PEOPLE’S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
UNIVERSITY OF IBN KHALDOUN, TIARET

UNIVERSITY OF IBN KHALDOUN-TIARET

MEMOIRE

Introduced to :
MATHEMATICS AND INFORMATION TECHNOLOGY FACULTY
INFORMATION TECHNOLOGY DEPARTMENT

Presented to obtain :

MASTER degree

In : COMPUTER SCIENCE
Specialty: Network and telecommunications

By:
GUERROUDJ MOHAMED AMINE

BENAZZEDDINE ABDELKADER

On the subject

An approach to improve Blockchain authentication protocol for Internet of Things

Discuss the graduation project on 03/10/2021 in Tiaret in front of the jury composed of:

Mr Mostefaoui Sid Ahmed	Grade	M.C.B	Univ Ibn Khaldoun	President
Mr Meghazi Hadj Madani	Grade	M.A.A	Univ Ibn Khaldoun	Supervisor
Mr Laid Lahcen	Grade	M.C.B	Univ Ibn Khaldoun	Examiner

2020-2021

Acknowledgements

In the name of Allah The Most Beneficent and The Most Merciful. All praises are to Allah SWT for all blesses so that the writer can accomplish this thesis. In addition, may peace and salutation be given to the prophet Muhammad prophet muhammad peace be upon him who has taken all human being from the darkness to the lightness.

Alhamdulillahirobbil'alamin, praise and gratitude only to Allah SWT, the Glorious, the Lord, and the All mighty, the Merciful and the Compassionate, who has given bless and opportunity for the researcher to finish the paper entitled " An approach to improve Blockchain authentication protocol for Internet of Things ".

In the process of writing this thesis, the writer got so many helps, motivation, and guidance form our Parents and our Supervisor Mr Meghazi Hadj Madani participation .

Dedication

As well as everything that I do, I would be honored to dedicate this compilation to my parents. The two people who gave me the tools and values necessary to be where I am standing today. My parents support me in every step I take and decision I make, but it is necessary to understand that they let me make my own decisions. I will never finish thanking my father and my mother for all the opportunities that they offered and gave me, for all the teachings that they have told me, and for every piece of advice that came out of their wisdom. Besides the unforgettable participation of my little sister, Dr.G I. with assistance in obtaining a higher education.
Not forgetting the good Friends that i had in my journey, my partner Ben Azzeddine AEk, my dears Friends, El Maati Nadir, Korichi Badre Dine and Ben Masroufe Islam ,next to Zhwani.M.B, Dekki.A, Benhamouda.Mohamed.H, Ait Hammo.Hamzi and Zoukel.R

GUEROUDJ MOHAMED AMINE.

Dedication

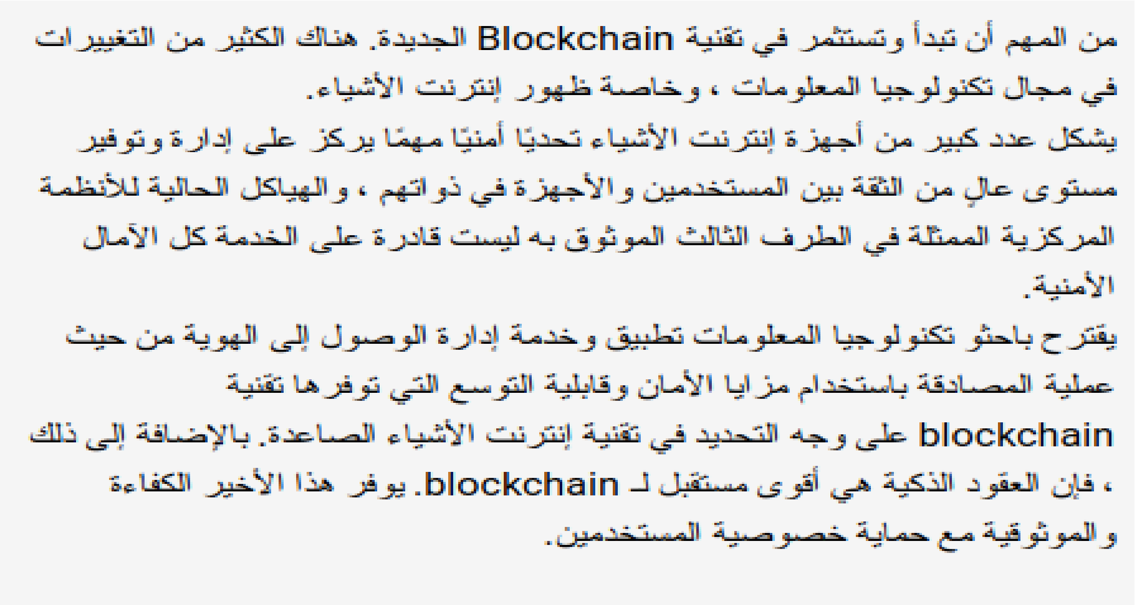
I wish to express my sincere thanks to my parents who stand for me in my journey with everything they could offer and guide me to achieve one of the most important steps in my life which are graduation and get a master degree in computer science without forgetting, by brothers and sisters for the encouragement they offered and all my families, I want to thanks all my friends from the closest ones to whoever assist me, thanks to: Guerroudj Amine, Korichi Badereddine, Elmaati Nadhir, Benmassrouf Islam, Dilem youcef, Chebbah mostapha, Azzouzi Dhiyaa, Zahwani Bahae, Zoukel Rami, Dakki Amine, Ait Hammo Hamza, Benhamouda Mohamed, Brahim, Taki, Hocine, and all the others. Finally, I thank everyone who contributed to help me to get what I am now.

BEN AZZEDDINE ABDEL KADER

Abstract

It’s important to start and invest in Blockchain new technology. There are so many thing changes in the Information Technology field, especially the rise of the Internet of Things. The large number of the IoT devices pose an important security challenge that focused to manage and provide a height level of trust between users and the devices in their selves, the current structures of the centralized systems represented in the trusted third party are not capable to serve all the security hopes. The IT researchers propose to apply and serve the Identity Access Management mechanism in term of authentication process by using the security and scalability advantages that the blockchain tech provides precisely in the Internet of Things rising technology. In addition, the smart contracts is the most powerful future of the blockchain. This last deliver the efficiency, reliability while protecting users’ privacy.

Keywords: Internet of Things , Identity Access Management ,Trusted Third Party , Blockchain Network , Smart contracts .



من المهم أن تبدأ وتستثمر في تقنية Blockchain الجديدة. هناك الكثير من التغييرات في مجال تكنولوجيا المعلومات ، وخاصة ظهور إنترنت الأشياء.

يشكل عدد كبير من أجهزة إنترنت الأشياء تحديًا أمنيًا مهمًا يركز على إدارة وتوفير مستوى عالٍ من الثقة بين المستخدمين والأجهزة في ذواتهم ، والهياكل الحالية للأنظمة المركزية الممثلة في الطرف الثالث الموثوق به ليست قادرة على الخدمة كل الآمال الأمنية.

يقترح باحثو تكنولوجيا المعلومات تطبيق وخدمة إدارة الوصول إلى الهوية من حيث عملية المصادقة باستخدام مزايا الأمان وقابلية التوسع التي توفرها تقنية blockchain على وجه التحديد في تقنية إنترنت الأشياء الصاعدة. بالإضافة إلى ذلك ، فإن العقود الذكية هي أقوى مستقبل لـ blockchain. يوفر هذا الأخير الكفاءة والموثوقية مع حماية خصوصية المستخدمين.

CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

TTP	Trusted Theard Party
IAM	Identity Access Management
IT	Information Technology
IoT	Internet of Thing
CAP	Consistency, Accessibility, Partition-tolerance
P2P	Peer-to-Peer
PoW	Proof of Work
DPOW	Delayed Proof of Work
DPOS	Delegated Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
PoH	Proof of History
VDF	Verifiable Delay Functions
DLT	Distributed Ledger Technology
SSC	Special Smart Contract
LWU	Light Weight UniquID

GENERAL INTRODUCTION

The IAM (Identity Access Management) mechanisms for the different networks have been a concerning subject all the way when the internet has got to the public using, especially when it was first used for online banking services access earlier in the 90ties. Moreover, all the systems are build in centralized manner, and need a TTP (TTP: Trusted Theard Party) to secure their access. The genuine issue here, is that the whole framework is built on one central point of failure, this make it vulnerable especially when a Malicious code gets through defense lines and get control over the system, it can control all the key-roles given by that framework. Nowadays the decentralized system is more used due to the limitation of centralised ones.Even this was not enough until the blockchain concept appeared with it's features. This new concept incorporates a tall and solid level of the IAM for decentralized systems, which is way more secure and can be almost impossible to be hacked compared to the current used approach. Beside the evolution and the development of the IT (Information Technology) industries,the IoT technology have emerged with the concerning subject to secure that a gigantic number of devices. In this specific context, systems require more trusted safety techs which can give a high level of security for the users' data and their budgetary resources.As the IAM merge into IoT in the blockchain environment, scalability is served. For the past couple of years the researchers have gone to combine the blockchain and IoT techs, precisely the second generation of it, for its nature of flexibility to go from basic things to whole complex systems. The blockchain technology can provide high level of security. Meanwhile, the community has created different access verification protocols to achieve the main goal ,and get the most excellent combination of the CAP theorem (CAP: Consistency, Availability, Partition tolerance) triangle,this theorem offer scalability and availability to systems. In this work, we going to compared and study multiple open-source access management protocols that secure the authentication access between IoT devices based on blockchain technology. We will gave full attention to one particular studied protocol, by analyzing its main structure and figuring out several miss-combined concepts, to propose an approach that will improve the level of security and scalability of the selected protocol.

The manuscript is organised as follow: the first chapter,we are going to speak about blockchain technology and its basic concepts ,in second chapter,we will mention IAM , IoT and cites some protocols that serve this two elements.Depending on critical standars we will choose three protocols and compare them. From that we proceed to chapter three in which we will select one protocol and find it's points of failure.After that,we will propose improvement for that model

1 CHAPTER : BLOCKCHAIN AND BLOCKCHAIN TECHNOLOOGEIS

One of the most highlighting tech in the information technology field as the researchers address it, the blockchain as the big thing coming since the internet has gone to the public using .become popular since the deploying of bitcoin as a digital currency in 2009. When the white paper has published by Satoshi Nakamoto [1] in the year before, who proposed working model of decentralized peer-to-peer electronic cash system .Plus the big Embracing by the users, in the recent few years have seen high demand for this specific tech. In this chapter, we are going to define the Blockchain technology and its aspects, also we going to mention it characteristics and some fields that use it and explains the big role-play decentrolized system that remain the key of the trustworthy, between his users.

1.1 Definition

The blockchain technology was first proposed and deployed by an anonymous person or group under the name Satoshi Nakamoto, in 2009 [1].Nakamoto developed a decentralized peer-to-peer electronic cash system ,later named "Blockchain", Blockchain includes blocks where blocks are interconnected like a chain. Each block contains information such as block number, the hash of the previous block, a nonce, and transaction information . This chain is called the ledger.Each node in the network has its ledger. Blockchain uses consensus mechanisms to verify the transaction and update the entire ledger. At the time of adding a new transaction in the ledger, all nodes in the network will check the correctness of the information and, after approving, will add the new transaction to their ledger. Each user subscribes to the network by registering a pair of public and private keys on the network. ,is is done by recording a transaction. Each user's keys are stored in their wallet. Miners created the blocks. Miners are nodes in the network, tasked with generating and approving blocks to the blockchain. To generate a block, the corresponding node solves a difficult problem, and the one who solves the problem sooner registers its block in the blockchain. Changing an approved block in the ledger is costly and difficult.

1.2 Blockchain technologies

This section highlights some basic concept of why blockchain can be the best alternative to manage our data credentials and authentication process and that by using hashing,public-private keys and digital signatures.This three elements constitute the foundation of blockchain technology with there cryptographic features make it possible for blocks to get securely linked by other blocks also ensure the reliability and immutability of the data stored on the blockchain.

1.2.1 Hashing

A term like “hash function” can mean several things to different people depending on the context. For cryptography it is a unique identifier for any given piece of content .it’s also the process that converts any size text into an exceptional ciphertext of a specific length. Any small change in input will lead to a whole different hash in the output and this argument is to ensure that any data you send reaches the destination in the same condition that it left you, completely intact and unaltered. Adding to it, it’s one only way which means it is impossible to determine what the input was. This concept is the main part of blockchain technology since it creates the chain and protects its continent. For example, a process of hashing public keys derives addresses on a Blockchain. An Ethereum account is computed by hashing a public key with keccak-256 [2].

