Cryptography Working Group
Introduction to Blockchain Technology

White Paper

Written by: Dr. Ramsès Fernàndez-València, Dr. Juan Caubet and Aleix Vila
Sponsored by:

eurecat
Centre Tecnològic de Catalunya

IT Security R&D Unit
Date 07/05/2018

INDEX

1. INTRODUCTION

1.1. What is a Blockchain?

A Blockchain is a distributed structure of data: there is no central authority supervising the operations made in the system and data are distributed among several entities. It is a list of blocks connected in such a way that a block is linked to its predecessor. It is quite usual to think of a Blockchain as a big ledger where each block of the Blockchain is represented by a page of the ledger. There exists several Blockchain proposals like those underlying Bitcoin (Nakamoto, 2008) or Ehtereum (Wood, 2014).

Every Blockchain is made of three basic components which are:

1. A **network of nodes**: although all nodes in the network may register transactions, it is usually split in two kinds of nodes, those who are responsible for creating new blocks and/or validating transactions and those who just register transactions.
2. A **shared ledger**: this is a kind database which is shared, replicated and synchronized among the members (nodes in our context) of a decentralized network. The ledger records transactions.
3. A **consensus algorithm**: the consensus algorithm is the mechanism accepted by all nodes in the Blockchain network as the main way to select the node responsible for adding a new node in the Blockchain.

One of the big deals of Blockchain is that it offers integrity of data: if a node wants to make any change in a unilateral way, it will be forced to modify not just the objective block, but also each of the blocks between its objective and the current block, what is an expensive operation either in terms of tokens, time or energy, depending on the consensus algorithm used by the Blockchain. Furthermore, the node will need to overcome the Blockchain itself and will have to publish the leading block.

Concerning access to data and availability to make contributions, Blockchains can be essentially divided into two categories:

1. **Permissioned**: where one finds a governing entity or entities delivering permissions allowing participants to access data or create transactions or blocks. In these kind of Blockchain a participant may be allowed to access data and generate transactions but not to create blocks. An example of permissioned Blockchain is Ripple (Schwartz, Youngs, & Britto, 2014) or Corda (Brown, Carlyle, Grigg, & Hearn, 2018).
2. **Permissionless**: in this kind of Blockchain the possibility to access data, generate transactions or create blocks is open to all participants. Permissionless Blockchains are also known as public Blockchains and these include Bitcoin or Ethereum, among many others.

1.2. How a Blockchain works

Although there exist several kinds of Blockchain proposals, they share a common functioning which is described step by step in this section, where Alice wants to pay Bob some tokens for the pizza she had in his restaurant.

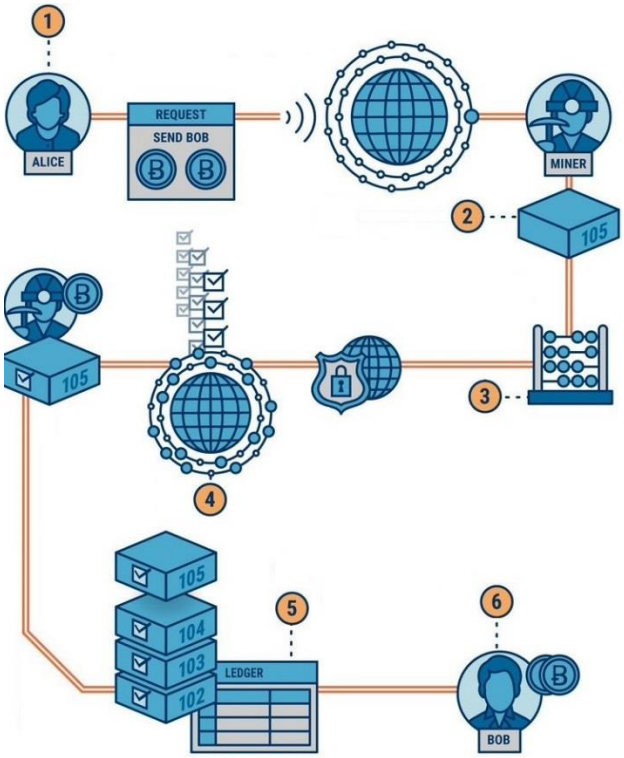

Figure 1: The basic functioning of a Blockchain (CB Insights)

