POLITECNICO DI TORINO

Master degree course in Software Engineering

Master Degree Thesis

Blockchain for Location Proving

Supervisors
Carla Fabiana Chiasserini
Paolo Giaccone

Candidates
Lorenzo Bonelli

Academic year 2020-2021

Abstract

Blockchain is a topic that has gained notoriety in recent years in relation to its use in cryptocurrencies such as Bitcoin, which has led to an extensive research of its potential applications. Many different fields and businesses have considered adopting it to transform their processes towards a more distributed, decentralized approach.

This thesis aims to analyze the application of blockchain technology to Proof of Location (PoL), a term which refers to the process of verifying and being able to attest the position of an individual at a certain space and time. A system that achieve this challenge can be useful for legal disputes, but more commonly it is applied to Location Base Services (LSBs) to prove that the location of the users is truthful and accurate. In some cases, such as location-based games, a user's self declared position is not sufficient, since it could be forged at their own convenience. Solutions to this problem are usually based on confiding on a single entity to do the checking and certification of the position for every single user. A blockchain system can provide decentralization to this process and is also able to maintain a better degree of privacy, removing the necessity of some entity continuously tracking the user's location.

A design is proposed employing the permissioned blockchain platform: Hyperledger Fabric. The design is directed to businesses which can cooperate to maintain a record of the visits of customers to their facilities and offering them benefits for opting in the service. As an incentive they can access anonymized data about their clientele and their habits, which could be valuable for data mining aimed at improving their commercial activity. In this scenario, the strengths of the solution are the relatively simple requirements of implementations compared to other Proof of Location systems and the existence of incentives to every participating party.

Contents

Chapter 1

Introduction

Today, a significant number of businesses have a vested interest in building a new generation of transactional applications that place trust, accountability and transparency at their core, along with an open and distributed architecture. The emergent technology called Blockchain is at the center of this shift and could revolutionize the approach for many complex real-life applications. Until now, various applications have been considered for the technology which could carry a strong potential, but, at the same time, the development and implementation present several challenges that are still far from being explored completely. Very few projects built on Blockchain have been shown to be successful, the trust on the solidity of Blockchain is still lacking and the user adoption is generally low. In this thesis it's studied a system which is able to provide a proof of truthfulness of the location of its users, also called Proof of Location (PoL). The challenge surges from the necessity of some Location Based Services (LBS) for which it is necessary to verify false location claims by the users could provide disruptions to the service. Users could have the incentive to lie when asked for their own position, in cases where cheating can provide better rewards in-app or could show a better desired image to their friends. LBSs are really diffused today and they offer users useful services such as geographic navigation, social networking, information about weather, the location of nearby services and tourist attractions and so on. The main system by which LBSs service receive the users' location is from the GPS receiver inside their devices. GPS is based on satellite geolocation, it's used extensively, but it lacks completely the possibility of verifying the location of the receiver. In addition to this, surges the possibility of malicious parties having access to tracking data, especially with the increasing number of services being built upon location. Given the

features of a blockchain architecture, it's interesting the idea of exploring its application to the problem of proving locations, to create a decentralized and secure solution. Several works have attempted to create solutions involving some sort of PoL and blockchain [14, 17, 18] in diverse scenarios such as car navigation, logistics or an augmented reality game. In this thesis a particular scenario is addressed, where some entities cooperate to offer a service that verifies the location of the customers near their businesses and which could be defined PoL or Proof of Presence, in fact the information which is managed doesn't properly correspond to a punctual position, but to the general presence in a delimited area. The parties involved could be for example a chain of gyms, a super market company or an event organizer; the incentive to the service would be commercial: the customers receive the location proving service, while the businesses could extract useful data about their customers without violating their privacy. The evaluated solution, built with Hyperledger Fabric, could also be considered as an evolution of a blockchain based loyalty program, since the system could be adapted easily to include points and rewards. The field of "business to customer" loyalty programs stands out as one in which the blockchain applications bring real benefits over the previously used solutions [19]. Evidence of the previous claim is the project currently on the market [20], by IBM, who has invested in creating a platform based on permissioned blockchain that fills this niche. The solution that is proposed in this work is based on a simple but effective design that was not studied before and that could be realistically implemented by businesses without serious obstacles.

1.1 Thesis outline

The structure of the thesis is as such:

- In chapter 2 the distinctive characteristics of Blockchain are described, as well as its main features. To understand the technology that is being employed.

- In chapter 3 the differentiation in the blockchain types are explored, together with the state of the art of this technology. The focus is also brought on Hyperledger Fabric which is the platform chosen in the project.

- In chapter 4 the field of geopositioning is analyzed: the main algorithms

are reported, the different approaches that are used to build a geopositioning system are evaluated to find which one could fit the blockchain architecture.

- In chapter 5 it is explained the motivation, the design, and the development of the distributed system which was conceived.
- In chapter 6, finally, the result of this thesis is summarized as well with a perspective on future research on the matter.

Chapter 2

Blockchain

2.1 Introduction

The word Blockchain describes a relatively recent technology which is experiencing substantial interest both from investors in the IT industry and from the computer science field. The potential of Blockchain is gradually being recognized in different fields, resulting in several development studies being carried out and active investments, its breakthroughs are being observed closely by many entities, who could be positively or negatively impacted. Its involvement in cryptocurrencies has shaken the world of finance: the non-centrally managed payment system Bitcoin, based on a blockchain, was deemed by some to be a real threat to central banks soon after conception in 2008. As of August 2021, cryptocurrencies retain a total market value of above two trillion dollars, attesting to their popularity [1]. The main idea introduced with blockchain technology is the removal of the need for trusted intermediaries in transactions between untrusting parties. For this purpose, it is employed a Peer-to-Peer (P2P) network architecture in which every node participates equally in the services needed by the participants. Compared to a client-server model the resources are made available by the participants instead of being offered by a central server. The participants in the system remain anonymous, but they can still collaborate securely if they can assume the majority of the resources isn't possessed by a single malicious party. The record of transactions is kept in ledger, a chain of data blocks (from which the name Blockchain) in which all the transactions ever made are grouped. The ledger is visible and stored by every party, but it can't be altered as it is immutable, blocks can only be appended to the tail. Being the best known and first noteworthy example of blockchain application, Bitcoin can be used

as a running example to explain the functioning of this technology. In fact, Blockchain is a broad concept and not entirely well defined, but most of its applications share several elements in common.

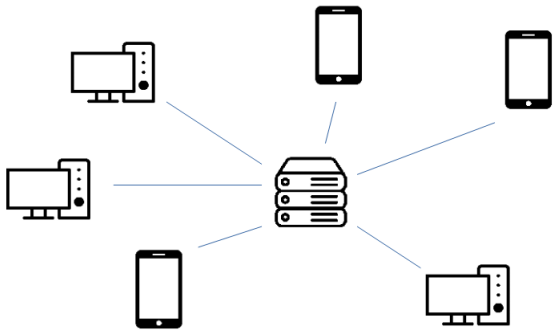

Figure 2.1. Client-Server Architecture

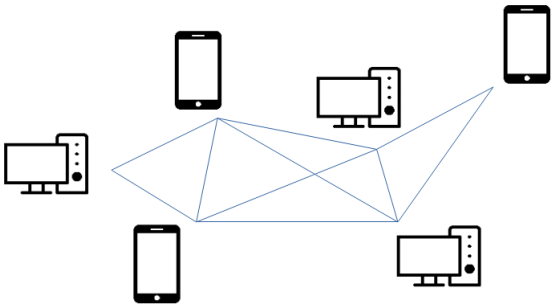

Figure 2.2. P2P Architecture

2.2 Architecture and functions

2.2.1 Blocks

The ledger is the data structure where all the record of previous transactions is stored. It is replicated between all the nodes belonging in the P2P network. As a consequence of knowing every transaction, it is also possible to calculate the current state of every peer, which, in case of Bitcoin, means knowing the

amount of coin contained in every wallet. When enough transactions are grouped, a block is formed and then added, binding it with the rest of the chain. When 2-3 more blocks are added to that block it becomes permanent in the ledger with all its transactions being considered final. A possible modification in the content of a transaction requires the manipulation of every subsequent block in the chain to hide this manipulation, which is an occurrence that is realistically impossible. Each block in the chain is identified by a cryptographic hash value generated by hashing its with a hashing function such as SHA-256. [2]