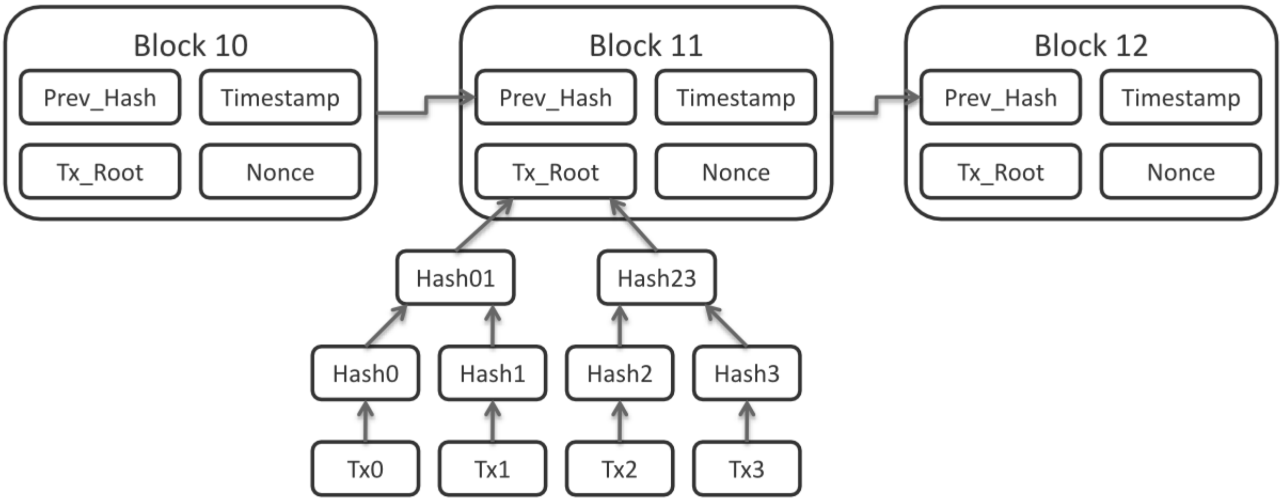


Figure 1 – Hashing

1.2.2 Public key cryptography

Blockchain technology uses asymmetric-key cryptography (also referred to as public-key cryptography). Asymmetric-key cryptography uses a pair of keys: a public key and a private key that are mathematically related to each other. Private must be kept secrete for data cryptographic protection and the public key remains public so it creates the way of communication between others for the private key to encrypt the message and public key to decrypt it. Alternately, one can encrypt with a public key and then decrypt with a private key[3]. The blockchain is build to be distributed and decentralized system so that each node of the network is responsible for keeping its digital ledger copy that holds data in the forms of blocks and transactions to be transferred between the node in a peer-to-peer network. This concept provides the following features in the blockchain : Authentication: only the owner of the private key account can generate transactions from the account.

Integrity protection: data must be protected against malicious modification since transaction or block pass threw numerous node from the sources to a particular node in the network. Identity management: creating a valid account only requires the generation of a private/public keypair and enables blockchain users to remain anonymous[4].

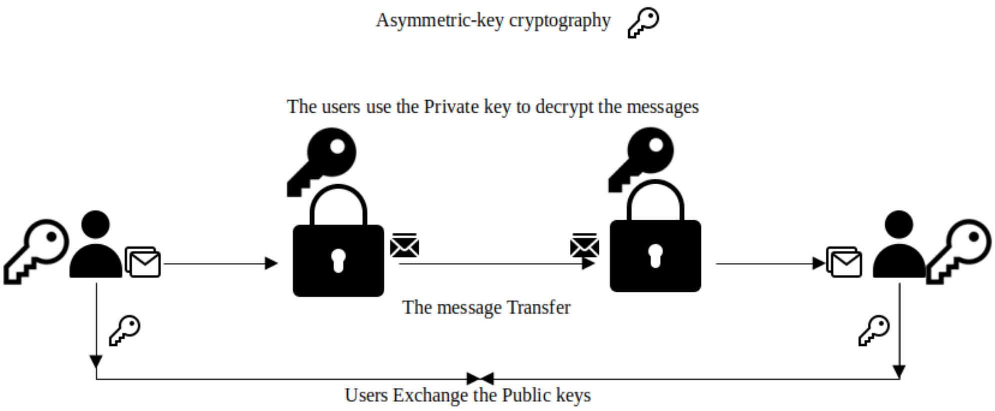

Asymmetric-key cryptography
The users use the Private key to decrypt the messages
The message Transfer
Users Exchange the Public keys

Figure 2 – asymmetric-key cryptography

1.2.3 Digital Signatures

Signatures, in reality, are a way to prove who a person claims to be, it's possible to forge it but hopeless for digital signature since it's based on cryptography so it's a secure way to use it in signing data that are transferred across the blockchain network. This concept ensures the sender isn't a hacker, asymmetric encryption systems provide this service with using the key pairs (the keys are associated with each other through some mathematical relationship) so the operator signed messages using his private key and send them to a destination that is holding his public key (serves as an address to receive messages from others) to verify the data. Generating a key pair is analogous to creating an account on the blockchain, but without having to register anywhere. Also, every transaction that is executed on the blockchain is digitally signed by the sender using their private key. This signature ensures that only the owner of the account can move money out of the account[5].

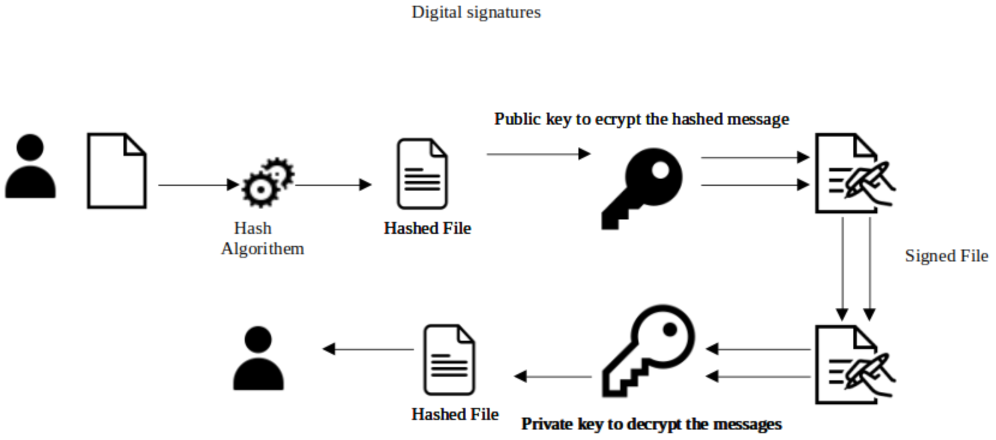

Digital signatures
Public key to ecrypt the hashed message
Hash
Algorithem
Hashed File
Signed File
Hashed File
Private key to decrypt the messages

Figure 3 – Digital signatures

1.3 Blockchain characteristics

There are multiple factors that characterize Blockchain systems. In what follows, we identify some of the important characteristics :

1.3.1 Decentralisation

The decentralization feature allows a group of nodes to be organized in a P2P manner and is responsible for maintaining the network's overall structure, rather than relying on a single governing authority to control and manage network-wide operations [6].

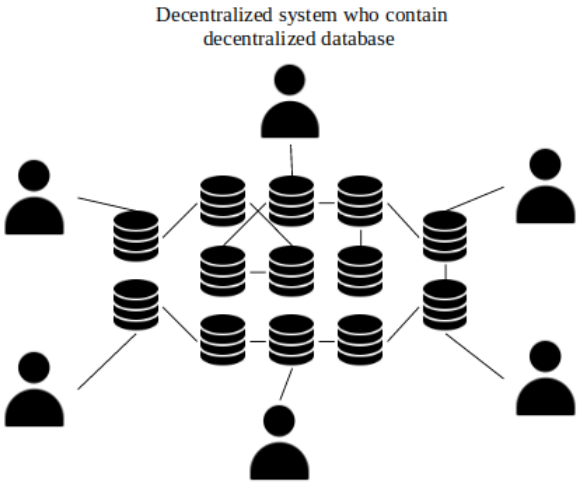


Figure 4 – Decentralized system

1.3.2 Immutability

Blockchain used a distributed ledger that is shared with every node in the network so it makes immutable against any changes in data without the approval of the majority,immutability ensures the integrity and traceability of Blockchain data in a verifiable manner [7].

1.3.3 Anonymity

Anonymity applies to an entity's status as being secret and unrevealed means that no one can access the users' true identity from their behavior or their transactions in the system [8].

1.3.4 Autonomy

Autonomy can be defined as self-governing in any system capable of performing functions independently to achieve specific objectives. The autonomy in the blockchain is represented in giving writes of a user to participate in a self-organizing system and gives them the freedom to verify transactions without involving any centralized third party [9].

1.3.5 Persistency

Transactions recorded in a Blockchain ledger are considered persistent as they spread across the network, where each node maintains and controls its records. As long as the majority of nodes are benign, persistency is persistently retained. Several properties are derived from this characteristic including transparency, and immutability (temper resistance). This transparency and immutability mean that Blockchains are auditable [10].

1.3.6 Validity

Unlike some distributed systems, Blockchains do not require executions from each node. Transactions, or blocks, broadcasted in a Blockchain system would be validated by other nodes. So any falsification could be detected easily. This system consists of three major roles: (1) proposers who propose a value, (2) acceptors who validate and decide which value to be taken, and (3) learners who accept the chose value [11].

1.4 Blockchain Structures

Blockchain is now recognized all over the world, the missing trust layer for the internet, when information has been written into a blockchain database, it's nearly impossible to remove or change it .this capabilities never existed before, with blockchain it makes real, in this section we going to mention the main parts of blockchain :

1.4.1 Blocks

After a transaction being made by blockchain users and submitted to the network, this wouldn't mean that the responsible node for publishing will be added to the blockchain. The transactions would be in the queue of the publishing node and will be added to the blockchain after the node publishes a block.

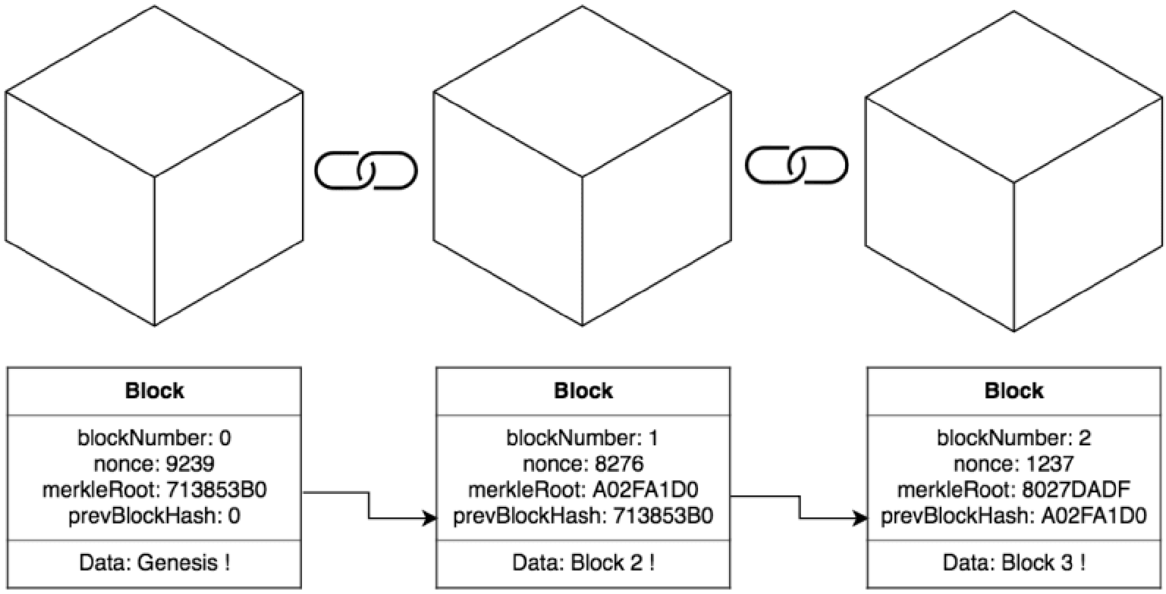


Figure 5 – Blocks

A block includes a block header where the metadata of the block is available and a block body where all valid transactions will be included [12]. The metadata of the block varies based on the blockchain implementation. A general structure of a block can be referred to in (block structure figure) These blocks are chained together through the hash of the previous block and form a blockchain. For instance, any change in data will cause changes in the hash, therefore, losing the chain. Hence it is easy to identify whether a block has been tampered with or not.