1. Alice sends a transaction to the Blockchain, which ends up in the mempool, the place where all transactions made worldwide wait to be included in a block.
2. One of the nodes (let us call it M) responsible for the creation of blocks collects Alice's transaction together with some other transactions in order to create a new block.
3. Before M can include the node into the Blockchain, M needs to satisfy the requirements of the consensus algorithm. In Bitcoin, for instance, M will have to perform several computations.
4. Once the consensus requirements are satisfied, some nodes verify the answer given by M. If a majority of nodes accept the answer, the block is included into the Blockchain. M receives a compensation for the work done.
5. As the block containing Alice's transaction is accepted and added into the Blockchain, the payment is considered valid.
6. Bob gets paid for the pizza.

1.3. Structure of a block

A block is the main object of a Blockchain. It is a data structure consisting of transactions together with a link to the previous block. Although blocks in different Blockchain proposals will have different structure, they usually share the following points in common:

1. **Header**, which contains the following data:
    - **Previous Blockhash**: it is the hash of the header of the previous block.
    - **Merkle root hash**: used to verify the set of transactions in the block.
    - **Nonce**: it is a counter involved in the consensus algorithm.
    - **Version of the block**.
    - **Timestamp**: Date of creation of the block.
2. **Blockhash**: it is the hash of the header.
3. **Size of the block**.
4. **Set of transactions**.

1.4. Consensus

1.4.1. The Byzantine generals problem

The importance of Blockchain lays on the fact that it is a solution for the problem of Byzantine generals problem (Lamport, Shostak, & Pease, 1982). The problem shows a group of generals leading several divisions of the Byzantine army which have besieged a city while waiting for the sacking. Each general leads a division of the Byzantine army and every general obeys a leading general who is responsible for the whole attack. The sacking of the city will success just if all the divisions attack at the same time. As the divisions surround the city, communications with the leading general are not easy. Communications to agree the time of the nal attack between divisions must be done using messengers. Nevertheless, some of the generals are traitors and they will not obey the messages or, even worst, they will send fake messages in order to confuse the rest of generals.

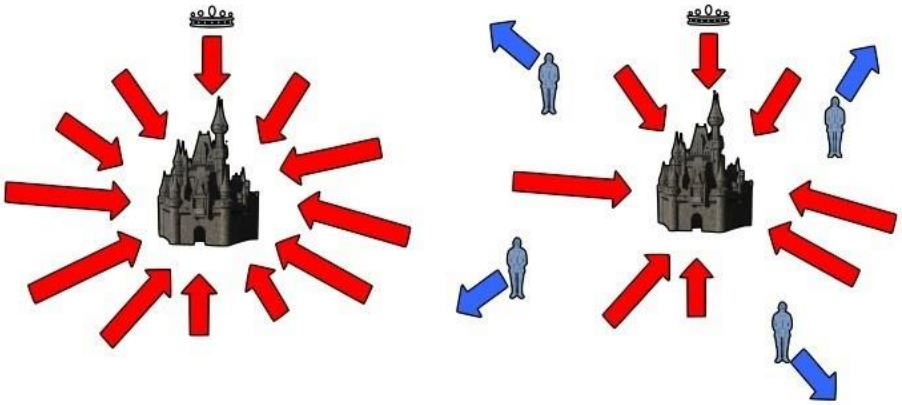

Figure 2: The attack will success if it is done at the same time (medium.com)

We can move this problem to the setting of Blockchain technology as follows: each node plays the role of a general. As it is a distributed system there is no leading general. There exists some nodes which are not faithful and which remain unknown. The time for the last attack can be understood as the moment when a block is created. How can we get a nal consensus? There exist several consensus mechanisms accepted for all the members of the system. There are algorithms requiring to solve a mathematical problem, to wait a certain amount of time or to prove that a node has certain balance. Once a node solves the problem, or satisfies a condition, the system allows it to publish a new block.

1.4.2. Proof of Work and Proof of Stake

A presentation of Proof of Work and Proof of Stake is given. These mechanisms are the main protocols through which consensus is attained in most of current Blockchain proposals.