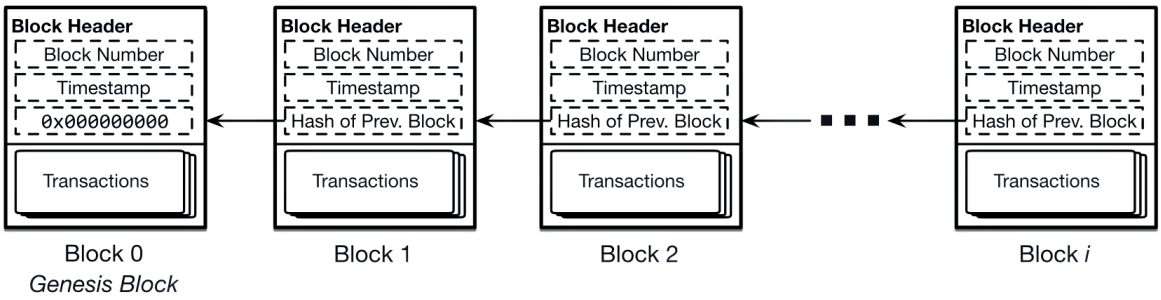

Figure 2.3. Blockchain structure from J. Kolb et al.[4]

At the start of each block there is a block header which includes [3]:

- The block version.
- Merkle tree root hash. The Merkel tree, which is a data structure that synthesizes the transactions contained in the block. This structure is built recursively by hashing pairs of transactions to obtain a single hash value, called root. It is used to verify accuracy efficiently.
- The minimum number of bits of the hash to be mined.
- A Nonce, which is an arbitrary single-use number.
- The hash of the previous block.

Following the header, the block body contains the transactions, whose number depends on the block's size. In the case of Bitcoin, transactions contain three elements: the Bitcoin address of the sender and the receiver together with the amount exchanged.

2.2.2 Peers interaction

A paradigm of collaboration founded in clear rules, known by every peer, permits the cooperation between participants without problems of agreement. The use of asymmetric cryptography provides authentication and integrity; each individual user or node interacts with the blockchain through its key pair, signing their own transactions with their private key; the public key is known by the other nodes and utilized to verify the signatures. Neighboring nodes are responsible for validating each incoming transactions before retransmitting them to the rest of the network, if they consider them to be valid. All transactions that have been collected and validated by the network using the above process during an agreed time interval, are sorted and packaged into a candidate block together with the timestamp. This is a process called mining. The first node that succeeds in forming a candidate block and transmitting it to the network is awarded with an amount of cryptocurrency. The rest of the nodes verify that the mining process was executed properly through checking the hash, otherwise they discard it. The transaction validation stage is essential to give the network a consistent and unaltered state as it may be managed parties who don't trust each other. To prevent potential possible chaos coming from this distributed environment and to help the network reach a proper global state, each blockchain network needs to establish certain rules to determine the global state and to verify the result of the miners.

2.2.3 Cryptography

Blockchain technology is built on two key cryptographic concepts: hash function and digital signature. Hash functions are mathematical functions with the following properties [5]:

- The input of the function is a string of any size.
- The output of the function always has a fixed size.
- For a small change in the input, the output varies significantly.
- It is computationally efficient.
- It is collision resistant which implies that it is not feasible to find a number x and y, such that H(x) = H(y) where H is the hash function.

- Calculating the inverse function requires an exceedingly great effort in processing time

A digital signature is a cryptographic method to guarantee the authorship and integrity of information. This is achieved by means of a hash function that works as a signature associating the identity of a user or system to a message or document.

2.2.4 Consensus

Digital signatures are used to verify that a transaction is signed by the person claiming to have signed. However, the problem arises when anyone can send the same transaction twice, each with a completely valid signature. In centralized systems, the central authority is the ruler of the network and therefore it has the role of preventing problems such as the double-spending problem, which consists in registering twice a transaction with the same coins, either by error or by malicious intention. In a fully decentralized system, network participants, regardless of whether or not they have full trust in each other, need to agree on common rules to prevent problems such as this. The distributed consensus protocol is employed to achieve this objective, where between the nodes that make up the network is taken into account a number of them which could be malicious. This consensus therefore ensures the possibility of agreement between all honest nodes to verify a transaction as non-malicious. The challenge is that simple majority cannot be relied upon, a malicious entity could act in the network pretending to be multiple nodes, this action is what is called Sybil attack. Multiple consensus algorithm have been studied, that can prevent this kind of attacks, the best known are [2]:

- **Proof of Work** (PoW): protocol where the computational power of the hardware is used by the nodes to determine which node will append the new block. Each miner tries to variate the nonce until the hash of the block is lesser than a predefined numerical value. The miner who accomplishes this objective is essentially chosen randomly, but has greater chance based on his mining capacity, and rewarded by a quantity of cryptocurrency. The drawback of this approach is the waste of energy and computational power which is not strictly necessary for operating the ledger.

- **Proof of Stake** (PoS): is based on the idea of deterministically selecting the creator of a new block based on a preference for its wealth (or stake).

In this protocol, the reward received is the commission paid for each of the block's transactions. Within the benefits of PoS as opposed to PoW are the ability to use economic penalties against malicious players and the lesser consumption of energy to sustain the network of miners.

- **Proof of Authority** (PoA): protocol where a subset of network nodes are nominated as validators or authorities to maintain the stable operation of the blockchain. Each validator is chosen to be the leader for a set period of time. It aggregates the transactions into the next block, which is appended after the approval of the majority of the other validators.

2.2.5 Smart contracts

To define what a smart contract is, it is useful to recall the meaning of a contract: an agreement or arrangement between parties who bind themselves on a particular matter which they may be compelled to perform. In the field of blockchain a contract establishes the rules of the interactions between the parties involved and are written in a specific programming language. They are used to eliminate intermediaries to permit implementing actions and controls that make it possible to create more complex transactions. A smart contract is created by one or more blockchain network participants and, once encoded, it is stored on the blockchain itself and it becomes available to be invoked by participants or other smart contracts as long as the execution conditions are met. A smart contract can be used to model the sale of a physical good without any external agents or mediators, where the payment and the transference of the good are both executed and stored as a consequence of the contract at the same time. If, after the sale, the previous owner tries to sell the same asset again to another participant, this action will be rejected by the participants of the blockchain network when executing the contract during the verification.

Chapter 3

Current state of the Blockchain Technology

3.1 Introduction

Blockchain is a very young technology that presents revolutionary aspects for the industry. As expressed above, its application in different businesses is of great interest. To better mold the technology of blockchain to such different fields, various platform have been developed that permit a degree of modularity and adaptability. Two of the most important project are Ethereum and Hyperledger.

3.1.1 Use cases

Some of the use cases where the technology has seen potential are:

- Supply chain management
- Digital identity
- The energy market
- Health care
- Real estate
- Voting
- Cryptocurrencies

By analyzing the use cases, together with the features of blockchain architecture, it is possible to compile a list of the characteristics they have in common which correspond to the difficult real life problems that are sought to be solved with Blockchain.

- The necessity of interaction between parties that don't trust each other.
- A high degree of security to maintain privacy and avert exploits.
- Transparency and traceability of the transactions, to avoid problems such as collusion between participants.
- Decentralization of the processes.

3.1.2 Types of blockchain

In this subsection are highlighted the three most relevant types of blockchain which are distinguished by their policies.

- **Public blockchain**: Any user is free to participate in the network, even acting as multiple members. There are no restrictions or members with higher governance power. As long as the elected consensus algorithm is solid and the majority of the participants are honest, the operation runs smoothly. A downside is the tendency by necessity of adopting the high power consumption consensus protocol called proof of work.
- **Private blockchain**: A participant can participate in a private blockchain only if they receive a valid invitation. The network operators owns the power of modifying the blockchain protocols and only one entity has the ability of appending transactions to the ledger [4], sacrificing most of the decentralization.
- **Permissioned blockchain**: Can be considered a hybrid between the previous two. Its participants need to be approved before joining. Having this possibility of screening members the complexity of the consensus algorithm can be relaxed, resulting in a more efficient network. They are particularly viable for use between cooperating, but separated, businesses [4].