1.4.2 Transactions

A transaction refers to an interaction between two entities in the blockchain,auto figure table libreoffice writer in the case of cryptocurrencies, the transfer of bitcoin or any other cryptocurrency from one user to the other is called a transaction whereas in a business scenario changing activities or transfer ownership assets are considered as a transaction. The data included in a transaction generally are transaction input, output, sender's address, sender's public key, and a digital signature [13].In the case of smart contracts, transactions can process then the result is stored in blockchain.to validate a transaction it' must be suitable to the blockchain implementation protocols policies.in addition, the sender has access to digital assets that are transmitted since his the sender of the transaction according to authenticity further the transaction is signed by its sender using private-key and can be verified by anyone using his public key.

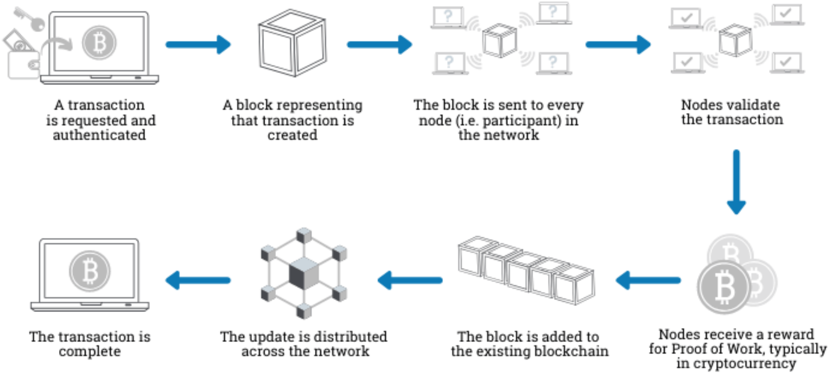

A transaction is requested and authenticated
A block representing that transaction is created
The block is sent to every node (i.e. participant) in the network
Nodes validate the transaction
Nodes receive a reward for Proof of Work, typically in cryptocurrency
The block is added to the existing blockchain
The update is distributed across the network
The transaction is complete

Figure 6 – Transactions in Blockchain

1.4.3 Blockchain network (peer to peer network)

What gives blockchain importance and credibility is the decentralization system applied for the network, like the one supporting bitcoin, is structured as a peer-to-peer (P2P) network on top of the Internet [1].P2P means that the computers participating in the network are all equal peers and that they all provide network services. It's inherently resilient, decentralized, and open, precisely reflecting the core characteristic of blockchain technology.

All the nodes in blockchain are equal with some differences depending on the node roles and functionality they are supporting. For instance, a node could take one or more of the following roles: Routing: Each node in the network includes the routing function (receiving and forwarding messages) since it maintains connections with peers, and validates and propagates transactions/blocks. Maintaining blockchain database: Some nodes maintain a replica of the blockchain/shared ledger and autonomously and authoritatively verify transactions. auto figure table libreoffice writer auto figure table libreoffice writerMining: A set of nodes serve as miners by participating in the process of creating new blocks .

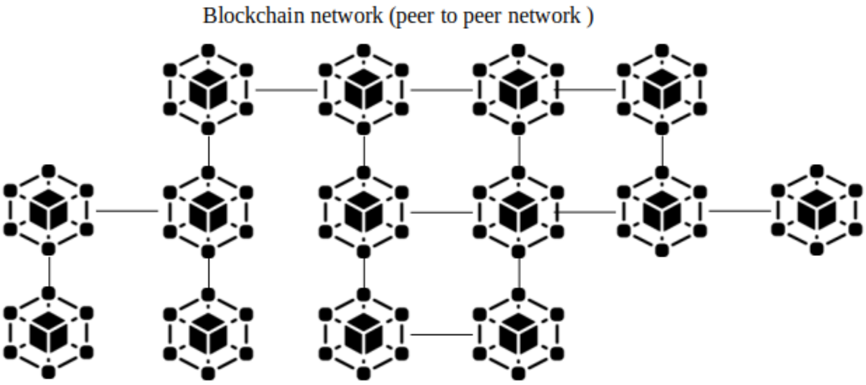


Figure 7 – Blockchain network (peer to peer network)

In addition to mining and routing, these nodes could also maintain a replica of the blockchain. Application-specific functions: Some nodes in the network specialize in running application-specific functions such as certain smart contracts features or digital wallets. Similar to the mining nodes, this category of nodes could maintain a blockchain replica and/or participate in the mining process, in addition to routing and running application-specific functions. Finally, there could be complementary nodes running other specialized blockchain protocols in the network.

1.4.4 The Consensus

The consensus is a mechanism that is to determine the user to publish the blocks. due to the reward offered by publishing block (cryptocurrency) nodes attempt to compete for the prize, here comes the role of consensus, in order to be fair between the user and give everyone his right, the chance to get the reward. Block can be published only with the approval of the majority of nodes, the node whose is responsible for, publishing is called a miner, to achieve this operation he must solve a cryptographic puzzle that requires huge computation and is hard to solve. Once the puzzle is solved it'll be broadcasted to the network for verification as we mentioned earlier and then it will be added to the blockchain[14]. Several consensus models are being used such as Proof of Work (PoW), Proof of Stake (PoS), Delayed Proof of Work (DPOW), Delegated Proof of Stake (DPOS), Practical Byzantine Fault Tolerance (PBFT), Proof of History(PoH).

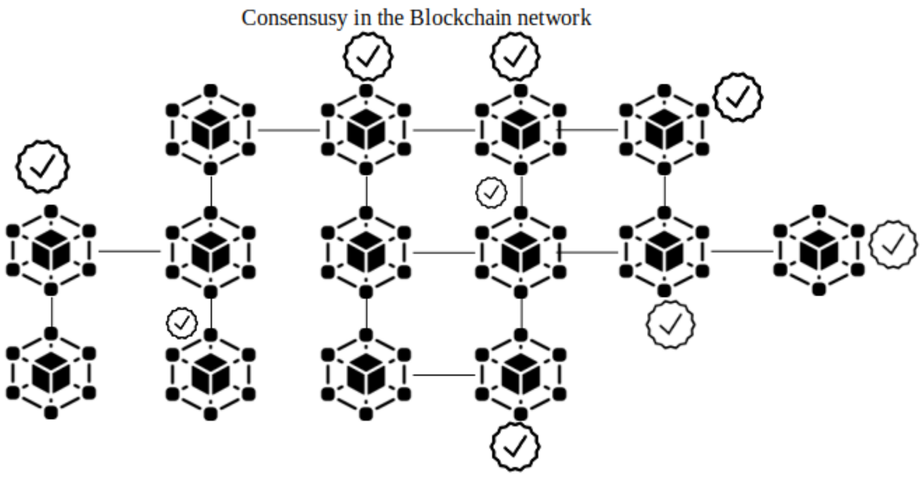


Figure 8 – Blockchain network (Consensusy in the Blockchain network)

Proof of Work (POW)

It was adopted since of introduction of bitcoin in 2009 [1].In PoW, network actors or participants use computational power to win the right of adding new blocks to the blockchain. The node who solves hash puzzles (resulting creation block) which take computational power gets to receive the predefined reward or transaction fees. Miner was referred to the node who make earlier operations and named for similar to miner discovering gold [15]. Anyone can participate in mining but because of the amount of energy-consuming PoW [16], for example, the energy required to run the Bitcoin and Ethereum networks is equivalent to powering 3.5 million and 1 million households, respectively [17].To control the network and get the most fees you need to amass accumulated superior computing assets compared to the combined computing asset of all honest mining entities. This is referred to as the 51 percent of attack [18].Bitcoin, Ethereum, Litecoin, and Dogecoin are cryptocurrencies based on PoW.

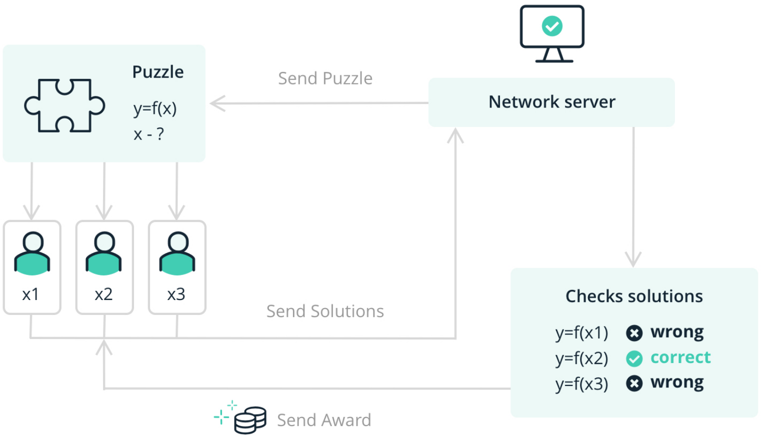


Figure 9 – proof of work

Proof of Stake (POS)

PoS was considered as a solution for overcoming PoW in some parts. In PoS, a participating entity must have some stake (cryptocurrency) in the system to mine or validate block transactions. The benefits depend on how many coins you staking if it's 10 then your profits will be ten percent which means nodes that stake are nodes that create and validate blocks [19].In order to stake you need to provide ownership of a certain amount of stake locked in the network[20]. Subsequently, a pseudo-random mechanism is used to select a leader or block proposer. A committee formed by selecting nodes based on their stake locked in the network decides on the validity of the block proposed by the leader. After it's validated form the block, a vote is made to approve or reject the proposed one, usually two-thirds of the committee size [21]. For 51 percent of attack in this case it's become meaningless because you must own 51 percent of the overall cryptocurrency. Ouroboros [28], Peercoin, Gridcoin, and Nxt are some examples of cryptocurrencies based on PoS.

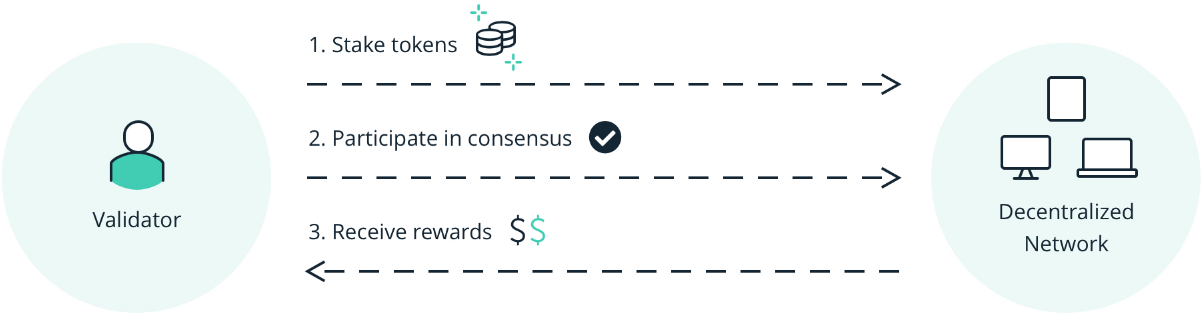


Figure 10 – proof of stake

Delayed Proof of Work (DPOW)

The dPoW consensus protocol is used by Komodo, a multi-chain platform [23]. As the name implies, a multi-chain platform leverages the security provided by a secondary blockchain (in this case, the security from solving hash puzzles in PoW) to secure blocks in the main blockchain. This process is facilitated by 64 notary nodes elected yearly, whose purpose is to write to the PoW blockchain. By doing so, DPoW avoids additional energy consumption and overhead costs. The dPoW consensus protocol utilizes the assigned PoW blockchain to save the Komodo transactions. Apart from being cost-effective, dPoW is also resilient against the 51 percent of attack, as an adversary must attack both the main and secondary chains to be successful.

Delegated Proof of Stake (DPOS)

DPoS is another voting-based consensus protocol that is derived from PoS. DPoS involves an electoral process analogous to a board of directors, whereby board members are limited in number and are elected by the populace. Additionally, they have the mandate of their electorates to exercise their rights. Apart from the amount of staked cryptocurrency, members with voting rights are picked through election and replacement [24]. Wealth staked in the protocol during voting rounds is locked in smart contracts. Transaction validation, new block creation, network operations, and maintenance are performed by the group of elected delegates. These delegates are the block producers (BPs), who are rewarded accordingly for work done. There is also a group of backup BPs who receive smaller rewards as well. For any negative action (such as collusion) or a missed turn, a BP may be voted off the list. The staked wealth or coin in the member's smart contract is frozen or confiscated as a penalty. DPoS mechanism addresses fundamental drawbacks, such as the nothing-at-stake problem, the long-range attack, and the weak subjectivity of the basic PoS system [25]. DPoS is more energy-efficient and has a high throughput

(EOS produces one block every 0.5 s). One of the major drawbacks of DPoS is that it tends toward centralization, and participating members with large stakes in the network can vote themselves into becoming validators. BitShares, Steemit, EOS, Lisk, and Ark are based on DPoS.