- **Proof of Work** (PoW): This consensus mechanism requires the node wishing to publish a block to solve a mathematical problem based on hashing several times the block header until a specific condition is satisfied. The main disadvantage of PoW is that it requires a massive ammount of energy that, for many people, is wasted in a useless computation. In order to try to overcome this problem some Blockchain solutions created Reusable Proof of Work (Nakamoto Institute, 2004), where the computations required to solve the mathematical problem are related to useful situations such as computations on proteins or integer factorization.
- **Proof of Stake** (PoS): The idea behind PoS is *the more you have, the more you get*. In the PoS setting, a node is allowed to create a block in a deterministic way which points at node's wealth. Generally speaking, if a node can prove that it has a certain percentage of tokens, it will have the same percentage of chances to get the permission to create a block. Compared in terms of energy to PoW, Proof of Stake costs are negligible. Nevertheless, its main disadvantage is that it increases the di erences between poor nodes and rich nodes.

2. MAIN BLOCKCHAIN PROPOSALS

Since the creation of Bitcoin, Blockchain technology has become the focus of almost every sector in industry, nance or retail. Although many of the proposals work in a similar way, some of them show some facts that make them interesting, like Ethereum's smart contracts or IOTA's tangled structure. This section is devoted to some of the most important Blockchain technologies: we give a brief introduction together with a few wprds about about what makes the special.

2.1. Corda

Corda is a Blockchain especi cally created for the banking sector (Brown, Carlyle, Grigg, & Hearn, 2018). Calling it a Blockchain is quite daring as many of the defining properties of Blockchain technology are not satisfied in Corda, such as the concept of miner node (or equivalent). Corda is a private Blockchain, a special kind of permissioned system: a prospective member cannot check data or contribute the system unless it has the right permissions. Corda allows the use of several consensus mechanisms, none of them being the PoW mechanism. The transactions in Corda are encrypted and can only be validated by the associated nodes (sender and receiver of the transaction). One more detail: Corda does not have a cryptocurrency like Ethereum or Bitcoin.

2.2. Ethereum

Ethereum appeared for the first time in 2014 (Wood, 2014). Although there are many similiarities between Bitcoin and Etehreum, in terms of general structure, the main difference between them is that the latter allows the execution of programs under the name of smart contracts. This fact allows Ethereum to be not only the main platform of a cryptocurrency, as Bitcoin, but also a solution for many other problems.

The main points in common between both platforms are that they have a cryptocurrency (bitcoin and ether) and the existence of miner nodes. Both of them use, as for today, PoW although Ethereum started in december 2017 a shift to PoS in such a way that currently PoS will be used every 100th block. Ethereum will increase mining difficulty gradually until the beginning of 2021, when PoW will be essentially replaced by PoS (Invest in Blockchain, 2018).

Concerning smart contracts, they are pieces of code that can be executed by the Ethereum Virtual Machine (we can think of it a decentralized computer). Each smart contract has an Ethereum account associated to it with its own balance and an address. It is interesting to point out that smart contracts can communicate between them using messages, which is a special transaction in Ethereum. One can form virtual entities ruled by smart contracts which are able

to execute code in an autonomous way. These virtual entities are commonly known as Decentralized Autonomous Companies (DAC).

Some of the current applications of Ethereum are in self-sovereign identity management, healthcare systems, gambling or supply-chain management.

2.3. Hyperledger Fabric and Sawtooth

Hyperledger is a collaborative solution for building Blockchain solutions created by the Linux Foundation (Linux Foundation, 2018). It has been created with an eye put on industry and banking. Among other modules, Hyperledger includes the Blockchains Fabric, developed by IBM (Linux Foundation, 2018), and Sawtooth, created by Intel (Linux Foundation, 2018).

2.3.1. Fabric

Fabric shares some similarities with Ethereum in terms of structure and smart contracts but its main difference is that it is based on permissions. Fabric, in the manner of Ethereum, also admits smart contracts under the name of Chaincode.

Fabric offers an identity to its members for authentication together with the possibility of using access lists to use some functionalities. Concerning privacy and confidentiality, Fabric allows the creation of channels, which are private subnet of communication between two or more specific network members, for the purpose of conducting private and confidential transactions.