3.2 Ethereum

Ethereum [26] is a public and decentralized blockchain based on an open source project, which allows for the creation of a wide variety of applications of different kind. It defines a cryptocurrency called Ether, which is consumed during the execution of each transaction carried out on the blockchain platform. By using smart contracts, different types of business logic can be implemented. Each computational step executed corresponds to a certain amount of gas used, the sum of all the gas needed for a smart contract can be converted into its total Ether cost for its execution. According to Ethereum's developers, the platform permits to instantiate any type of transaction, agreement or any activity with economic or governance aspects. Ethereum uses proof of work for consensus, which implies considerable costs per transaction and can lead to dissatisfaction among miners and users. Innovation is underway to migrate the platform towards proof of stake. As for an initial estimate, the migration was intended to be at the end of 2017, but this was delayed due to the need to scale the platform.

3.3 Hyperledger Fabric

3.3.1 Introduction

Hyperledger Fabric [21] is a framework that arises from an open source project, initiated in December 2015 by the Linux Foundation. The aim of the project is to bring together independent efforts to develop open standards for working on blockchain technology, as well as to provide a modular framework that supports different components for different purposes. The network defined by this framework is private and permissioned and therefore requires its members to be enrolled. For this reason, Hyperledger defines in its architecture a Membership Service Provider component, which is called MSP and whose main objective is to issue certificates for each member of the blockchain network. Hyperledger Fabric is designed specifically for enterprise use cases and provides some remarkable features of adaptability: the consensus mechanisms can be updated according to the needs of the network and it supports multiple MSPs with different configurations. There are several details regarding its internal functioning that are important, such as topology of the network, the configuration of channels, the consensus conditions, the configuration of the orderers and the definition of the chaincodes. These elements will be described throughout this section, sourcing the information

directly from the Hyperledger Fabric official documents [21].

3.3.2 Ledger

The data is stored in a structure called ledger, which consists of two components: the "world's state" and the "transaction log", as shown in Figure 3.1. Each participant has a copy of the ledger of each network to which it belongs. The World State component describes the state of the ledger at a given point in time, the values stored are in the format key-value, permitting easy access. The Transaction Log component component records all transactions that resulted in the current value of the world state, essentially it is the history of all the updates to the world state. The record of transaction has a specific order which corresponds to the order of execution. The ledger is stored in all nodes belonging to the network, while the orderer only stores the transaction log. The transaction log, stored in the orderers, provides fault tolerance and it allows the nodes to replicate the world state building it by executing the transactions in order.

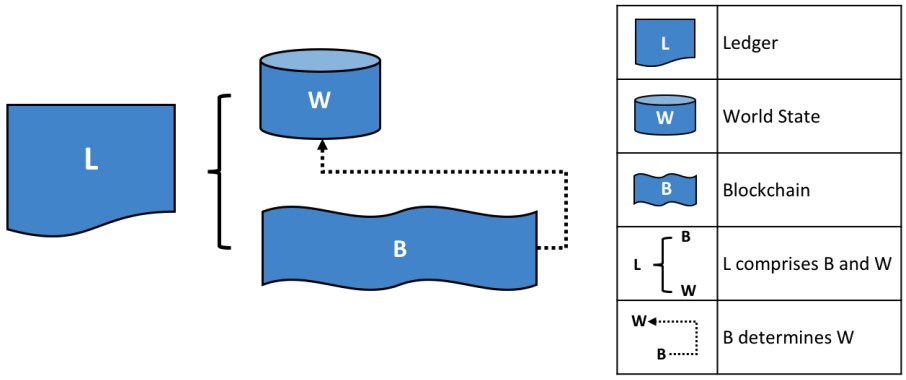

Figure 3.1. Hyperledger Fabric Ledger [21]

3.3.3 Channels

Hyperledger Fabric provides one feature that stands out from other frameworks, named channels. They are a private subnet which permits private

communication between two or more members of the network, the transactions generated in a channel can't be accessed by members outside the channel. Therefore, nodes that are not registered in the channel, will not be notified of transactions affecting that channel. Data entering the channels may also be restricted to be accessed only by certain nodes belonging to the channel, by means of chaincodes and their write policies. Channels can be added at any time in the network.

3.3.4 Orderer

Given its characteristic of being a private blockchain, Hyperledger Fabric can employ a non-probabilistic consensus algorithm. The orderer is given the role of packaging the blocks by determining the transactions' order in a globally consistent way and then propagating the blocks to all members in the network. At the same time the orderer is the component in charge of verifying that the write policies corresponding to the channel and the chaincode policies corresponding to the transaction are complied with. The digital signatures generated by the nodes where the transaction is executed are used for this purpose. There are different types of configurations for the orderer, each one of them has its particular characteristics and therefore each is recommended for different scenarios. The recommended configuration is called "Rafta" and uses a "leader and follower" mode: for each channel a leader node is elected and its decision replicated by the follower nodes.

3.3.5 Chaincodes

Chaincodes are the implementation of smart contracts and are the element that permit creating transactions and also communication between organizations. They are programmed, versioned and deployed in each node of the network where they are executed, they can be implemented in different programming languages such as Java, node.js and Go, the latter being the most widely used. During the consensus process, they are used by the participants to verify that the transactions that are sent to them are valid. They are installed based on channel, which limits the visibility of the information exchanged only to the nodes belonging to the channel and where the chaincode has been deployed. When installing a chaincode in a network, it is necessary to define: peers where it will be installed, name, channel, version number and policy. The policies are specified in a language defined by Hyperledger Fabric which allows to indicate which organizations and how many peers of

must sign the transaction to be considered valid. Additionally, chaincodes can invoke other chaincodes by using an API that provides a specific function for this purpose.

3.3.6 Nodes

In Hyperledger, nodes are the communicating entities of the blockchain network: they execute the chaincodes to perform write and read operations on the ledger. They are grouped in trusted domains and associated to logical entities that control them, the organizations. Organizations are entities which have a big role in the functioning of a Hyperledger network, they have access to channels and own peers and clients. Through the Membership Service Providers (MSP) they can issue certificates to the participants as a way of guaranteeing their identity.

As can be seen in Figure 3.2, there are three types of nodes:

- **Client**: they send transaction invocations to the endorsers and broadcast transaction transaction proposals to the orderer. The endorser is in charge of returning the received transaction, together with its signature, to the orderer.
- **Peer**: a node that creates transactions, maintains the state and a copy of the ledger. It can have a special endorser role. This only belongs to a single organization.
- **Orderer**: a node running the service of verifying and ordering transactions for other nodes.

Furthermore the peers cover different functions essential in the network, they can be classified by different attributes that can be given depending on policy:

- Anchor peers: they are the nodes on a channel that are reachable to all the peers, even form outside their organization. Each organization must have at least one such node.
- Leader peer: they are nodes in an organization that have the function of communicating with the orderer and propagating the transactions to the other organization's peers. Their existence improves scalability.
- Endorsing peer: they are in charge of receiving transactions from clients or applications and the execution of the transaction, but without leaving

a record of it. If the simulation is successful, it is then sent to the ordering service to gather them and transmit them to the rest of the network. This simulation occurs for several reasons: to avoid an intentional attack by a client against the network and to avoid configuration errors, either in the chaincode or in the network.

- Committing peers: they append the block to the ledger after it has been created by the orderer.

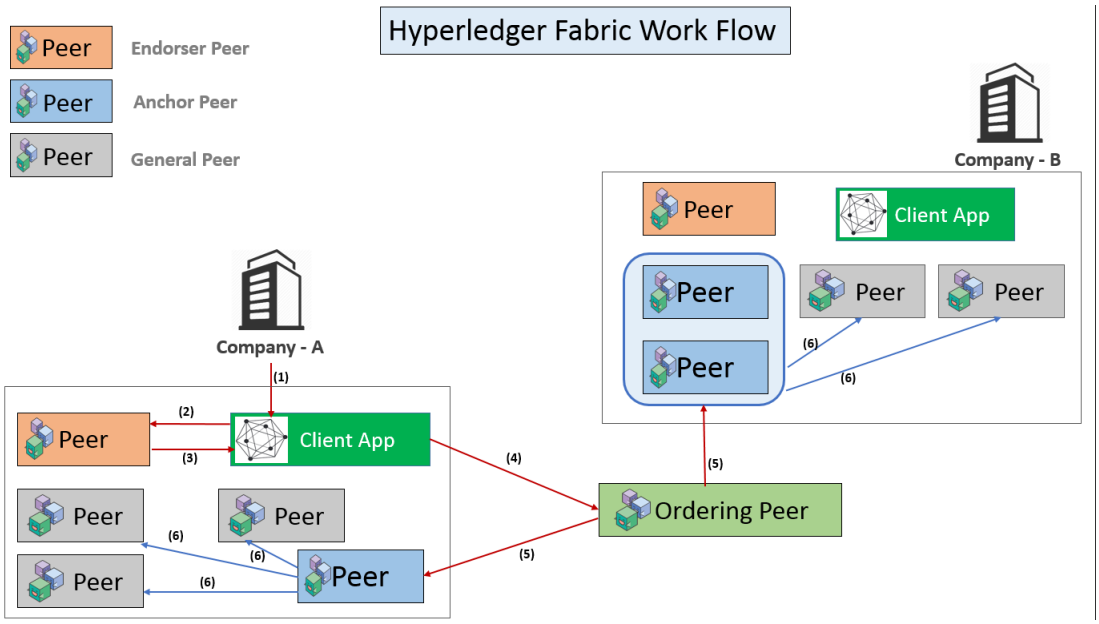

Figure 3.2. Hyperledger nodes structure [25]

Chapter 4

Geopositioning

4.1 Introduction

Geopositioning or geolocation is the process which consists in calculating the univocal position on earth of a particular point in space, which can then be registered or communicated through a set of coordinates.