Practical Byzantine Fault Tolerance (PBFT)

PBFT is a consensus protocol based on replication between known parties that can tolerate a failure of up to one-third of the parties [26,27]. It is an algorithm for solving a Byzantine fault resulting from a failure in achieving consensus caused by the Byzantine Generals Problem (BGP) [28]. In general, an elected leader (primary node) creates an ordered list of transactions that is broadcast to other validation nodes, who then execute them. After transactions have been executed, validation nodes compute the hash code for the new block which is then broadcast to their peers. If two-thirds of the received hash codes are the same, the block is committed to the node's local copy of the blockchain. PBFT ensures network fault tolerance and allows thousands of operations per second with a negligible increase in waiting time. However, one of the major drawbacks of PBFT is the ability to practically implement the algorithm, due to the enormous amount of calculations required [26]. Tendermint [29], the Diem blockchain [30], Hashgraph [31], and Hyperledger Fabric [32] achieve consensus-based on PBFT.

Proof of History (POH)

Proof-of-history is a consensus protocol introduced by a blockchain project called Solana, this proposed algorithm is to speeding up consensus in the blockchain platform also assured the scalability between the network nodes, with that POH is to remove the bottlenecks caused by PoW, but still achieves the security of decentralization, while maintaining the right balance on honest actors and deterring bad ones. It aims to lighten the load of the network nodes into the processing blocks by providing a means of encoding time into the blockchain platform itself, to reaching consensus over the time of a particular block was mined as much a requirement as reaching consensus over the existence of the transactions in that block. To get critical by the "timestamping" is to tell the network that transactions took place in a particular sequence of the blockchain. In detail, PoH uses a newer cryptographic concept called Verifiable Delay Functions(VDFs.) A VDF can only be solved by a single CPU core applying a particular set of sequential steps. No need to parallel processing, in this method is not allowed, so it's easy to define exactly how long it takes to apply those steps. Therefore, the passage of time is evident. With all of that being said the platform that implements the POH consensus algorithm is more decentralized due to the low cost or the fees of the participation, which allows more entities to participate easily. It is also much easier for participating entities to verify whether the block is legitimately added to the platform. A Verifiable Delay Function requires a specific number of sequential steps to evaluate, yet produces a unique output that can be efficiently and publicly verified. The implementation uses a sequential pre-image resistant hash that runs over itself continuously with the previous output used as the next input as shown in the figure “. the count and the current output are recorded and added Periodically, This concept guarantee that real-time has passed between each counter as it was generated and that the recorded order each counter is the same as it was in real-time.

1.5 Blockchain types

Blockchain technology is being adopted by various industries and can have numerous applications. It can be used in different domains in different ways; the following are the types of blockchain networks that can be selected by the users based on their requirements. All these types of blockchain are different from one another, but they have commonalities such as peer-to-peer connections, distributed decentralized network structure and block-based time-stamped transactions.

1.5.1 Public blockchain

A public blockchain is a permission-less distributed network that does not have any types of restrictions. Anyone who wants to get access of the blockchain can join the network and become an “authorized node”. After joining you will have the right to perform transactions and verifiy the blocks of data ,as a public blockchain there common used in cryptocurrencies ,its secure but users need to respect protocols strictly ,they can trust blockchain with out knowing the others , but since it ‘s has proof-of-work to ensure the trust ,it’s size is usually very large, that makes it more secure because larger the chain, more distributed are the records.The ledger of all racords is open and available to all the authorized nodes that achieves transparency.All of throw we mention benefits ,there are few desadvantages including the slow speed of processing transactions as long as the large number in the network ,which means more time to verificate it that also makes it difficult for adding more nodes to the network and hence the scalability is also a concern.In addition amount of energy need to be considered in the network.Examples of Public Blockchain are Bitcoin, Litecoin and Ethereum.

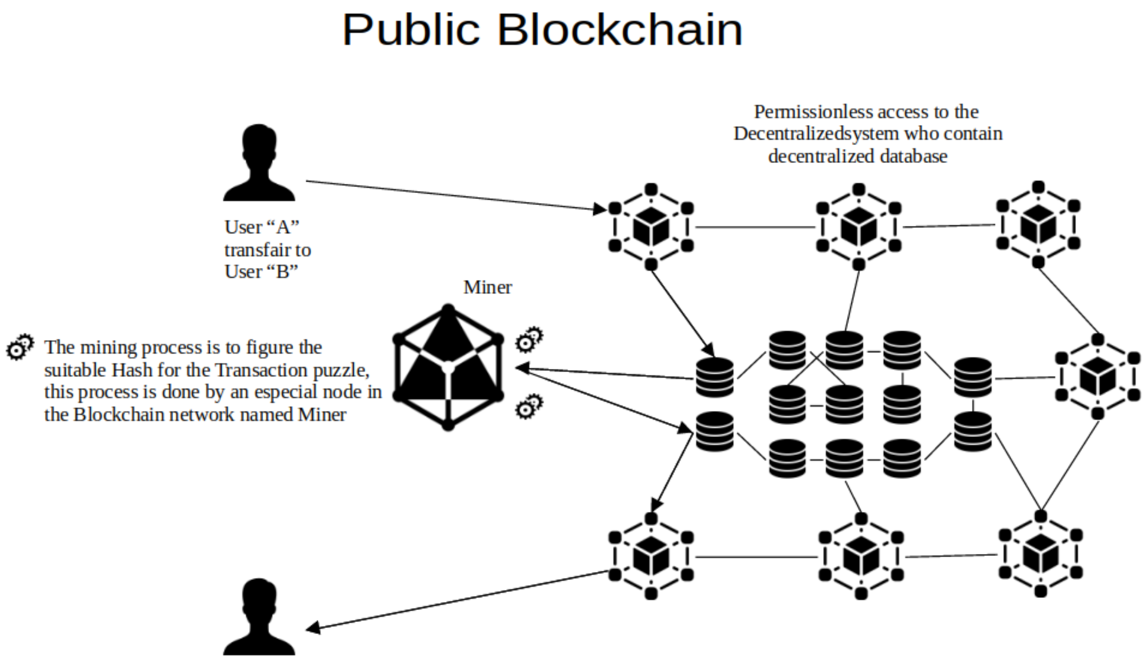

Public Blockchain
Permissionless access to the Decentralizedsystem who contain decentralized database
User "A" transfair to User "B"
Miner
The mining process is to figure the suitable Hash for the Transaction puzzle, this process is done by an especial node in the Blockchain network named Miner

Figure 11 – Pablic Blockchain

1.5.2 Private blockchain

A private blockchain is a permission-based distributed network that has a few restrictions and only works within a closed network. These blockchains are usually preferred by organizations that want only the restricted members to access and participate in the network. And no one from outside the network can access the information [33]. Such networks can be used for managing identity, ownership management of assets, managing supply chain, etc. in this case number of nodes is limited by the company so the time process will be fast with possibilities the surpass than sound transaction per second, which makes it flexible and scalable. this type of blockchain is private so only trustworthy members are being added, security decreases and the breach is more possible. Examples of Private Blockchain are Corda, Fabric, and Sawtooth.

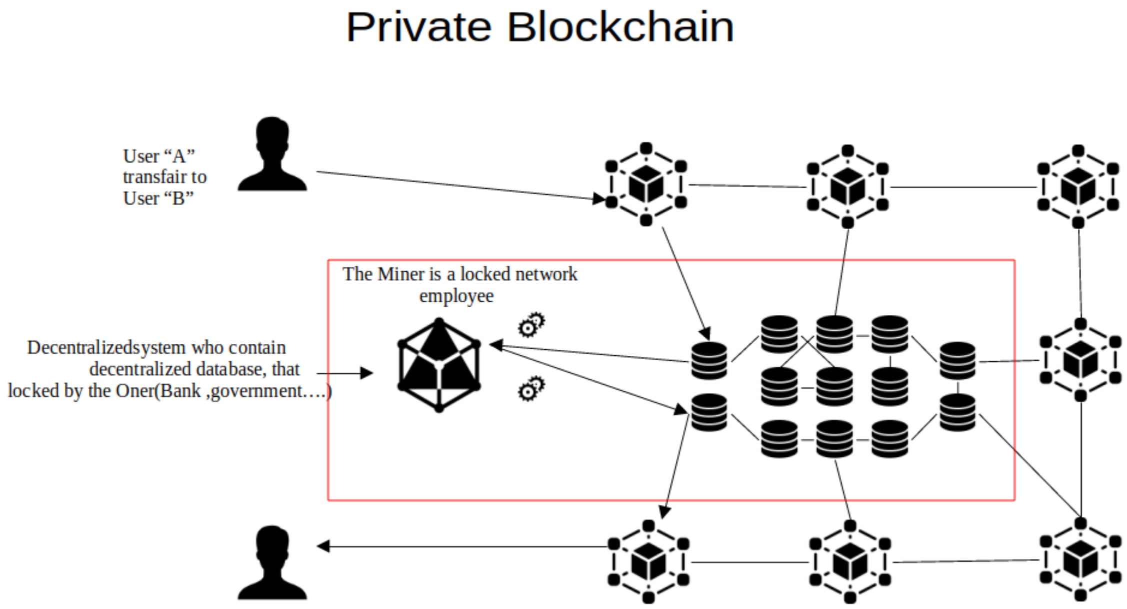

Private Blockchain
User “A”
transfair to
User “B”
The Miner is a locked network
employee
Decentralizedsystem who contain
decentralized database, that
locked by the Oner(Bank ,government….)

Figure 12 – Private Blockchain

1.5.3 Consortium blockchain (hybrid)

It is a type of blockchain that is controlled by some of the nodes. In this, a group of representatives of several organizations called “consortium” come together to make the decisions for the betterment of the network. These networks are used mainly in the banking sector and government organizations. In such networks, some of the nodes are responsible for controlling the consensus procedures while some of them are allowed for participation in the transactions. It might be seen as a combination of a public and private blockchain, as the network consists of multiple nodes like public blockchain and the restriction on these nodes like private blockchain [34]. Examples of Consortium Blockchain are Energy web foundation and R3.

1.6 Blockchain evolution

Blockchain technology continues to evolve its underlying architecture through a sequence of phases or evolution for developing a variety of applications, as illustrated in Fig. 2. In each phase, Blockchain technology identifies the various inherited challenges and has proposed splendid solutions to overcome them. To this end, the Blockchain evolution phases (1.0 to 4.0) are designed to provide a variety of lookouts, such as functionality, features, strengths, challenges, and security issues. Version 5.0 is currently under development, and research communities are working on it to improve its functionality for different business models. Table 2 summarises the different Blockchain generations (from 1.0 to 5.0) with respect to their applications, consensus mechanisms, and features for each generation.

1.6.1 Blockchain 1.0

Following this, the first application of Blockchain technology was a very famous cryptocurrency named Bitcoin proposed by Satoshi Nakamoto in 2009 under the first evolution phase called Blockchain 1.0 [1]. The Bitcoin concept is very famous with the most commonly used terms on the internet is “Cryptocurrency” [35], “Cash for the internet” [36], and “Internet of money” [37]. Bitcoin used the concept of distributed ledger technology to transfer money without the need for a trusted third party. On the scene, this technology has become a fast and rapidly growing digital payment system adopted by most financial organizations around the globe [38]. At present, Bitcoin is not just a currency system; it also changed the economic models and working structure of different organizations, for example, government sectors [39], banking [40], and accounting. For security purposes, Bitcoin utilizes the immutable feature of distributed ledger, to ensure the integrity of recorded transactions and to guarantee that no one can change or modify the transactions. In addition, advanced cryptography protocols, such as hashing algorithms and digital signatures, provide the authentication trust and privacy of users in the Blockchain environment [41]. However, at present, in Blockchain 1.0, there are a few issues about computational cost, extended waiting times, lack of inter-operability, and versatility which are recognized as major barriers to wider adoption.