Consensus in Fabric, named Practical Byzantine Fault Tolerance, works as described below: there is a leader node, choosen in a deterministic way among all nodes responsible for validation, that orders the transactions candidates that should be included in a block, and broadcasts this list of ordered transactions to all other nodes responsible for validations in the network.

When each of the validation nodes receives the ordered list of transactions, they perform the following steps:

1. It starts executing the ordered transactions one by one.
2. As soon as all the transactions are executed, it will calculate the hash code for the newly created block, which includes hashes for executed transactions and nal state of the world.
3. Then it broadcasts its answer (the resulting hash code) to other peers in the network, and starts counting the responses from them.
4. If it checks that 2/3 of all validation peers have the same hash code, it will commit the new block to its local copy of the ledger.

2.3.2. Sawtooth

Sawtooth is Intel's proposal for the Hyperledger solution (Linux Foundation, 2018). It has been conceived for working as a permissioned blockchain or a permissionless blockchain with up to 100 nodes.

Sawtooth's main di erence with respect to Fabric is the consensus mechanism, called Proof of Elapsed Time (PoET). Roughly speaking, nodes in Sawtooth looking to publish a new block generate, randomly, a waiting time. The first node who runs the waiting time up is the node allowed to publish the block. This algorithm claims to be as energy saving as Proof of Stake and, furthermore, more egalitarian, as the probability to be choosen to create a new block does not depend on node's wealth.

2.4. IOTA

IOTA's proposal is based in a cryptocurrency whose underlying structure is an acyclic directed graph instead of a chain. This graph is commonly known as the tangle (Popov, 2017). The tangle is made of a set of vertices, which are the transactions made by nodes, and a set of directed edges, which work as follow: each time a new transaction is registered it must approve two previous transactions; this approval is represented with a directed edge, as shown below:

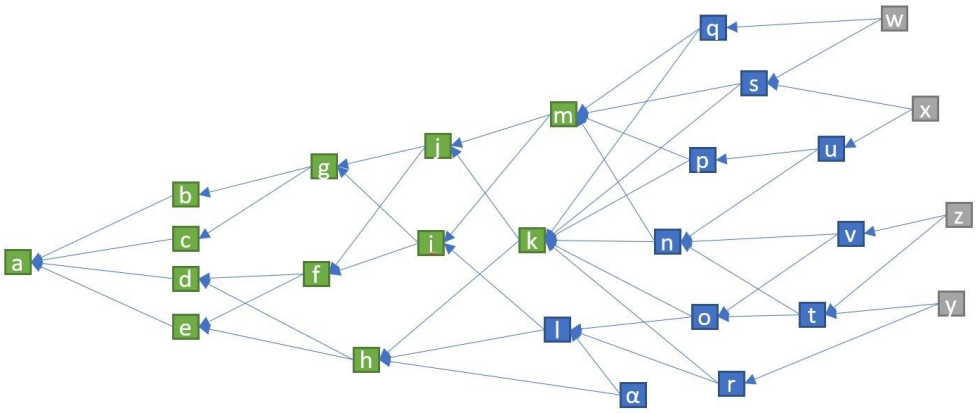

Figure 3: IOTA's tangle (iotafeed.com)

As shown in the gure, there may be transactions and g which may not be directly connected. In this situation we say that approves g indirectly.

The main idea about how IOTA works is the following: in order to issue a new transaction, users have to work towards approving other transactions: a node must approve two previous transaction before it can register a new one. With each approval, a transaction gets accepted by the system with more con dence. For instance: transactions b; c; d and e are con dently accepted whereas w; x; y and z are new transactions which may be fraudulent.

The main eld of operation of IOTA is the Internet of Things (IoT), the network of physical devices which are able to connect and exchange data by using the Internet. IOTA may be applied in public transportation, telecommunication systems or interactive maps.

2.5. NEM

NEM (NEM, 2015) is a Blockchain whose main di erence with the rest of solutions lies in its consensus algorithm: Proof of Importance (PoI). This algorithm, on the one hand, is much less expensive than PoW when it comes to computational power required and, on the other hand, although it is pretty similar to PoS, its functioning does not relies only on the balance of a node.