4.1.1 Techniques

This process requires having other objects or anchors, whose position is known, and making measurements to them and between them, then, to obtain the coordinates of the desired position, one of the following geometrical algorithms is applied:

- **Triangulation**: determines the location of the point applying trigonometric formulas with the angles formed by two known anchors and of the observed object. These three points are used to construct a triangle. It was used in the past with mechanical tools; right now it is used for the Angle of Arrival (AoA) technique, by calculating the direction of radio signals.

- **Multilateration**: determines the location through the measure of distance to other known points and then finding the intersection of the calculated ranges. In particular to find the location on a plane just three measurements are needed. The distance can be measured with different methods, analyzing the passage of a signal between two points it is possible to measure the difference in timestamps, energy or phase.

Depending on the case radio, acoustic, laser or seismic waves can be employed.

- **Fingerprinting**: relies on storing, in an offline phase, some features of an environment that is position-dependent, such as the location of beacons producing a signal . Later, the position of a particular point can be discerned by taking a measurement of that feature and consulting the database to deduce which position could the measurement be taken from. It is mainly used in indoor Wi-Fi positioning which will be discussed later.

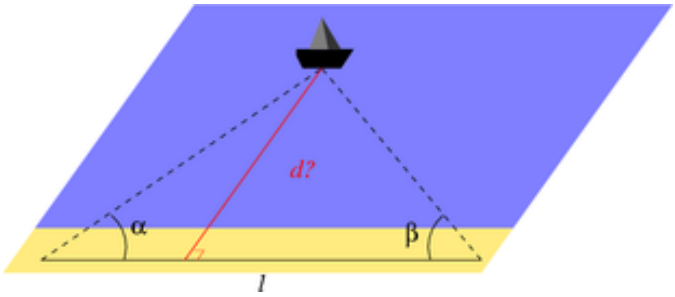

Figure 4.1. Calculation of distance based on triangulation. [6]

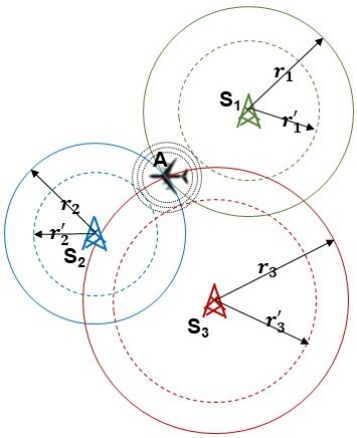

Figure 4.2. Calculation of the plane's position with radio towers based on multilateration. [7]

4.1.2 Coordinate system

A geographic coordinate system can be defined as a frame of reference that can map on a geographic area. The necessity of this reference frame is to provide a standardized way of describing the positioning an object, so it can be recorded and communicated. There are several types of of coordinates conventions used worldwide in history. However, the best known and most widely used is the system using latitude and longitude. Latitude is the distance that expresses the position relative to the equator in the north or south direction. Longitude is the distance that expresses the position in the perpendicular direction, east-west. With these two values, it is possible to locate any point within a two-dimensional representation of the earth's surface.

4.2 Geopositioning systems

Different kind of systems exist or are theoretically possible, which fulfill the necessity of geolocation. GPS is currently the most diffused system because it's well established and very effective, but other methods could provide other benefits, such as creating some sort proof of the produced location, either by other users acting as witnesses or a trustworthy central entity which can verify the position and assure its correctness.

4.2.1 GPS

The Global positioning systems is a project lead by the United States Space Force and started in 1973. It consists of a network of 24 to 32 satellites in orbit which contain a high precision atomic clock. The system can provide the terrestrial position and accurate time to the users. The service is open and free to any company and civilian. The GPS receiver can compute its location as long as it has a clear line of sight of at least 5 satellites. The distance from each satellite is calculated comparing the timing of the messages received from the other satellites, then a multilateration algorithm is applied to obtain the coordinates, which possess an accuracy in the range of a few meters in normal conditions. GPS is completely reliant on the US Department of Defense and, for this reason, the US can selectively restrict its usage at any time and without notice, for example for political reasons. This was the case in 1999 when the GPS service was denied to the Indian military to influence the outcome of an international conflict. Since then multiple countries started developing their own positioning system to avoid a similar occurrence [9].

An other issue is that the accuracy can be greatly affected by meteorological conditions, mountains or even man made objects. This fact can make it non viable in some cases, especially in case of indoor environments. These issues also render the technology unusable for real time applications where consistency is key, like for giving directions to an autonomous vehicle as well as for contact tracing applications between people, because when the GPS receiver moves inside buildings the signal is unable to work correctly. A problem which is more particular to military use involves manipulating GPS signals with malicious intent:

Jamming consists of preventing the correct reception of satellite data by using radio interference.

Spoofing consists of producing false GPS signals which are broadcasted at greater strength to overpower the authentic signals. It can be used to "confuse" the GPS receiver, this technique can be used by a hacker to induce the navigation system of a vehicle to give wrong directions.

Finally a GPS communication is one directional and unencrypted from the satellites to the receiver, so, by its nature, GPS can't be used to prove the receiver's device location, since false GPS coordinates could be easily provided.

4.2.2 Mobile phone tracking

Another approach to identify location, is based on mobile phone network data. By virtue of its nature, this solution can only be applied to cellphones connected to a mobile phone operator. Each antenna included in the mobile phone network provides coverage for the radius reachable by radio communication. Using this rule, the territory is partitioned into regions, which are called cells. This process is more generally called Voronoi tessellation and finds application in many other fields. Signals are generated when mobile phones try to connect to multiple available antennas and when crossing between different cells. Furthermore data on distance can be gathered from the strength of the radio signal received. This infrastructure is suitable for geopositioning but suffers several limitations. The accuracy of the position obtained is low, because the main purpose of the infrastructure isn't locating the cellphones in the network, but establishing which cell they belong to.An option would be using cellphone tower triangulation to reduce the error but this would increase the load on the infrastructure, which isn't well equipped for this purpose, thus limited. The position obtained through these

means has the advantage of being trustworthy: since it is verified by the mobile phone operator it cannot be forged. On the other side of the coin the issue which surges is privacy. The location data of the users needs to be protected. The mobile phone operators require special attention in storing this data since it is susceptible to attacks which could cause loss of sensitive information. Mobile phone tracking is used today mainly for statistic studies on aggregated anonymous data or, in isolated situations, for legal cases. Camenisch et al. [10] proposed a solution which solves the problem at least partially, its privacy-by-design approach ensures that sensitive information is only shown to the approved party that requests the verification of a location claim.