1.6.2 Blockchain 2.0 :

Blockchain technology is considered a fast-growing technology that has been revolutionized by continuous improvements and rapid progression in the distributed ledger to develop smart applications for society and businesses. Blockchain version 2.0 comes with the concept of smart contracts, small executable user programs which run in the Blockchain environment called Ethereum Blockchain to carry out different automatic tasks and make valid decisions [42]. The key features of such programs are that they execute automatically, based on defined logic and conditions in them, for example, time, performance, the decision, and verification policies [43]. It is equally important to describe here that these small programs (or contracts) run with the autonomous identities of users to protect personal information in the Blockchain network [44]. The advantage of smart contracts is that they can possibly reduce execution and verification times without requiring additional system resources to perform computation. Further, it can also allow the users to write smart contracts in a transparent way which prevents different fraud and hazard problems [45]. To summarise, the Ethereum Blockchain [46] is the most prominent feature of Blockchain version 2.0 in which the users are allowed to write and execute smart contracts in a secure way.

1.6.3 Blockchain 3.0 :

The major limitations found in previous Blockchain versions (1.0 and 2.0) are that they mostly rely on the public Blockchain network and cannot store a massive amount of data in the distributed ledger of Blockchain technology. Bitcoin and Ethereum are open to everyone and the data are produced and recorded on the Blockchain daily. Therefore, the primary need is to store a large amount of data in different storage places, such as data servers and clouds [56]. For this purpose, a new version of the Blockchain has proposed a Blockchain 3.0 in which the decentralization concept is utilized to store a huge amount of data and to legally support a wide variety of communication mediums [48]. Indeed, the code in decentralized applications supports multiple servers to run and compile it; whereas a single server with limited storage only runs limited applications [49]. The advantage of Blockchain 3.0 is that it allows the developer to write the code of applications in any language since it requires system calls to communicate with the decentralized system for the execution of the program. Apart from the disadvantages, there are various security challenges faced by these decentralized networks such as authentication, authorization, and access control of users and their data. The privacy of users and their transactions in a decentralized network is also a challenging task, along with other security requirements [50]. To illustrate the concept of Blockchain 3.0, the developers of smart contracts introduced Genaro [51], a first Turing machine-based public Blockchain, which permits the users to write and deploy native smart contracts in decentralized storage systems with the support of different network modules in the one place.

1.6.4 Blockchain 4.0

With the completion of a successful journey made by leading Blockchain versions (from 1.0 to 3.0), the new version of Blockchain 4.0 is presented to address the industrial challenges and limitations of real-world applications. Blockchain 4.0 is a new generation or version of Blockchain technology that aims to introduce Blockchain into the industrial world and make it practical for developing and running real-world applications in a secure and decentralized way. The new version also enables us to propose new solutions and fills the gap between business and information technology industries [52]. Furthermore, Blockchain 4.0 enables the industry and business sectors to transition their entire structure and processes (or parts of them) transparently, to stable, self-recording applications built on a decentralized, distributed, and immutable ledger. As Industry 4.0 is known as a revolutionary technological wave for the interconnectivity between people and machines, it provides substantial industry growth and productivity change that positively affects both the human quality of life and the environment [53]. The convergence of Industry 4.0 and the Blockchain 4.0 generation creates a joined paradigm based on trusted networks that eliminate the need for a third party. Individual manual processes are transformed into linked systems using automated, autonomous systems, which are also underpinned by Blockchain technology. This convergence is primarily centered on the use of Blockchain features such as public ledgers and distributed databases, as well as the implementation of smart contracts in industry processes to remove the need for paper-based contracts and to control the network through consensus [54]. Moreover, introducing Blockchain version 4.0 into Industry 4.0 aims to achieve transparency in the industrial processes from planning to implementation, and to establish the relationship between industry policies and underlying Blockchain features [55]. There are a few examples of Industry 4.0 that have recently adopted this new version into their business processes: financial services [56], IoT [57], Transport and Logistics [58], SG [59,60], and eHealth [61].

1.6.5 Blockchain 5.0 :

Although Blockchain technology is relatively new, it has advanced dramatically. It is now used in a broad range of industrial sectors, including banking, healthcare, IoT, and supply chain management. After achieving considerable success in earlier versions, Blockchain 5.0 is designed to serve the needs of the next generation business peoples' by formalizing and standardizing digital lifelines. Therefore, it is becoming extremely important to have Blockchain 5.0 in today's world. The aim of Blockchain 5.0 is to concentrate on the integration of AI and DLT to develop the next generation of decentralized Web 3.0 applications to achieve data privacy, security, and interoperability. By making this option, a project called ”Relictum Pro” is well on its way to achieving success in the new age of Blockchain technology, which is characterized by Blockchain 5.0. The “Relictum Pro” Project has advanced technology to use Blockchain 5.0 to build virtual channels on this dedicated network. As a result, there is a significant increase in transfer rates and the introduction of a seamless system with smaller block sizes and faster transactions [62].

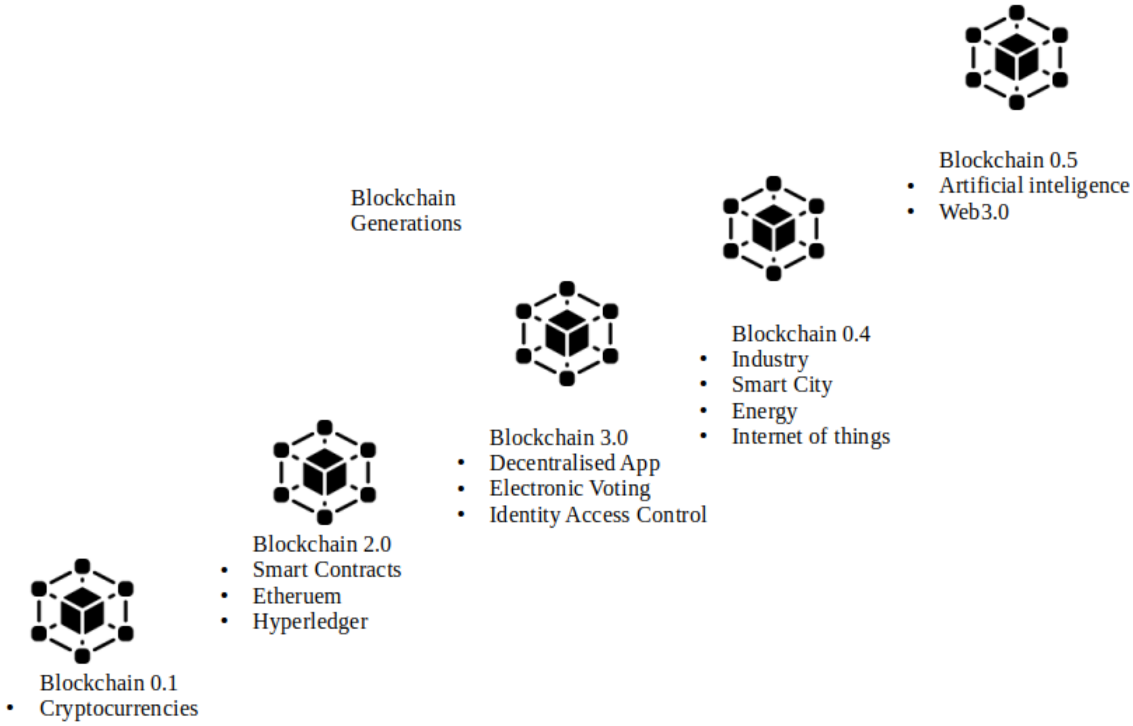


Figure 13 – Blockchain

1.7 Blockchain application areas

Blockchain is a platform for maintaining the transactions and records that can be used by any application domain. It is a transparent way of protecting and securing the data and keeping it indestructible. Since the blockchain is a distributed network, the data is broken into pieces and distributed among all the nodes of the network, and hence no one can tamper it. This has made the blockchain the hero and is being adopted by several industries to make their business more secure, cheaper, and faster. A few of them are depicted graphically in Figure 5, and discussed in this section below:

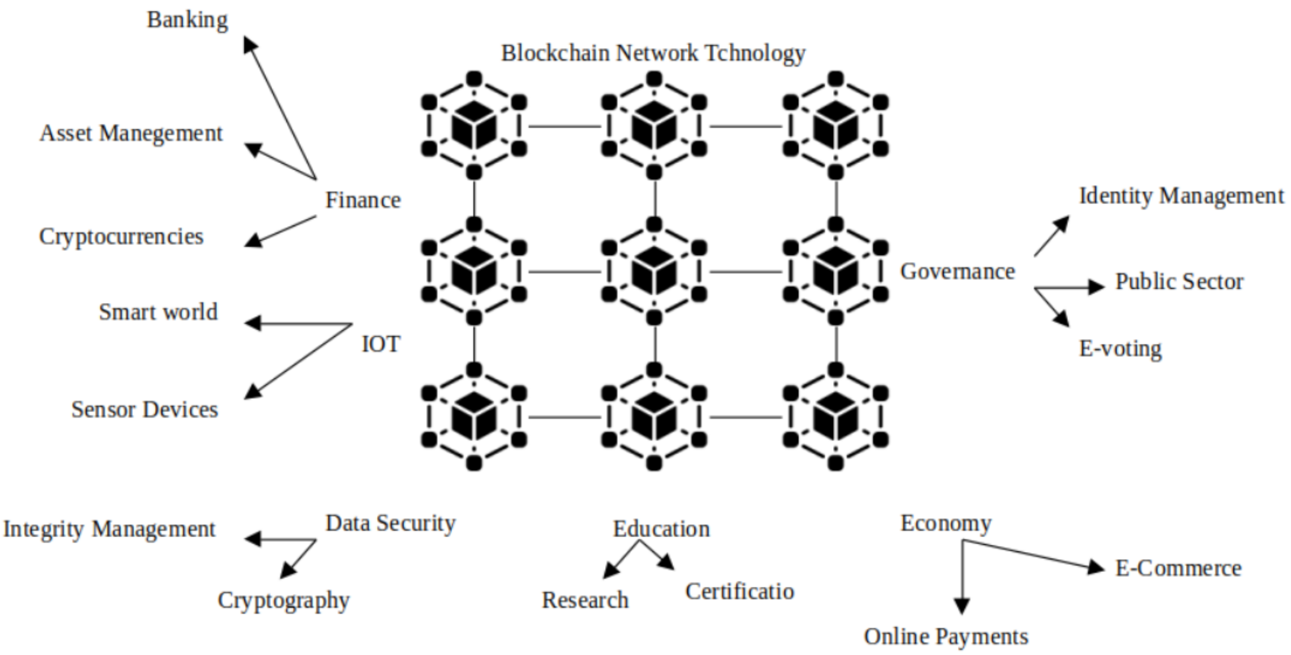


Figure 14 – Blockchain Application Areas

1.7.1 Crypto Currencies and Finance

Blockchain technology is being used in various financial areas nowadays including banking, settlement of assets, prediction marketing, etc. [63]. If we talk about the banking industry, thousands of transactions take place every second and involve money and other assets, this makes the blockchain an ideal choice for this sector. The blockchain can be beneficial for banking in terms of storage, speed as well as electricity consumption [64]. Blockchain offers a variety of applications in finance industry like loan management [65], digital payments [66], financial auditing [67], banking services, crypto-currencies etc. [68,69]. Blockchain provides a secure and safe way of money exchange and allows the user to work on a transparent platform with a very low operational cost. It also eliminates the need for any intervening party that makes it cheaper because managing all the mediators is quite costly. Furthermore, with more and more persons in between means more vulnerable and error-prone the system is, so blockchain eliminates all these vulnerabilities from the finance network.

1.7.2 Education and Innovation

Education is another area in which the blockchain is making progress and several researchers are being conducted to promote online education and training [70,71].

The blockchain networks are known for their immutable record generation process that might help in the education and development sector to keep a track of all the activities and researches across various learning institutions and research organizations [72]. The blockchain could also be used for keeping the record of the courses studied by the students and the degrees and certificated issued to them [73] so that no one can generate or show any fraudulent certification or degree. It can also help in carrying out the research in a protected manner, as one can use the blockchain network to keeping and maintain the intellectual properties. Since the network itself, on the basis of the timestamps, verifies the blockchain, the intellectual property would be safe and maintain its origin by itself. The researcher can also work on this platform to keep their research safe and maintain its integrity throughout the entire process. In regard to research papers, a blockchain platform is proposed in [74], that keeps a track of the contributions made by the authors on the basis of the editing.