Another di erence with the majority of Blockchain solutions is that NEM allows accounts satisfying some requirements to delegate it mining power allowing them to mine blocks in a remote server without the risk of having the keys exposed.

One of the main disadvantatges in P2P systems is that, due to the fact that all partcipants are anonymous, it is easy to introduce hostile nodes in a network allowing them to broadcast false data or trying to interrumpt the normal functioning of the system. This is a problem that forces to nd a method to decide which nodes are faithfull.

In order to prevent from unfaithful nodes, NEM introduces a system of reputation where, once the netowrk receives some data, the nodes verify if this data is useful or not. Each node of the network who participates in an interaction with another node must classify this interaction as a success (received data is new and useful), neutral (received data is valid but not new) or as a failure (the information is not valid). From the interactions in the network, NEM is able to give each node a reputation score that will allow hostile nodes to be easily identi ed.

2.6. Quorum

Quorum (Bashir, 2017) is a proposal made by JP Morgan for a permissioned Blockchain built on Ethereum. Transactions in this proposal may be private thanks to a mechanism called Constellation which allows sending encrypted messages between peers in the network.

The Quorum network considers two roles for nodes: voter and maker, the latter being responsible for creating the blocks of the Blockchain. A node can play either one of the roles, both of them or none of them.

The consensus mechanism used in Quorum is called QuorumChain and is a Byzantine Fault-Tolerant mechanism which allows sending and verifying votes through transactions. A smart contract is responsible for managing the consensus process together with assigning voting rights to nodes. Once a block is backed by the needed number of votes, it is considered valid and included in the ledger.

2.7. Ripple

Ripple (Schwartz, Youngs, & Britto, 2014) is a permissioned Blockchain which appeared by 2014 and has been created to work as an open payment network. It admits smart contracts and shows some similarities with Ethereum and Bitcoin in terms of structure, although the main di erence with them lies in the consensus mechanism.

Ripple gets consensus not through PoW or PoS, but through a mechanism called federated consensus. If the idea behind PoW is the harder you work, the better and the idea behind PoS is the more you have, the more you get, in Ripple a block is accepted and included in the system if a minimum number of server nodes (the equivalent of miner nodes) votes for it. This minimum is determined by the protocol.

The main applications of Ripple are in banking, as it was created as a solution for currency exchange.

3. BLOCKCHAIN USE CASES

Blockchain technology has some features that make it attractive to several sectors besides cryptocurrencies. We are talking about smart property, digital identity management or digital voting. We give a little introduction to how Blockchain is being used in the latter situations and some others below.

3.1. Digital currencies

Digital currencies, or cryptocurrencies, were the first application of Blockchain technology. The main feature of Blockchain technology that have made the appearance of cryptocurrencies easier is the fact of being a distributed network, so there is no need for a central bank or central authority. It is also important to point out the fact that registers in a public Blockchain are open to everybody and almost impossible to tamper in most of cases, what o ers trustworthiness to cryptocurrencies, giving the impression that the currency supported by the Blockchain is returning the power to people. Nevertheless, in some cases (such as Bitcoin), payments are extremely hard to trace back to its origins, what opens the door to illegal activities. Some solutions are (Nakamoto, 2008) and (Wood, 2014) together with Litecoin, Zcash, Dash, Monero, Cardano, Stellar, Qtum, Siacoin, Bytecoin, Steem, Enigma and more than 1500 further cryptocurrencies (Coinmarketcap, 2017).

3.2. Smart property

A smart property is a property whose ownership is controlled using a Blockchain platform through a smart contract. Such registration could be stored on a ledger along with contractual details of others who are allowed ownership in this property. Smart keys could be used to facilitate access to the permitted party. The ledger stores and allows the exchange of these smart keys once the contract is veri ed.

The decentralized ledger also becomes a system for recording and managing property rights as well as enabling the smart contracts to be duplicated if records or the smart key is lost.

Making property smart decreases risks of running into fraud, mediation fees, and questionable business situations. At the same time, it increases trust and e ciency. We point out (Legal Desk, 2018).