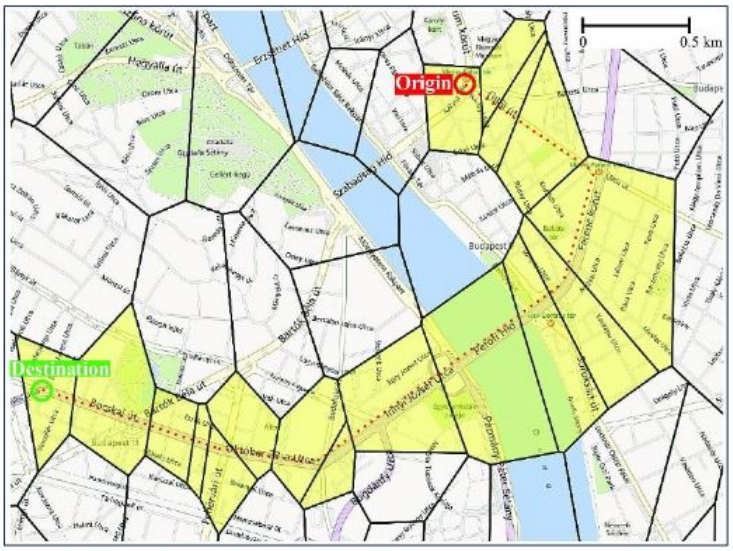

Figure 4.3. Network cells crossed by a traveling terminal [8]

4.2.3 Wi-Fi scanning

Wi-Fi based geolocation can take advantage of the several Wi-Fi access points that are present on the territory, such as routers, to generate a device's coordinates. One advantage of such approach is the great effectiveness in indoor environments, especially in cities. The Received Signal Strength Indicator (RSSI) is a measurement taken by an antenna that reflects energy of a signal. Each particular location in a building is characterized by a unique set of Wi-Fi signals that are available and a particular RSSI associated to them.

Wi-Fi fingerprinting is an approach that employs a database recording the Wi-Fi fingerprint of an indoor location. It consists of recording the position and the power of the signal of every AP. A user device, having access to nearby Wi-Fi signals, can consult the existing database to compare its RSSI and discover its location. The precision of this technique can vary substantially but the error is generally around 1-2 m [11] and can be improved by using a probabilistic approach. Other locations systems based on Wi-Fi scanning are less common. Angle-of-arrival based techniques use triangulation to calculate the position. The direction of the Wi-Fi signals are obtained computing the change of phase in the signal received from different antennas in the same receiving device. Time-of-flight location employs the timestamps produced by the access points to reach the same purpose. The advantage of these solutions based on Wi-Fi scanning is definitely the low complexity of implementation, they don't require any significant additional infrastructure or device. On the other hand, as GPS, it doesn't provide any verification for proving the location to third parties in its standard implementation.

4.2.4 Custom Wi-Fi communication

A different way of geolocating a user's device is to verify the position through the communication between the user device and one or more APs. It can be assigned to an entity the role of authority which controls the APs, this entity can certify a user position when requested. Pham et al. [12] introduced a method based on this approach, the motivation is to prevent cheating in activity tracking apps which permit to share personal fitness result. Its functioning is dependent on the existing distribution of routers already present on the territory and that are owned by a particular Internet Service Provider. The ISP can control the routers to connect to a user smartphone and then verify its location claim. The weakness of this approach is the necessity of a wide scale availability of APs that are capable of running some sort of script and the design of a custom procedure that permits the communication between the user device and AP. The above solution [12] proposes a mechanism that requires the periodical broadcast of PoL requests from the user to the nearby routers. However current smartphones and network protocols aren't able accommodate this system without significant implementation costs and challenges. Zhanikeev [13] also attempted to create a system in which APs provide PoL for users, but it concludes that the currently the infrastructure isn't capable of fulfilling such role "unless one assumes that WiFi APs play active role in supplying and validating locations". Finally for this approach

the accuracy isn't very high because the range of a router is generally around 50 m, but can vary greatly, as it can vary the range of the user's antenna.

4.2.5 Peer-to-peer communication

A P2P architecture, given its features and advantages, is suitable for geolocalization as a distributed effort between equal peers. Some peers can act as witnesses of others' presence by guaranteeing the correctness of the positions. By assuming the majority of the witnesses are truthful it is possible to discover false location claims to maintain reliability in the network.Furthermore this kind of architecture would apply especially well to a blockchain system, which permit the service to possess features such anonymity of the users, decentralization and so on. This is the case of the work by Amoretti et al. [14] who introduced a system whose objective is to achieve location proof through the activity of prover nodes and witness nodes, therefore distributing the job of location proving. A similar architecture is presented in other papers [15], always proposing the use of the Bluetooth technology. The weakness of this approach is the great inconsistency of the Bluetooth range, which for most of the smartphones in use is estimated around 10 meters. This fact, paired with the necessity of multiple witness nodes next to the prover, makes the Bluetooth technology not practical for this kind of application, compared to Wi-Fi. P2P systems using Wi-Fi connections have been studied for smartphone communication, in particular texting. The FireChat is an app developed for Android and iOS which permits communicating to nearby users without access to the internet thanks to its off-the-grid connection, employing Bluetooth or Wi-Fi Direct. Several attempts at similar applications have been made without significant success, in 2018 the support for FireChat [27] was discontinued. The example of this app was described to show the difficulty of implementing direct Wi-Fi connections for ad hoc wireless device communication. Android currently offers Wi-Fi direct which is a standard for P2P communication available for Android devices, while Apple offers the Multipeer Connectivity platform. A big challenge is to create a solution which can work through different competing platforms and which also doesn't encounter an easy market, since it presents a threat to telecommunications companies. As of now very few real world applications are found in P2P Wi-Fi and the support for the existing platforms is scarce. Nevertheless this type of system has great potential and could find interest and support for many different uses. The possibility of multipeer connection and the extended range of 200 m (declared by Wi-Fi Alliance®) would

make it a better candidate compared to Bluetooth. Good accuracy could be obtained using multilateration algorithms and multiple peers.

4.2.6 Ad hoc radio location

Wi-Fi, Bluetooth and 5G operate at high frequency, greater than 2 GHz; meanwhile LPWAN is a radio technology meaning low-power wide-area network, designed for IoT devices to communicate at great distance with low power usage. It takes advantage of various ultra-narrow frequency bands are not licensed. LoRa is a type of LPWAN that operates at "low data rate (27 kbps with spreading factor 7 and 500 kHz channel or 50 kbps with FSK) and long communication range (2-5 km in urban areas and 15 km in suburban areas)" [16]. With these kind of specifications building a network based on LPWAN definitely has many advantages for building a geolocation application, although the infrastructure would be very costly to build. FOAM [17] is a project that aims to build a global network consisting of fixed beacons that use LPWAN which can localize customer devices. It is a shared and open protocol whose goal is "to support a decentralized, privacy preserving, highly accurate, censorship resistant alternative to GPS". The accuracy is not declared, but, it is limited by the resolution of the grid: physical addresses are encoded with a unique hash that correspond to location with resolution of a one square meter.

4.2.7 Hybrid systems

Finally, there is another way which is possible to adopt when creating a geolocation system which consists in combining two or more technologies. GPS, Bluetooth, Wi-Fi signals, fingerprinting, etc. are all valid sources of location information when creating a solution. For example Wi-Fi fingerprinting and GPS share similar accuracy and features, the indoor weakness of the GPS is complemented well by the effectiveness fingerprinting. Another option would be combining the simplicity and wide availability of GPS with Bluetooth verification to add a way of proving the user position. Sporadically users could act as witnesses for other users to catch attempts at cheating by false location claims. With a mixed approach potential limitations of a single technology can be overcome at the price of a more complex implementation.

4.3 Comparison table

Each solutions comports different benefits and limitation and each is valuable in some real world use cases. In Table 4.1 they are evaluated and compared according to the different variable that have been discussed.

Table 4.1. Comparison of location systems

	Accuracy	Scale	Location Proof	Privacy	Difficulty ofImplementation	Consistency
GPS	5 m	Global	No	Yes	Already available	Affected by meteorologic events and attacks
Mobile Tracking	~50 m	National	Yes	Partial,thedata is possessed by the MPOs	Medium, the infrastructure already exists	High,the mobile networks antennas are widespread
Wi-Fi Scanning	1-2 m	One building	No	Yes	Low	Medium,varies on the richness of the database
Custom Wi-Fi	~50 m / 1-2 m	Dependson the authority	Yes	Feasible	Medium	Niche, only works next to valid APs
Phone Bluetooth	20 m	City area	Yes	Feasible	Medium	Low,requires many other users to interact with
Phone Comunic.	~50 m	Broadcity area	Yes	Feasible	High	High
Radio Location	1 m	Large area	Yes	Feasible	Very High	High

4.4 Conclusion

In this chapter, firstly they are reported the general components and possible algorithms of a geolocation system. Then, every significant system that can be used for this purpose is analyzed highlighting strengths and weaknesses. At this point in time GPS is the standard system that is being used for the vast majority of applications, but many different protocols are being studied that rely on widely different technologies. Particular attention is given to the possibility of producing a proven, not forgeable location. There are two main approaches for this purpose: one is having a third party who owns the network, the entity with this role has be trusted and has to have the means to verify and guaranty the locations of the users. The other is a P2P systems in which the users entrust the rules and the architecture of the systems to collaborate and provide the PoL service to the users. No existing platform is widely available to address the problem of Proof-of-Location. The technologies that could be suitable for this goal are a few but none has been

shown to have the advantage given the extremely small number of systems established in the market.