1.7.3 Healthcare Welfare

The Healthcare industry is one of the industries that might have the most possible use cases of blockchain in order to develop a transparent infrastructure for storage and analysis of healthcare data [75]. It can also help in the development of new medicines and also a less costly healthcare diagnosis. Several types of research have been conducting in this area focusing on secure data management [76], medical image sharing [77], digital contact tracing [78,79], and general medical records storage [80]. Apart from the patient diagnosis and the medical records, the blockchain can also help in analyzing the data generated by intelligent devices, tracing the origin of the drugs, records of side effects of a particular drug, etc. Moreover, the pharmacies could also use the blockchain platform to keep the supply chain information traceable among the producer, consumer, and seller [81]. Blockchain can also improve the state of the art of the insurance sector, from putting the quotation to claiming the expenses; the blockchain can provide a transparent way and reduce the fraudulent requests.

1.7.4 Security Privacy

The data available today in any sector is huge in amount and heterogeneous in nature and demands security and privacy. And using blockchain technology, the security aspect can be enhanced [91], and the system can become more scalable and flexible. One of the main aspects to maintain security in the blockchain is to use cryptography and secure the transactions among the users. Since the blockchain uses the hash values of parent nodes to connect the new blocks and also each block has the timestamp along with the encrypted data, it becomes impossible for the hacker or any outsider to break into the network and hence, the security and privacy are maintained. Several blockchain-based platforms are already available in the market today like is Namecoin [83] and Alexandria [84] that gives privacy, efficiency along with censorship resistance.

1.7.5 Business Economy

The potential of the blockchain platform can be utilized in the field of managing business processes using blockchain-based communication. The blockchain can be exploited in managing the supply chain of the business products, satisfying the supply and demand [85], automatic payments using verifications [86], etc. The blockchain can be used in e-commerce for commercial marketing [87], verifying product ownership [88], and identifying fraudsters [89]. Apart from the electronic purchase, the physical vending machines can also be managed by the blockchains, by maintaining the correct and updated information regarding the availability of products. Another aspect of e-markets is online payments, which can also use the blockchain platform to work properly. The rating of sites and products also plays an important role in e-business, and blockchain can be used in that direction as well. This rating procedure is known as a reputation system that can be done either by using a scale of 1to5 or by writing the reviews in human language [90].

1.8 Blockchain Limitations

As is known as scientific wealth, the technology that will change the history of IT also have to analyze for malfunctioning and disadvantages and it seems, it has some weak points, we indicate some of them :

1.8.1 Loss of Privacy

In a blockchain, a considerable amount of privacy is maintained by using a public key cryptography mechanism in transactions to keep the user identity anonymous. However, transactions anonymity cannot be assured by blockchain because the identities of all transactions and balances for each cryptographic key are publicly accessible. Thus it is possible to recognize the user by keeping track of the transactions.

1.8.2 Consensus Protocols

Blockchain is a technology based on a distributed network, that decentralized structure needs a consensus procedure to get all the nodes on the network to agree on common rules, in order to use them and get effective resultant.

1.8.3 Selfish Mining

It is a strategy for miners to secretly keep their blocks without publishing them until some of the conditions are achieved, in this situation, miners will have their privates chain that makes honest miners would have wasted their resources on a chain that is going to be abandoned so instead selfish ones may be rewarded with higher incentives. Likewise, blockchain is susceptible to many attacks like Sybil attacks, Double spending [91], 51 percent of attacks, and so on. Nevertheless, Blockchain has been transforming both the industry and academia with its distinct properties like decentralization, anonymity, integrity, and transparency. Even though blockchain has not reached its maturity it continues to suit applications of different domains globally.

1.9 CONCLUSION

In this earlier section we spoke about blockchain technology, we defined blockchain, its characteristics, and the main structure that create this technology without forgetting its evolution throw time furthermore it's applications, that we clarified the image of this concept so we can use its features in the next sections.

2 CHAPTER: COMPARATIVE STUDY OF IAM PROTOCOLS IN IOT

2.1 Introduction

After getting to know the technology, the question is where do IAM and IoT get involved in our topic, this is what we get to know incoming section, besides we will talk about some researches that took advantage of the blockchain technology and merging it with IoT technology, from that perspective we are going to choose some of this articles including IAM with the consideration of some critical standards that classify these protocols throw our study, as a result, we select one of them, which we going to analyze and get some point of failure and suggest the improvement in the last section.

2.2 Identity Access Management

The internet of things is having a profound impact on the IAM market, as IoT devices become users themself this proposed for IAM to exploit here technology to be effective in the IoT field, in such a scenario, every interaction within IoT entity, building smart home or city environment requires authentication to confirm of the user or device that want to access the resources, and authorization to decide how much info you can access to, here comes identity access management that based on blockchain to reduce the possibilities for attackers to get or tempered with data in our network areas. In this context, as we consider IoT devices as users that interact with our system as the immigration of IAM to the internet of things is required[92].

IAM CONCEPT

For many years the security breaches was a failure to manage identity and access to different online banking and corporate web sites , for that reasen fisrt by Poor management of access rights that leads to unauthorized use of access plus Excessive access rights accumulated over time through changes in jobs and roles together with Poor implementation of access controls and that also taks to weak of layered access management defense in applications, systems, and networks that allows for rapid spread of attacks .

2.2.1 IAM Definition

IAM is an essential function for protecting the privacy of information, enhancing user experience, enabling accountability, and controlling access to an organization's assets. Its the collection of processes and technology used to manage these digital identities and the resource access provided through them. IAM is best described by defining its core components, Identity management, and Access management.

Identity management

refers to the people, processes, and technology required to manage their digital identities and profiles. Identity management functions include the following:

- Establishing unique identities and associated authentication credentials.

- On-boarding these identities into target applications, systems, and platforms.

- Provisioning and de-provisioning.

- new user accounts.

- Managing identity data and credentials.

Access management

refers to the processes and technology used to control the access to specific information assets provided to a specific identity. Entitlements are a set of attributes that specify the access rights and privileges of an authenticated identity. For example, security groups and access rights are entitlements. Roles, a logical grouping of entitlements, are a defined set of job functions that can be consistently associated with a defined set of access rights. With these definitions in hand, typical functions of access management include the following:

- Providing the capability to request specific entitlements and/or roles.

- Implementing workflow processes for approving the granting of entitlements and/or roles to an identity.

- Providing the ability to modify or remove the entitlements and/or roles assigned to a user.

- Managing the association of entitlements to roles.

- Associating entitlements and roles to job functions.

- Providing the ability to review, remove, approve, and certify the entitlements and/or roles assigned to users.

- Providing the ability to review and audit historical access associated with an identity.

Identity and credential

Identity refers to the set of characteristics by which a user (i.e., a person, system, or application) is definitively known. In this framework, identity is represented by an identity profile that is the combination of a unique identifier by which a user is unambiguously known and the set of identifier attributes that further describe the user. Associated with the concepts of an identity and credentials are activities performed to manage identifiers and credentials throughout their life cycles, namely:

Generate

The processes, standards, and tools associated with the creation of an identifier, identity profile information, and credentials. Register The processes, standards, and tools used to associate an identifier, identity profile information, and credential with a system.

Proof

The processes and tools used to perform identity proofing; that is, validating an identity using authoritative data sources and identity profile data with sufficient information and evidence. This is to uniquely identify persons as having the identity they claim.

Store/update

The processes, standards, tools, and repositories associated with the reliable storage and maintenance of credential and identity profile data.

Reset

The processes and tools used to disable a forgotten credential and establish a replacement of a forgotten credential.

Expire/renew

The processes, standards, and tools associated with the automatic suspension and reestablishment of a credential after a specified duration.

Recover

The processes and tools used to delete a lost or stolen credential and establish a replacement credential. Revoke/dispose: The processes and tools used to suspend or disable a credential, typically due to suspected compromise.

Other important concepts associated with identity and credentials concern the availability of the attributes comprising the credential and identity profile and the reliability of that data:

Availability

A measure of the accessibility of identity profile data upon which other components of the IAM solution rely.

Federation

The ability to pass a user's authenticated identity and/or entitlements across organizational boundaries to a relying party, platform, or application. Identity and credential quality A measure of the accuracy of the identity profile and credential data.

Access

Access refers to the permission to use a protected system or application to create, read, update, and delete information. In the framework, access includes the processes and tools by which users request and are granted or denied the rights (or entitlements) to access protected resources and the grouping of entitlements into roles. The framework subcomponents related to the management of accounts and fine-grained entitlements (or rights) reflect the common life-cycle phases associated with access management, including:

Request and de-provision

The process of requesting and approving access on a target system, application, functionality, or resource for a user (person, system, or application). This includes the processes and tools for routing the request to the appropriate approver, registering their decision, and forwarding the request to the next stage of processing based on the actions of the approver.

Provision and deprovision

The process of granting access on a target system or application to a user and/or the revocation of access to systems and applications for a user (person, service, or application). Deprovisioning may be triggered due to various reasons such as termination of employment, transfer to a new role, or sun-setting an application.

Enforce

The process that ensures the implementation of access decisions (authentication and authorization) within and across systems and applications for a user (person, service, or application). Authentication is the enforcement mechanism whereby systems securely identify their users. Authorization, by contrast, is the enforcement mechanism by which a system determines what level of access a particular authenticated user should have to target resources controlled by the system. Once the identity is recognized and validated, the application will authorize the user to perform functions in the application based on the access rights associated with the user identity. For example, an application might be designed so as to provide certain specified individuals with the ability to retrieve information from the application but not the ability to change data stored in the back-end systems, while giving other individuals the ability to change data.

Review and certify

This process includes determining the person responsible for certifying the access, routing the access certification request to the appropriate person, confirming that all associated access rights are appropriate for a specific individual in his or her current role, and revoking all access from the user that is discovered to be inappropriate.

Reconcile

The process of detecting and correcting discrepancies between approved access and actual access to systems and applications. Periodically, the target systems and applications have to be reconciled with the centralized repository to detect any unauthorized changes and inconsistencies.

Report and audit

The process of logging transactions, enabling audit trails, and providing a mechanism for authorized users to develop customized reports.

2.2.2 Authoritative Sources

This component of the IAMF focuses on the creation and maintenance of an inventory of an organization's IT resources, roles and rules repositories, entitlements and credential repositories, application inventories, and HR information repositories that are key components of the IAM ecosystem. Key concepts and definitions in this component include the following:

Identity repository

Identity repositories represent, store, and manage identity and profiling information and provide mechanisms for their access. Identity repositories are often implemented as an LDAP (The Light weight Directory Access Protocol) accessible directory, metadirectory, or virtual directory; a database; or identities contained within an operating system. Information on policies governing access to and use of information in the repository is generally stored here as well. IAM products and services on the market today provide one or more of the above components and target different types of users and contexts, including ecommerce, service providers, enterprises, and government institutions. Entitlements repository or entitlements data warehouse An entitlement repository is a system that houses the privileges granted to users over time and records access requests, approvals, start and end dates, and the details related to the specific access being granted. This data can be used when auditing access and determining whether access activities were approved or performing user entitlement reviews, entitlements analytics, or risk scoring.

Roles and rules repositories

Roles are a construct used to aggregate common patterns of entitlements into a single object for ease of management, provisioning, deprovisioning, and entitlement review. Roles and rules can be maintained within the entitlement repositories or as a separate repository.

Roles are typically defined at the following levels:

- Enterprise roles are groupings of basic entitlements granted to all users in a specific category such as employee or contractor.

- Business/functional roles are entitlement groupings associated with a particular job function or which are applicable to all members of a business unit or job title.

- Application roles are predefined entitlements or entitlement groupings within a single application.

Rules define the logic that a system uses to make access decisions or execute transactions. Rules are enabled through complex Boolean operations, an interpretive language, or a scripting language that can be executed as part of a runtime process that dynamically determines outcomes based on attribute values. Rule-sets are typically defined in the configuration modules of a system such as an access review system. Examples include definitions of segregation of duties (SofD) conflicts at entitlements level, roles level, application level, transaction level, process level, and organizational level.

2.2.3 Administration and Intelligence

The administration component of the framework refers to the processes, applications, and tools used to manage and maintain elements of the IAM solution. These systems can include request, approval, and provisioning sys- tems; review and certification systems; reconciliation systems and tools; authentication and authorization systems; reporting and monitoring systems; and authoritative sources. The intelligence component of the framework refers to the processes and tools used to perform analytics targeted at IAM data such as identity and entitlements, user activity, or risk event data. Other key concepts associated with administration and intelligence include the following:

Identity analytics

The discovery and analysis of meaningful patterns in identity and entitlements data. This is especially valuable in determining outliers of access that rely on the simultaneous application of statistics and programming for data visualization to communicate insight.

Logging and monitoring

The standards, processes, and tools associated with the capture, aggregation, correlation, and analysis of IAM solution component audit data.