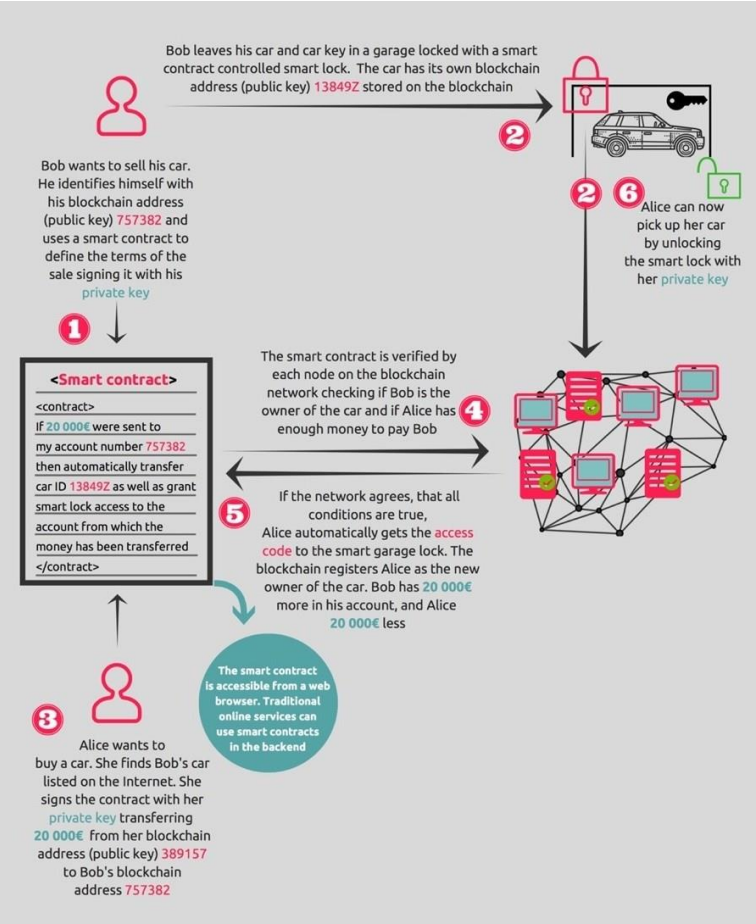

Figure 4: A smart property solution (blockchainhub.net)

3.3. Decentralized notary

One interesting feature of the Blockchain is its timestamp feature. The whole network essentially validates the state of wrapped piece of data (called a hash) at a certain speci c time. As a trustless decentralized network, it essentially con rms the existence of something at a stated time that is further provable in a court of law. Until now, only centralized notary services could serve this purpose.

One may think that Blockchain technology will get to replace notary services. Neverthelss, one cannot forget that a Blockchain-based notary service only would be able to prove existence at a point in time, that is: that someone created a particular document in the past. But notarising implies, among other things, that if a document was signed by several people, all of them signed it willingly; and this is something that a nlockchain-based notary service would not be able to prove. Furthermore, cryptographic keys can only prove the ownership of a hash, but not identity.

Despite the above considerations, Blockchain technology is being under use by notary services with the idea of reducing time and e orts in some tasks in mind. Some of the main solutions in this eld are BitNation (Bit Nation, 2018) and Proof of Existence (Proof of Existence, 2018).

3.4. Digital identity management

Blockchain technology o ers a solution to many digital identity issues, where identity can be uniquely authenticated in an irrefutable, immutable, and secure manner. Current methods use problematic password-based systems of shared secrets exchanged and stored on insecure systems. Blockchain-based authentication systems are based on irrefutable identity veri cation using digital signatures based on public key cryptography. In Blockchain identity authentication, the only check performed is whether or not the transaction was signed by the correct private key. It is inferred that whoever has access to the private key is the owner and the exact identity of the owner is deemed irrelevant. See (IBM, 2018) for more details.

3.5. Digital voting

The greatest barrier to getting electoral processes online, according to its detractors, is security. Voters expect the voting process to be anonymous, but veri cation of candidate countings should be possible. Votes should be impossible to tamper with and illegitimate votes should not be counted. All vote counting should be performed in a publicly observable way. Currently a voter cannot verify his/her vote was indeed counted appropriately. Furthermore, voters today are expected to trust the polling station and voting process. When designing a new voting system, a core tenet would be to remove all need for trust, and place strong emphasis on open veri cation of the process and the votes. A similar problem was addressed with digital currency such as Bitcoin and Ethereum.