Chapter 5

Business-User Proof of Location system

5.1 Introduction

After exploring the possibilities of Blockchain in this work, it was created a design of an application aimed at generating Proofs of Location (PoL) for the users in certain locations. The specifics are described in this chapter, starting with general characteristics, then describing the architecture and its operation and finally evaluating the effectiveness and feasibility.

5.1.1 Basic model of operation

The elements that are considered for the design of this products can be synthesized as two: the users and the blockchain network. A stylized architecture with all the components is visible in the Figure 5.1. The user doesn't participate in the network but they can interact with a client, which instead communicates with the blockchain network. From the point of view of the system, the user is anonymous and it is associated with a unique key. A client, which is located next to a Point Of Interest (POI), is able to initiate the request procedure to produce a PoL for the users that are situated in its vicinity. The blockchain contains a record of the visits of each user to each POI, and a timestamp of said visit. The network is maintained by different cooperating organizations, which own and operate a subset of the existing client and nodes.

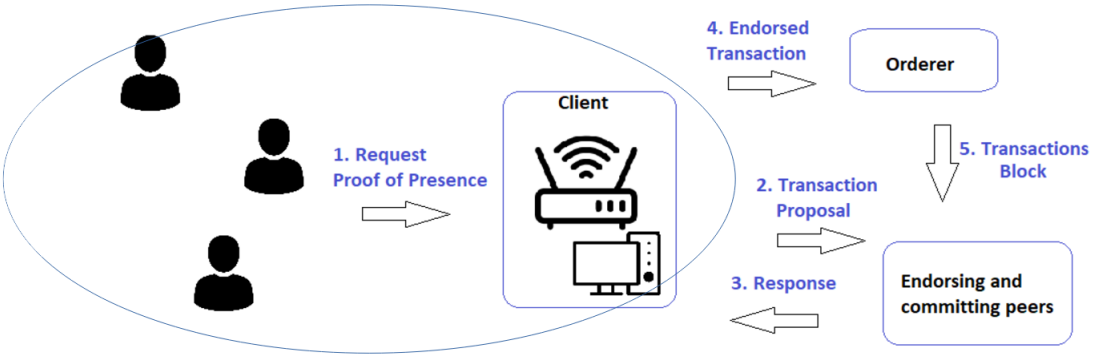

Figure 5.1. Architecture design

5.2 Design choices

In this section most of the project's characteristics and features are described.

5.2.1 Hyperledger Fabric

It is preferable to adopt a permissioned blockchain compared to a public blockchain given its feature of quicker transaction times among its other benefits. This choice can be possible since the organizations that own the nodes of the blockchain are a limited number, their fitness to participate can be screened to prevent malicious actors, so there is no need to employ a more robust consensus algorithm, which would increase the server load given its complexity. In particular Hyperledger Fabric was selected, as it stands out as one of the most popular permissioned blockchain platforms and is characterized by low latency and high volume of the transactions. It is designed to provide high flexibility and scalability. The target of the chosen platform is to grant Business to Business (B2B) cooperation in blockchain applications, so it is suitable for the case studied in this work. Since the data that is being recorded in the ledger isn't particularly sensitive or important and the peers are trusted, the default endorsement policy can be adopted: majority endorsement, where the majority of peers' validation is needed and sufficient for the approval of the transaction. A single channel is established where every peer participates, since multiple channels are not needed to

occult transaction to some of the peers.

5.2.2 Architecture components

Looking more in dept in the architecture the different parts of the blockchain network are discernible. Each organization owns a subset of clients, committing peers, endorsing peers and orderers to fulfill the functionalities of Hyperledger Fabric. To simplify further the structure the POI can act both as a client and a peer for one organization. Each peer keeps a complete replica of the ledger with the world state. The process of validation of the transactions needs to follow the process mandated by the platform, Hyperledger Fabric. It is as such:

1. The client receives a request by a user to generate a PoL.
2. The client proposes to the endorsing peers the transaction.
3. The peers check if there aren't issues with the policies and the transaction is approved.
4. The transaction is then sent to an orderer to guarantee consistency in the ledger between the transactions; a block is created.
5. The block of all the transaction received by the orderer is sent to the committing peers, to be appended to the ledger.

In the POI some sort of terminal needs to be installed with hardware capable of handling the database size and the transactions' throughput, which are not too demanding thanks to the lightness of Hyperledger Fabric. It also connects and communicates to the users' devices thanks to a Wi-Fi AP. The hardware required could be just a router and a PC or a Raspberry Pi. On the other hand, the user doesn't participate in the blockchain so it doesn't need to be trusted; the user's hardware requirements are just a smartphone to run an app that communicates with the client and is able to show the PoLs through a simple GUI.

5.2.3 Services to the users

While building the architecture, the product was imagined to fill a specific user necessity in the real world and to do so in a viable way. Different scenarios of use were considered that are compatible with this design. The only

difference in the following descriptions is the feature of the user's smartphone application. By doing so the application could provide a slightly different service while the blockchain infrastructure remains unvaried. The main design of the system has the objective of commercial use by the customers of shops and businesses. A user frequently visiting these place in their city can use the app to track the chronology and frequency of the visits, and, at the same time, could receive benefits from the aforementioned shops, like discounts. To validate the cost of the discounts, the incentive to the businesses is to have the possibility to gather useful data: to opt-in the service the users are required to fill a survey containing anonymous personal information like family size, age range, interests and so on. The organizations can mine this data to extract insights such as which businesses have intersecting sets of customers or what are the time habits of their customers. As a consequence, customer service and marketing campaigns could be improved. The other possible modification of the application shifts the vision to add value to the client by providing "badges", which prove their presence in some place. Event organizers can set up POIs in film festivals or video game conventions, or else a coffee shop chain can give badges for every countries that was visited by the user and included a stop in one of their franchised locations. The badges posses collectible value for the users who can show them to their friends.

5.2.4 Data

In the world state database the data which is available consists of each user's asset containing: a unique key for the purpose of storing and querying, the personal attributes which are provided in the survey and their last visit to a POI with a timestamp, an illustration is shown in Figure 5.2. The full list of their visits is obviously stored, but not in the world state. By virtue of the blockchain it's possible to retrieve every PoL of the users by reading the ledger from the start; this process would be costly, but it is not needed to query it frequently since the user's PoLs are also kept in the user's device. The transactions are the main element that permit the ledger to be updated, once a set of transaction is approved they are placed in a block by the orderer and then inserted in the ledger. Two types of transaction are present: to write in the ledger or to read in the ledger. All of them are listed below:

- `CreateUser`: Allows to register a user in the world state, initializing its values.
- `AddProofOfLocation`: First, it is checked in the world state if the user

in question wasn't logged in another place at the same time, which would make their current location impossible. The time that would be required to reach the current POI form the last POI is calculated by multiplying the maximum realistic speed of transfer with the distance between the two POIs, taking into consideration sufficient error. If the time frame between the two visits is deemed as unrealistic the transaction can't be endorsed and it will be discarded. Subsequently the transaction adds the new PoL to the ledger by registering the user's ID, the POI's ID, the POI's coordinates, the approximate duration of the visit and the timestamp of the visit with date and time.

- `ReadUserHystory`: Retrieves every transaction involving a particular user ID, it can be used to send this data to the user application.
- `ReadPOIHystory`: Retrieves every transaction involving a particular POI ID, it is run by an organization to gather commercial data.