Reporting

The ability to generate and distribute information intended to provide insights into the administration and operations of the IAM solution components to various constituents.

2.3 Internet of Things concept

Internet of Things (IoT) is one of the most widely used IT domains that have gained huge popularity in the past few years. It is estimated that the number of devices connected to the IoT is going to increase with time. The implication of IoT has not just remained restricted to smart devices and smart homes, in fact, it is going to cover almost every possible industry at a very large scale. And in the future, the world will become a densely connected network. The main security areas of IoT are the transactions and connections among the devices, IoT can be merged with blockchain for safe and secure transactions, and because of its decentralized nature, there would not have any single point of failure that would cause the loss of personal data [93]. The integration of IoT and blockchain would return good more trust among the parties; faster transactions because of the distributed nature and require no intermediary that would give a low-cost system.

2.3.1 IoT definition

The definition of the Internet of Things (IoT) is evolving so there is no common definition by worldwide users, but what is share in terms is being multiple objects that interact with each other to exchange data and make a better version of daily lives. The “Thing” in IoT can be any device with any type of sensor embedded with the ability to collect data and transmit it across the network without manual intervention. The technology embedded in the object helps to interact with internal states and the external environment, which in turn aids in the decision-making process. The Internet of Things (IoT) is a framework in which all things have a representation and a presence on the Internet. More specifically, the Internet of Things aims at offering new applications and services bridging the physical and virtual worlds, in which Machine-to-Machine (M2M) communications represent the baseline communication that enables the interactions between Things and applications in the cloud. This is defined by IEEE communication magazine. Oxford Dictionaries provides a summary definition that calls the Internet an element of IoT: “Internet of things (noun): The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data” [94]. As a simple explanation, IoT is a giant network with connected devices. These devices gather and share data about how they are used and the environment in which they are operated. It’s all done using sensors, sensors are embedded in physical devices .it can be your mobile, phone, electrical appliances, and everything that you come across in day-to-day life.

2.3.2 How IoT works

For Iot as we mention earlier ,the basics element are devices and network that bind them to create smart system with self interaction ,in the contexte of iot devices hardware can be classified into general devices and sensing devices ,the general devices are the main components of data hub and information exchange,they are connected either by wired or wirless interfeaces home appliances are classic exemple of such devices ,the sensing devices on the other hand include sensors and actuators ,they messures the tempirature humidity light intensity and other parameters these iot devices are connected to the network with the help of the getway ,theses gateway or processing nodes process the information collected from the sensors and transfer it to the cloud , the cloud act as both storage and processing unit ,actions are performed on the collected data for further learning and inferences wired and wirless interfaces like wifi ,blutooth ,gsms, and so on are used to provide connectivity to ensure its ubiquity applications need to support a devese set of devices and communication protocols from tiny sensors capable of sensing and reporting the desired factor to powerful back-end servers that are utilized for data analysses and knewledge extraction .

2.3.3 Architecture of IoT

While accepting that various IoT architectures exist, they are classified as conceptual, domain-based, or industrial. As previously stated, the focus of our research is on layered-IoT systems and industrial designs. Before being integrated and performing as a system, each layer's address points must first be separated. This methodology assists in the management of the system's complexity. Because of the integration of numerous types of technologies, devices, objects, and services, IoT scenarios are extremely complicated. The main research created layered architectures ranging from 3 to 7 layers, which are made up of the IoT platforms' fundamental building components,varying from the basic to the end-to-end solutions. Gubbi et al. proposed a three-layer architecture as an early IoT paradigm. Perception is the base layer, which includes sensors and actuators as things, cloud is the information processing layer, and the third tier is the application layer, which allows users to interact. The four-layer architecture is completed with the addition of a business layer [95].Furthermore, A. Al-Fuqaha et al. [96] define IoT architecture as a five-layer model built on middleware layers. Service composition, service management, and object abstraction are all part of the middleware layer. There's also a six-layer model, which adds a fog layer or a gateway layer to the five-layer model, as well as edge and hybrid edge-cloud [97]. Finally, Cisco presents a seven-layer approach for IoT layered architecture in its recent proposal. A user and process layer, as well as an edge computing layer, were added to the preceding architecture [98].

2.3.4 3-Layers Model

The basic design for IoT systems, according to Ray [99] and Lin et al. [100], is named 3-Layers because it comprises three layers: perception, network, and application layers (Figure 2a). The items are on the Perception Layer: Sensors are used to collect data, and actuators are used to interact with the environment. The Networking Layer is in charge of establishing connections between objects, network devices, and servers. The Application Tier, which covers the delivery of services to the end user, is the final layer of the architecture, and it is on this layer that the clouds and servers are located.The IoT 3-Layers structure is widely understood, although modeling the IoT ecosystem is simple [101]. The fact that there is no Business layer is a key aspect of 3-Layer architecture.

2.3.5 5-Layers Model

To address the challenges raised by the 3-Layers design, researchers developed a new architecture. With the addition of Processing and Business Layers [102] and [103], the 5-Layers (Figure is an expansion of the 3-Layers. The Perception and Application Layers have the same qualities and aims as the 3-Layers architecture. In both directions, the Transport Layer is responsible for transporting data from items to the Processing

Layer.In the 5-Layers architecture, the Processing Layer serves as middleware, storing, analyzing, and processing the information of objects received from the transport layer. Various technologies, such as database, cloud computing, and big data processing modules, can be used with the Processing Layer. Finally, the Business Layer, which encompasses the application, business, and profit models, as well as user privacy, poses a danger to all IoT system management. Data storage and processing are described in the 5-Layers, but neither security nor privacy are addressed.

2.3.6 7-Layers Model

- The first layer contains a range of devices, sensors, and controls that allow them to communicate with one another.

- In the IoT system, the second layer is in charge of all connections and data exchanges. As a result, the communication protocols are defined by this layer.

- The data analysis and transformation are done at the third layer, the Edge/Fog Computing layer.

- The fourth layer, Data Accumulation, starts with the stored data and ensures that it is moving properly.

- The fifth step is to prepare the data for analysis using data mining techniques or machine learning data implementation. Application and Collaboration Process are the final two layers.

- The Application Layer is where users may make use of the information about the environment that the things collect.

- Finally, the seventh layer depicts the actors who use data from the IoT ecosystem to make decisions [104].

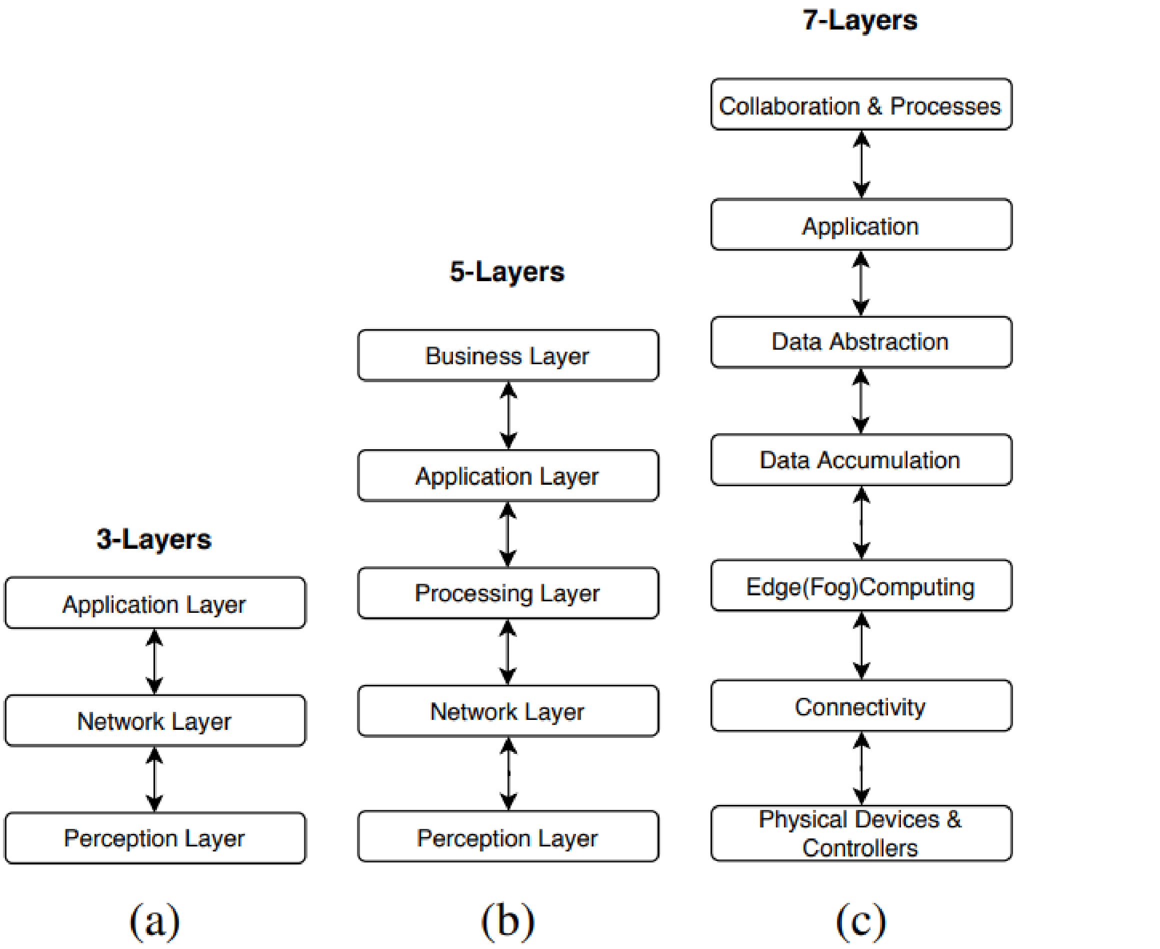


Figure 15 – Layers Models for IoT

2.3.7 Applications of IoT

This new wave of technology will stand at the leading position for all technologies around the world, which are directed towards billions and billions of connected smart devices that use all the data in our lives. With new wireless networks, high sensors, and superior capabilities, IoT applications promise to make our lives easier and bring enormous value. Some uses of IoT applications are found in several important areas. The following application areas are the top for 2020 analysis.

2.3.8 Manufacturing/Industrial

According to an expert on the IoT fields, there are multiple chances for this technology to affect various parts of human domains Several case studies indicate that the main drivers for OEMs to provide IoT solutions are "reduced downtime and cost savings".

2.3.9 Autonomous vehicles

Free-roaming robots move across factory floors: the merge of technologies such as 3D cameras, 5G connectivity, software, and artificial intelligence, etc...free-roaming robots exceed their limits in automated tasks as a result of improvement inside manufacturers all of the world. For example, an Italian manufacturer namely Automotive Systems Manufacturer Faurecia (ASMF) is using autonomous vehicles from Mobile Industrial Robots to increase the efficiency of its logistics. Machine utilization: Making the most of industrial assets: The IoT architecture has emerged as a popular and powerful way to monitor machine usage, sending valuable performance data to operators via dashboards to inform them of machines that are running more efficiently compared to other equipment. These platforms can act as a major driver in improving factory floor production, primarily by eliminating bottlenecks due to low-performing assets. They can also be used to compare the performance of devices across one or more sites.

2.3.10 Transportation/Mobility

Maintaining vehicle health: with IoT communications system of collecting data, Predictive maintenance technology made a big step to evolution with using it for measuring the performance of different parts, in addition to good use of transfer data between devices and cloud systems, the risk of a possible malfunction of vehicle's hardware or software are minimized. The ability of cloud processing is informing the driver to pay attention to any potential accident or risk and what repair is necessary to do. Transforming the meaning of vehicle ownership: vehicle ownership is one of the main applications of IoT which considering an important interest for future implementation. According to a recent study by Tony and James, car ownership will decrease by 80 percent by 2030. Thanks to Uber, DiDi, and Alibaba ride/vehicle-sharing these statistics are becoming facts addition to steadily improving public transportation services.

2.3.11 Smart Cities

The power of IoT is embodied in its mechanism of collecting data from different sub-systems therefore the best field for IoT is to publish its techniques and show excellent improvement in the city, so smart cities are a part if we didn't say all of the world's futures for amelioration citizens lives. It can make better infrastructures, transportations, requirements, crime, and safety. A study shows that using existing smart city applications, cities improve quality of life indicators (such as crime, traffic, and pollution) by between 10 percent and 30 percent. Internet of Things technologies in everyday life as part of your home, transportation, or city, relates to a more efficient and enjoyable life experience. IoT promises a better quality of life through routine chores and increased health and wellness [105].

