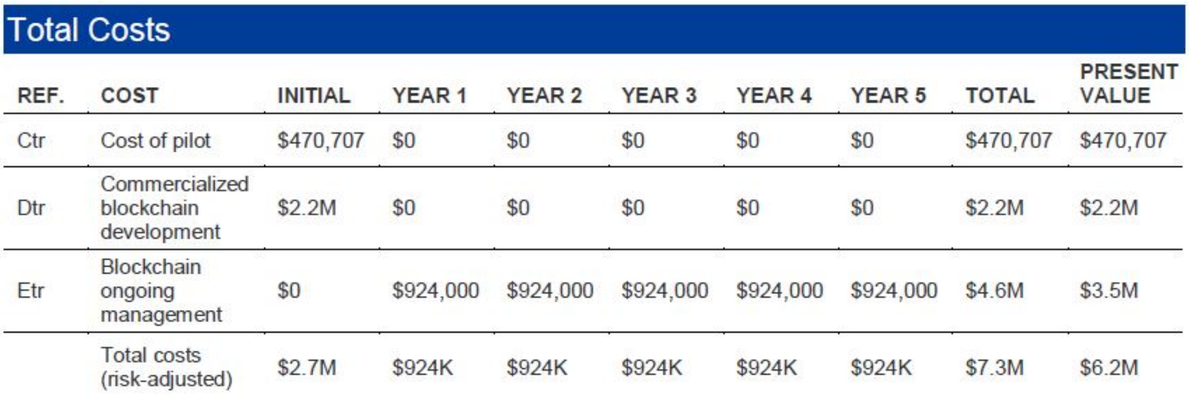
The costs can vary due to the complexity of blockchain implementation, project duration, numbers of employees involved and complexity for developing a governance model suitable with organization business model.

During the commercialization phase, further costs have to take into account. Additional development effort have to be considered in order to improve the governance model and facilitate the onbording of new members, as communication, administration and marketing costs.

Usually pilot and commecialized phase occur in the initial year when organization attempt to implement a blockchain solution suitable for its business model.

Finally in the ongoing phase, organizations keep to invest in order to maintain and growth the network, establishing new business partnership and developing an ecosystem that bring benefits to all members of the network.

Forrester have developed a quantitative model in order to estimate costs that a organization may incur.



Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5	TOTAL	PRESENT VALUE
Ctr	Cost of pilot	$470,707	$0	$0	$0	$0	$0	$470,707	$470,707
Dtr	Commercialized blockchain development	$2.2M	$0	$0	$0	$0	$0	$2.2M	$2.2M
Etr	Blockchain ongoing management	$0	$924,000	$924,000	$924,000	$924,000	$924,000	$4.6M	$3.5M
	Total costs (risk-adjusted)	$2.7M	$924K	$924K	$924K	$924K	$924K	$7.3M	$6.2M

Figure C.20. Total costs in IBM blockchain implementation[74]

Figure 42 shows the estimation of the total costs that a company may face in the implementation of the blockchain technology. In order to estimate the present value(PV) integrating a certain level of risk, Forrester(2018) has used a discount rate of 10%

For the pilot phase evaluation, the following features have been taken into account:

- This phase lasts six months.
- Organization pays fees to IBM
- The workers involved are five developers/ information technology professionals and they have worked 15% of their time for the entire pilot phase.
- A business owner and a legal professional were also involved in the development of a governance model and for negotiations for 20% of their time for the entire pilot phase.

Finally Forrester have adjusted the full calculation upward by 20% for including the risk adjustment.

For the commercial phase Forrester has assumed :

- This phase lasts 12 months
- Organization pays fees to IBM
- Five software engineering and IT professionals dedicate 15% of their time for the entire phase.

- Three business and legal professionals dedicate 20% of their time in the development of a governance model and for negotiations
- Companies spends $5,000 in communication, administration and marketing in order to facilitate the onboarding of new members
- prior of the ongoing phase, the organization has onboarded three members

Finally Forrester have adjusted the full calculation upward by 20% for including the risk adjustment.

For the ongoing phase evaluation, the following features have been taken into account:

- This phase was calculated for 5 years
- Organization pays fees to IBM
- three software engineering professionals/IT dedicate 20% of their time to the maintenance of the platform
- a legal professional is in charge of contracts and governance model and he dedicates 100% of his time.
- The company spends $200,000 per year in order to manage relationship with the blockchain members

Finally also in this phase Forrester have adjusted the full calculation upward by 20% for including the risk adjustment.