Using Blockchain technology, a voter could check that her or his vote was successfully transmitted while remaining anonymous to the rest of the world. On a Blockchain, each group of transactions is hashed together, along with a hash of the previous block, and the entire Blockchain would be publicly accessible. Using a Blockchain for digital voting could record both voter and candidate ID, as well as the time. The voter IDs are a public/private keypair, not traceable to a voter's identity.

Among all the solutions for digital voting based in Blockchain technology there is Follow My Vote (Floow my Vote, 2018), based on the Blockchain BitShares (Larimer, Hoskinson, & Larimer, 2015).

3.6. DNS services

DNS system is a crucial component for the current Internet. Nevertheless, this is a centralized service (GNUnet, 2012), what may become a serious problem as the governing entities could modify the way the Internet works for every user.

There are three desirable requirements for a DNS system:

1. It has to be secure.
2. It has to be decentralized.
3. It has to be understandable for humans.

Since the appearance of Blockchain technology, it was believed that building a DNS system with the three requirements was impossible.

The first solution which was able to solve the problem of decentralizing DNS systems was NameCoin (Kalodner, Carlsten, Ellenbogen, Bonneau, & Narayanan, 2015). Roughly speaking, NameCoin is a solution based on Blockchain, with its same structure and consensus algorithm. The main di erence between Bitcoin and NameCoin is that the latter can store data within its own ledger. Another solution, similar to Namecoin, for DNS services based on Blockchain is Emercoin (Emercoin, 2018).

3.7. Logging services

Logging services are used to register actions made by users in a setting where information is shared in order to leave proof of access permissions given, denied, annomalies or suspicious activities detected.

The main problem in logging services lies in the fact that its reliability is conditioned to the security of the information storehouse where the registry is being saved. If a malicious agent get access to the storehouse, it would be able to tamper registry's data.

Blockchain's feature of o ering a panoramic view of every single transaction which gives participants the opportunity to trace transactions back to its origin in a setting of total integrity o ers very promising applications for the forensics community. Furthermore, as Blockchains are decentralized networks, central authorities would not be useful anymore.

One of the main proposals for the application of Blockchain technology in logging services is LogSentinel (Logsentinel: Blockchain-inspired secure audit trail, 2018).

3.8. Distributed computing

The role of Blockchain in computing power goes well beyond simply allowing users to draw resources from their peers across the world. Some groups are focused on getting peers united on a distributed computing platform for the cause of scienti c research. The possibility of accessing computer users worldwide and enlisting them to help solve scienti c problems has enormous potential.

Cloud computing provides users with processing power, storage, and other resources to help them execute their tasks.

With the cloud computing market dominated by a few entities like Microsoft, Amazon, and Google, an enormous portion of the world's population become dependent on these companies to carry out tasks that in the future may demand cloud computing. It is likely that purchasing the services of these companies will be relatively expensive, with conditions that are disproportionately in favour of the companies themselves.

There are two main issues in cloud computing: it still leaves the average individual out, and the centralized locations where the resources are held are still subject to failure.
Blockchain o ers solutions to both those issues. It can leverage the power of computers across the world, tied together by a Blockchain network, and distribute the task's workload among each computer.

Enigma (Zyskind, Nathan, & Pentland, 2015) is a peer-to-peer network which allows storing of information together with performing computations ensuring privacy of involved data.

Blockchain technology plays the role of the network controller as it manages the access control, identities and provides an immutable events registry.

Enigma's functioning depends, on the one hand, on threshold cryptography where in order to decrypt a message several parties must cooperate to succeed, and on the other hand on Blockchain as a source of immutability.

4. CONCLUSION

Since its first appearance in 2009 as the underlying technology for Bitcoin, Blockchain technology has become a promising solution for hundreds of problems ranging from governance to digital identity management. The impact it may cause on the way we know the world and how we imagine it can change dramatically.