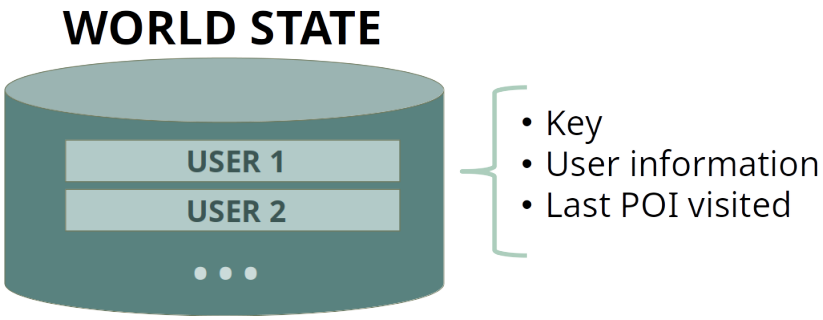

Figure 5.2. World State Data

5.2.5 User-Client interaction

The user, entering a zone belonging to the POI area needs to establish communication with the client, then a sequence of signals is exchanged between the two. After establishing the connection and before beginning the sequence of signals, optionally the client can be set up to calculate the distance between the POI and the connecting user. This process is generally unnecessary, but can be adopted to ward off potential users that never access the POI's zone and claim to deserve a PoL. The solution selected for this purpose is

the calculation of the round trip time, which is the time span needed for a packet sent from the client to be received from the user and then sent back to the client. A recently released WiFi standard, introduces the protocol WiFi-RTT which fulfills exactly this necessity and is able to calculate the position with an accuracy of ±1.2 m [24]. After calculating the distance it is possible to discern if the user's device is effectively inside the POI's area. The communication process is described in Figure 5.3 and its sequence is as such:

1. The user connects to the client Wi-Fi network, through this connection the app communicates with the client.
2. The user initiates the request of a PoL and sends a randomly generated string, called salt.
3. The client returns its signature, hashing the salt with its private key, hence proving its identity. Furthermore it generates a salt as well, sending it to the user.
4. The user verifies the signature with the client's public key and responds in the same way, hashing the salt provided by the client. The user's set of keys was provided to them at the moment of creating their asset in the blockchain.
5. The user's signature is received correctly and the parties mutually end the communication.

If the client judges the user to be in order, it keeps monitoring the Wi-Fi connection in the router to calculate its duration. When it is lost, the client also collects the location, the time and the identification number of the user, thus it initiates the transaction to be added to the ledger.

5.3 Analysis

5.3.1 Privacy

Privacy is always an important aspect in evaluating a design, especially in the field of Blockchain. The only information which is sensible in this design is the users' location paired with its timestamp. By default, the identity of the user is never associated to their asset in the ledger, so the privacy of the user isn't threatened. For this reason no other mechanism is strictly needed

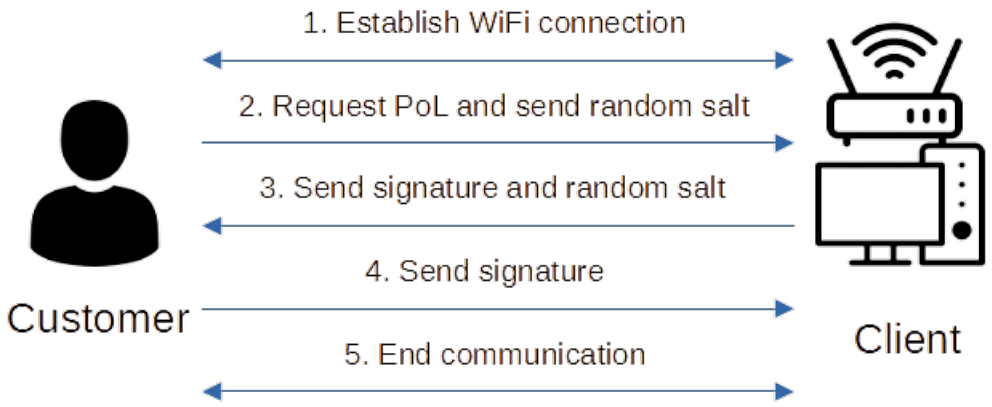

Figure 5.3. User-Client communication

to make the users anonymous. However the risk of the user identity to be associated to their ledger asset is still present. It would be produced by illicit actions carried out by a party with access to the ledger, hence putting their whole location history in danger. Even in this extreme case the data wold only be in the hands of the organizations who hardly would be motivated to revealing to other parties. Furthermore it needs to be pointed out that the organizations owning the POI's facilities could still possibly track their users with other forms of illegal behaviors, such as employing cameras and monitoring credit card information.

Nevertheless another solution is thought if the privacy issue is deemed to be a problem: the ledger architecture can be modified and the users' asset with ID can be omitted from the design, their attributes can be instead communicated for each PoL and be recorded inside each transaction. The outcome of this choice would be greater transaction size and, more importantly, the reduced value of the information obtained from the organizations, which wouldn't be able to data mine the users' habits.

5.3.2 Scalability

Hyperledger Fabric, compared to other blockchain platforms, is characterized by its focus on scalability, which normally is a weakness of blockchain architectures. It was made an effort to estimate the level of scalability of this

design. The main critical points that influence the statistic are the total size of the ledger and the transaction throughput, the latter being more dominant, given the inexpensiveness of storage devices. As highlighted on the paper from Thakkar et al. [22] there is a negative correlation of block size with latency but a positive correlation with throughput. The transactions' validation for this system's intent doesn't need to be instant and can afford a delay, thus the block size can afford to be expanded until the saturation point. At this point it's acceptable to make a few assumptions to analyze the hypothetical throughput of the network without making a fully scaled test. which would be unworkable for its challenging implementation and hardware requirements. Glorenflo et al. [23] point out that the reachable throughput threshold that is achievable by optimizing a few independent parameters is about 20000 transactions per second. Given the choices made in the design of block size, endorsement policy and channels, it is possible to deduce that reaching 20000 tps is achievable, and as a consequence make the following calculation, acknowledging the employment of generous approximations. If **N** is the number of total users and it is assumed that in the peak one hour of activity there are **3N** transactions, the transaction latency and throughput would remain stable up to a number **N** of user equal to 24 millions. Therefore any problem for the scalability of the network are ruled out thanks to Hyperledger Fabric's features; no benchmark is needed to infer the feasibility of the architecture about this aspect.

5.3.3 Malicious actors

Here are reported the issues that could surge in case of some party acting in a selfish or disruptive way for their own gain:

- **Malicious User**: It's impossible for a user to disrupt the service for other users in any realistic way, however it is possible for a user to act selfishly to gain advantages, in case that some benefit is desired. An example is to connect to the Wi-Fi AP from a position that is situated outside the POI area. This behavior isn't particularly threatening because the potential losses at stake are small and the selfish users that abuse this possibility by connecting to multiple clients a day can be identified easily between the small number of users belonging in the outliers. For completeness, it is take in into account that it is possible to create a minor inconvenience to the organizations by providing false information in the survey, but it wouldn't generate any significant damage assuming it is a rare practice.

- **Colluding User and Organization**: This scenario is more damaging to the design, it shouldn't occur since the organizations need to be considered worthy of confidence to cooperate between each other. The organization could easily forge several false transactions who would be impossible to be identified as such by the other peers. In the extreme case presented, there aren't obvious measures to be taken, but the false transactions would all belong to a particular organization leaving the others unaffected and the damage limited.

5.3.4 Comparison with other projects

One of the features of the design presented in this work, compared to the other blockchain PoL systems, is that it doesn't need a high adoption for the system to actually work, since the organizations provide the service and the infrastructure and have an incentive for doing so. The PoL project based on the blockchain Ethereum, FOAM [17], does need a high quantity of investors who invest in operating radio beacons in the territory, which present a steep starting wall to begin operation. Meanwhile the solution proposed by Amoretti et al. [14] needs a minimum threshold of adopters to let the witness-prover system work correctly. Since the users provide PoLs for each other, and need to be present in the same location, a low density of nodes would entail the complete unemployability of the system for its purpose. This project doesn't require neither high user adoption or high business investment and could be employed effectively in multiple different scalability levels. The users don't interact with the blockchain and only need a smartphone, the process of participating is very streamlined. Every party in the system can enjoy some sort of clear incentive, meanwhile, for some other systems, such as FOAM, there is the necessity of employing a cryptocurrency to make everything work finely. This signifies establishing fees between the participating entities, which motivate them to provide the service to others, hence making the whole project more complex and delicate. On the downside, the structure of the system is pretty rigid. it can't provide good precision and consistency in the available locations since it is highly dependent on where are the POI stationed. For this reason the application isn't employable in legal scenarios or to keep track of transports.