One of the most important impacts of Blockchain technology will be related with authomation. With the use of smart contracts, implementing Blockchain as a replacement for the typical multiple executive approval processes would cut down project delays and create a universal agreement across business sectors impacting both clients and agencies.

Similarly, Blockchain can automate the sourcing, supply chain and procurement processes by tracking responsibilities throughout their life cycle, which would ensure accurate data and accountable transactions. This would disrupt the way marketers engage with and service their clients. As Blockchain continues to evolve, we wiill see a changing dynamic within the marketing community. Business transactions will get a makeover and this will create a veri ed transparent network that will ensure privacy and security. The adoption of Blockchain processes will lead to a boom that will disrupt traditional business and impact marketing.

Within the healthcare industry, Blockchain can automate and decentralize patient-provider functions that are currently highly time-consuming and highly costly. Blockchain's decentralized nature will create potential for hospitals and other healthcare providers to break down data access hierarchies and provide every individual in the health delivery and health consumption value chain with equal access to relevant healthcare data, while maintaining patient privacy.

Blockchain's potential is undeniable, and as more and more projects successfully bring its bene ts to the public, its overall impact on various aspects of modern life will grow. Healthcare, marketing, sourcing or supply chain are just some of the many industries that are ready to be disrupted through Blockchain technology.

5. REFERENCES

Bashir, I. (2017). *Mastering Blockchain.* Packt.

Bit Nation. (2018). *Bitnation public notary*. Obtenido de https://bitnation.co/notary/

Brown, R., Carlyle, J., Grigg, I., & Hearn, M. (2018). *Corda: An introduction.*

Coinmarketcap. (2017). *Cryptocurrency market capitalizations*. Obtenido de https://coinmarketcap.com/all/views/all/

Emercoin. (2018). Obtenido de https://emercoin.com/en

Floow my Vote. (2018). *Follow my vote: The online voting platform of the future*. Obtenido de https://followmyvote.com/

GNUnet. (2012). *Gnu's framework for secure peer-to-peer networking*. Obtenido de https://gnunet.org/centralized-dns

IBM. (2018). *Blockchain for digital identity*. Obtenido de https://www.ibm.com/blockchain/identity/

Invest in Blockchain. (2018). *What is the ethereum casper protocol?* Obtenido de https://www.investinblockchain.com/ethereumcasper-protocol/

Kalodner, H., Carlsten, M., Ellenbogen, P., Bonneau, J., & Narayanan, A. (2015). An empirical study of namecoin and lessons for decentralized namespace designand lessons for decentralized namespace design. *Proceedings of the 14th Workshop on the Economics of Information Security.*

Lamport, L., Shostak, R., & Pease, M. (1982). The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*.

Larimer, D., Hoskinson, C., & Larimer, S. (2015). *Bitshares: A peer-to-peer polymorphic digital asset exchange.*

Legal Desk. (2018). *Understanding blockchain-based smart property*. Obtenido de https://legaldesk.com/blockchaintechnology/

Linux Foundation. (2018). *Hyperledger*. Obtenido de https://www.hyperledger.org/

Linux Foundation. (2018). *Hyperledger fabric*. Obtenido de https://www.hyperledger.org/projects/fabric

Linux Foundation. (2018). *Hyperledger sawtooth*. Obtenido de https://www.hyperledger.org/projects/sawtooth

Linux Foundation. (2018). *Sawtooth*. Obtenido de https://sawtooth.hyperledger.org/docs/core/releases/1.0/contents.html

Logsentinel: Blockchain-inspired secure audit trail. (2018). Obtenido de https://logsentinel.com/

Nakamoto Institute. (2004). *Rpow - reusable proofs of work*.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.*

NEM. (2015). *NEM: Technical Reference.*

Popov, S. (2017). *The tangle.*

Proof of Existence. (2018). *Proof of Existence*. Obtenido de https://proofofexistence.com/

Schwartz, D., Youngs, N., & Britto, A. (2014). *The ripple protocol consensus algorithm.*

Wood, G. (2014). *Ethereum: a secure decentralised generalised transaction ledger.*

Zyskind, G., Nathan, O., & Pentland, A. (2015). *Enigma: Decentralized computation platform with guaranteed privacy.*