5.4 Conclusion

In this chapter is described an original design based on a blockchain architecture and aimed to grant to its user a certified proof of their location. Hyperledger Fabric stands as an ideal platform to be implemented on. The general structure reflects the most intuitive and simple way to implement a PoL system with a permissioned blockchain. Furthermore the scenario of usage is described, which takes into account the feasibility as a product on the market and the value it can offer to both users and organizations. During the definition of its architecture relatively few obstacles were encountered and the design attests to its uncomplicated implementation compared to other blockchain projects in the same field. It was avoided to delve into further development and a prototype because of the limitations of the deploy environment, which would impede carrying out tests with multiple peers and clients. The implementability of the solution on the Hyperledger platform, anyway, is not in doubt.

Chapter 6

Conclusion

The author of this thesis has been faced with the challenge of applying the blockchain technology to the problem of geolocation and Proof of Location. To reach this objective, firstly it was explored the background and context of the field. Blockchain principles have been described and its platforms. One of the first choices was adopting a permissioned blockchain platform, in particular Hyperledger Fabric, for its widespread use and high capabilities of low latency and high transaction throughput. Secondly the field of geolocation has been studied to evaluate the state of the art technologies that can be employed to locate a user. Given the complexity of the task, few solutions are applicable to the problem of Proof of Location effortlessly. The only project that reaches the goal of creating a system capable to provide high accuracy PoLs on large scale is FOAM [17], which is still in a deployment phase. After researching more information about other research in this field, different alternatives for creating a solution were identified. The proposed design doesn't attempt to create a worldwide system active everywhere to generate PoLs. Rather, the objective (which is successfully achieved) is focused on creating a functioning system, which can be deployed with the current state of technology and fills a particular niche. The design and its operation is described in chapter 5, it consists of a Hyperledger network apt to generate PoLs to the customers of businesses, but it is flexible and can be applied also to similar scenarios with no modification to the Hyperledger architecture, by changing the end-user application. The choice of relying on businesses to offer the service is driven to the necessity of some entity to play the role of organization in the Hyperledger architecture. Being a blockchain project, the steps between design and implementation of a working product require a substantial amount of work, so a complete prototype

was not created. Instead different possible platform set ups modifying peers and channels number have been tested on a Linux environment. Further improvements can be done to the project by calculating the exact position of the user instead of just the general presence next to the POI, to accomplish this task a solution could be to require multiple anchor point near the POI to triangulate a device position. The research on the topic is plentiful, but further effort and investments are required to establish a valid product that is effectively capable of provide the service of location proving, which is the goal this project aims to achieve.

Bibliography

[1] Joanna Ossinger *Crypto Market Retakes $2 Trillion Market Cap Amid Bitcoin Gains* Bloomberg, August 15, 2021 from www.bloomberg.com/news/articles/2021-08-15/crypto-market-retakes-2-trillion-market-cap-amid-bitcoin-gains

[2] John Kolb, Moustafa AbdelBaky, Randy H. Katz, and David E. Culler. 2020. Core Concepts, Challenges, and Future Directions in Blockchain: A Centralized Tutorial. ACM Comput. Surv. 53, 1, Article 9 (May 2020), 39 pages. DOI: https://doi.org/10.1145/3366370

[3] Zheng, Zibin et al. *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.* 2017 IEEE International Congress on Big Data (BigData Congress) (2017): 557-564.

[4] J. Kolb, M. AbdelBaky, R. H. Katz, and D. E. Culler, *Core concepts,challenges, and future directions in blockchain: A centralized tutorial,* ACM Computing Surveys (CSUR), vol. 53, no. 1, pp. 1-39, 2020.

[5] Menezes A., Van Oorschot P. C. & Vanstone S.; *Handbook of Applied Cryptography.* CRC Press. October, 1996.

[6] Wikipedia contributors. (2021, June 26). Triangulation (surveying). In Wikipedia, The Free Encyclopedia. Retrieved 16:29, August 16, 2021, from en.wikipedia.org/w/index.php?title=Triangulation_(surveying)&oldid=1030512637

[7] Wikipedia contributors. (2021, August 7). Multilateration. In Wikipedia, The Free Encyclopedia. Retrieved 18:15, August 16, 2021, from https://en.wikipedia.org/w/index.php?title=Multilateration&oldid=1037594550

[8] Tamás Tettamanti and István Varga *Advances in Civil and Environmental Engineering* (2014) Vol. 1 No. 1 pp. 1-15

[9] M. Goswami, R. Ghatak and A. Bose, *Global Navigation Satellite Systems and Indian Defence Research - A Review*, 2019 International Conference on Range Technology (ICORT), 2019, pp. 1-4, doi:

10.1109/ICORT46471.2019.9069614.

[10] Camenisch, J.; Ortiz-Yepes, D.A.; Preiss, F.-S. *Strengthening authentication with privacy-preserving location verification of mobile phones.* In Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society, Denver, CO, USA, 12 October 2015

[11] Xia S, Liu Y, Yuan G, Zhu M, Wang Z. *Indoor Fingerprint Positioning Based on Wi-Fi: An Overview.* ISPRS International Journal of Geo-Information. 2017; 6(5):135. https://doi.org/10.3390/ijgi6050135

[12] Pham, A.; Huguenin, K.; Bilogrevic, I.; Dacosta, I.; Hubaux, J.-P. *Securerun: Cheat-proof and private summaries for location-based activities.* IEEE Trans. Mob. Comput. 2016, 15, 2109–2123.

[13] Marat Zhanikeev, *The Last Man Standing Technique for Proof-of-Location in IoT Infrastructures at Network Edge*, Wireless Communications and Mobile Computing, vol. 2019, Article ID 7317019, 12 pages, 2019. https://doi.org/10.1155/2019/7317019

[14] Amoretti, M.; Brambilla, G.; Medioli, F.; Zanichelli, F. *Blockchain-Based Proof of Location.* In Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018

[15] Ni, X., Luo, J., Zhang, B., Teng, J., Bai, X., Liu, B., and Xuan, D. (2016) *A mobile phone-based physical-social location proof system for mobile social network service.* Security Comm. Networks, 9: 1890– 1904. doi: 10.1002/sec.926.

[16] Ferran Adelantado, Xavier Vilajosana, Pere Tuset-Peiro, Borja Martinez, Joan Melià-Seguí and Thomas Watteyne. *Understanding the Limits of LoRaWAN* (January 2017).

[17] FOAM White Paper. https://www.foam.space/publicAssets-/FOAM_Whitepaper.pdf, January 2018.

[18] C. F. Chiasserini, P. Giaccone, G. Malnati, M. Macagno and G. Sviridov, *Blockchain-based Mobility Verification of Connected Cars*, 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), 2020, pp. 1-6, doi: 10.1109/CCNC46108.2020.9045104.

[19] D. Agrawai, N. Jureczek, G. Gopalakrishnan, M. Guzman, M. McDonald, K. Henry, (2018) *Loyalty Points on the Blockchain* Business and Management Studies. 4. 10.11114/bms.v4i3.3523.

[20] IBM, Customer loyalty program hyperledger fabric VSCode, (2013), GitHub repository, https://github.com/IBM/customer-loyalty-program-hyperledger-fabric-VSCode

[21] *A Blockchain Platform for the Enterprise*, Hyperledger Fabric docs,

https://hyperledger-fabric.readthedocs.io/en/release-2.2/

[22] P. Thakkar, S. Nathan and B. Viswanathan, *Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform,* 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), 2018, pp. 264-276, doi: 10.1109/MASCOTS.2018.00034.

[23] C. Gorenflo, S. Lee, L. Golab and S. Keshav, *FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second,* 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2019, pp. 455-463, doi: 10.1109/BLOC.2019.8751452.

[24] C. MA, B. Wu, S. Poslad and D. R. Selviah, *Wi-Fi RTT Ranging Performance Characterization and Positioning System Design,* in IEEE Transactions on Mobile Computing, doi: 10.1109/TMC.2020.3012563.

[25] *How does Hyperledger Fabric works?* Tech Geek, 2018, https://techgeek628.medium.com/how-does-hyperledger-fabric-works-d5a4d4ff6b07

[26] *INTRO TO ETHEREUM*, 2021, https://ethereum.org/en/developers/docs/intro-to-ethereum/

[27] FirebaseExtended, Firechat, (2016), GitHub repository, https://github.com/FirebaseExtended/firechat