2.4 Identity Access Management protocols For IoT

There are multiple reasearch in which they tried to use blockchain's security features such as distribution,integrity and temper proof properties to create security and privacy in communications protocols ,we cites some of them : Kshetri[106] suggests the use of blockchain in strengthing IoT by securing it from DDoS and IP spoofing attacks, also he predicts by 2020 that the IoT will require 1000 of 2016 network capacity. Roman et al[107], thought that due to the inherence dynamism introduced by device mobility, unstable connections, and related problems, they should focus on the identity and authentication process in IoT. Ouaddah et al [108] first published under the title of: Towards a novel privacy-preserving access control model based on blockchain technology in IoT, and manage to make an improved type [109] Access control in The Internet of Things: Big challenges and new opportunities, ComputerNetworks, that avoid the financial bitcoin transactions and introduces new types of transactions that are used to grant, get, delegate, and revoke access. In our study, we focused on UniquiID, as one of the protocols depending on some of the critical standards in the next section we going to mention these criticals and we're going to speak about the other two protocols and make a comparison between these two and the choosing protocols.

2.5 Critical standards

There are too many critical standards to achieve the best and a higher level of security protocols and a highly scalable system at the same time. CAP theorem is one of the principal critical standers its main goal is to serve the Consistency, Availability, and Partition Tolerance in a system that guarantees to it can't be out of service and get it runs smoothly, next to it, using the Scalability and Reliability to get the best performance. and of course without forgetting essential critiques that the protocol has to be open sources so you can access them and understand there works.

2.5.1 Consistency, Availability, and Partition Tolerance (CAP)

CAP is theorem is also called Brewer's Theorem, it's relay on logic to distributed systems by delivering the best combination of two of them, under normal circumstances, all three can be assured simultaneously. The misunderstanding is about consistent-available (CA) systems, which are simply not possible in a distributed scenario. According to CAP theorem, a system is designed to be CA, but it would require a network that ensures it dropped no packet over at any moment. For a fixed partition tolerance requirement, the only actual choice is between consistency and availability. Consistency, which is a property related to the reading operation, can be strong or eventual. In a consistent-partition-tolerant (CP) scenario typical of relational database management, the system ensures that every commit to the database is propagated and kept consistent throughout all database replicas so that every read operation returns the most recently updated result. In an available-partition-tolerant (AP) scenario, the read operation does not ensure that all user receives the most up-to-date results. But even though AP sounds problematic, consistency is eventually achieved, and this approach is common in many non-critical applications because of its powerful support for partition tolerance and availability.

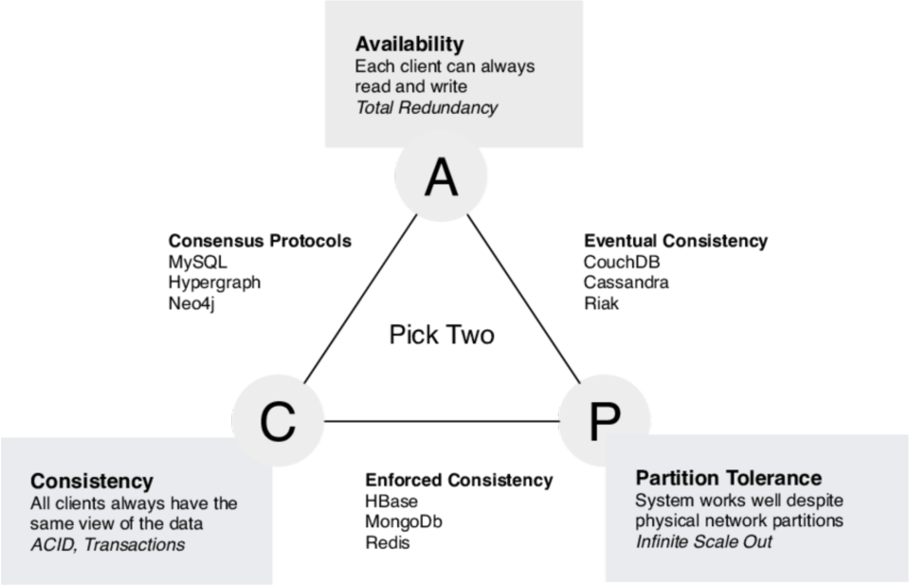


Figure 16 – CAP-Theorem

Consistency

Consistency is aim is all clients see the same data at the same time, without the need of knowing which node connects to which. For this to perps, whenever data is written to one node, it must be instantly replicated to all the other nodes in the system before the written data is considered a success by a node in the network.

Availability

Availability is a requested data by any client and gets a response, even if one or more nodes are down. In another way to sai, all working nodes in the distributed system return a valid response for any request, without exception.

Partition-Tolerance

A partition is a communications break within a distributed system, a lost or temporarily delayed connection between two nodes. In this stage of failure that decide either Cancel the operation and ensure consistency or Proceed with the operation by providing availability but risk inconsistency.

2.5.2 Scalability and Riability

Scalability is referred to as scaling up the ability to increase the capacity of existing hardware or software by adding more resources to it. For instance, processing power to a server to increase its speed. Give a solution for the network designs and the growth of the challenges of the system. The primary objectives :

- flexibility that allows systems to better address and achieves the specific users' needs.
- making the device/system scalable is to meet the changing demands and they can never be.
- static since the interest of ures even the changes with time and the environmental conditions.
- It contributes to competitiveness, efficiency, and quality.
- The importance of scalability is that it helps the system to work gracefully with no undue delay and unproductive resource consumption and makes good use of the resources.

Furthermore, Reliability is a synonym for assurance, it is a communication protocol that notifies the sender whether the sending and receiving data was success operation,in other term Reliability is to deliver data through a routing path is strong enough to handle the transaction from the source to the destination . The delivery data process is to ensure the weak links are minimized.

2.6 Novo et al

Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. Under this title, Novo et al.[110] published a white paper that contributes a newly designed decentralized access control architect for IoT devices using blockchain technology and reveals in it whom this access manager architecture works and its strong points and limitations.

2.6.1 Overview

Novo et al. clarify the primary goal is to eliminate centralized access management. On the other hand, This proposed architecture in his paper is to describe a new decentralized access management system where access control information is stored and distributed database using blockchain technology. add a solution to the access management technologies exists who's based on centralized models which introduce a variety of a technical limitation to manage them globally, especially with IoT revolution.

2.6.2 Novo et al, a walk throw

They based the novel approach on a fully distributed access control system for IoT, besides the primary use of the blockchain and the proof-of-concept implementation, with all of that the scalability of IoT. This architecture contains several entities who contribute to each other:

- Wireless sensor networks
- Managers.
- Agent node.
- Smart contract.
- Blockchain network.
- Management hubs.

Wireless Sensor Networks

A wireless sensor network is a communication network that allows constrained connectivity with limited power and light requirements, the IoT devices belong to the wireless sensor network, in contrary IoT devices do not belong to the blockchain network, one of the requirements of the architecture is that all the devices will have to be uniquely identified in the blockchain network plus:

- All registered IoT devices in the system have to belong to at least one registered manager.
- A registered IoT device can belong to multiple managers at the same time.

Managers

A manager is a lightweight nodes entity that's responsible for managing the access control permissions of a set of IoT devices, its characteristics :

- The manager do not store the blockchain information or verify the blockchain transactions as the miner nodes do .
- The manager do not need to be constantly connected to the blockchain network.
- Any entity can be registered as a manager.
- The manager controls the registered devices as IoT devices.
- The managers can define specific access control permissions for registered IoT devices.
- The manager is the only entities with the ability to interact with the smart contract in order to define new policies in the system.

Agent Node

The agent node is a specific blockchain node he's responsible to deploy the only smart contract in the system.

- The agent node is the owner of the smart contract during the lifetime of the access control system.
- Once the smart contract is accepted into the blockchain network, the agent node receives an address that identifies the smart contract inside the blockchain network.

Smart Contract

The Smart contract, which has a unique smart contract, serves as the governess supervisor in this architecture. Once it's deployed in the blockchain network, it can't be deleted from it. All the operations allowed in the access management system are defined in this contract. When the operations are triggered by blockchain transactions, the miners will keep the information of the transaction globally accessible.

Blockchain Network

The blockchain network in this architecture is a private blockchain. they chose a private blockchain since all the elements of the prototype are more dimensioned, a public blockchain should facilitate the adoption of the solution.

Management Hubs

IoT devices are very limited in terms of CPU, memory, and battery, for being part of the blockchain network implies keeping a copy of the blockchain locally and a track of the network transactions, for that they are not connected to the blockchain because of their constrained nature. On the other hand, a management hub is an interface that :

- Translates the information encoded in CoAP messages by the IoT devices into JSON-RPC messages understandable by the blockchain nodes.

- They connect directly the management hub with a blockchain node.

- Multiple sensor networks can be connected to a management hub node.

- A multiple management hub nodes can be connected to the same blockchain node.

- IoT devices will only be able to request access information from the blockchain using the management hub.

- Management hub is high performance characteristics node that able to serve as many simultaneous requests as possible from the IoT devices.

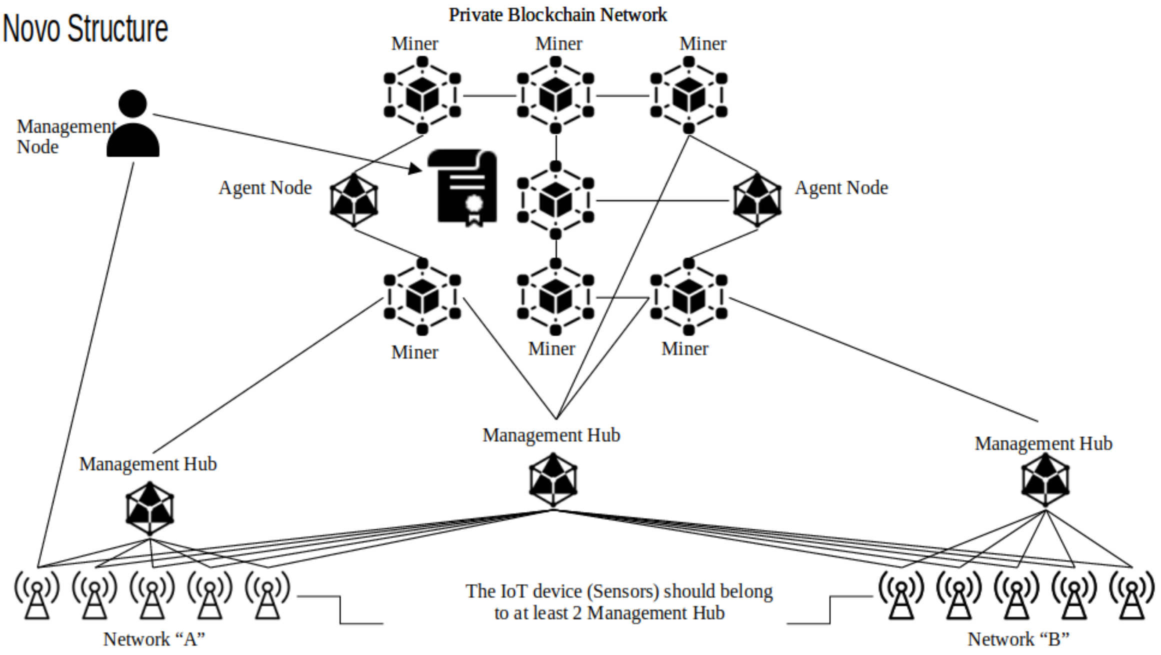


Figure 17 – Novo Structure

System Interactions As all entities previously mentioned, the interaction between the entities will be explained in this section. The interactions can be divided into four different phases:

- Setting up the management blockchain network. possible from the IoT devices.
- Registering the managers and IoT devices into the system.
- Defining the policy for those aforementioned components.
- Discovering the policy.

Network Set-Up

in this phase, firstly creation of the blockchain network, secondly the creation of the access management system in the blockchain, then deploying of the smart contract into the blockchain network by the agent node, who defines all the operations of the access control management system, after that the managers and management hubs in the system need the smart contract's address to interact with it to register as managers or change the control access rules of the IoT devices.

Registration

Any blockchain node in the access management system can register as a manager in condition to know the address of the smart contract. When that information is obtained, it can register itself, sending a transaction to the function “Register manager” defined in the smart contract. Thereafter, the manager will receive the address of its registration once it successfully accepted the transaction into the blockchain. That address will identify the manager in the access management system. That for the manager registration, for the new IoT device registration, the manager will identify the device into the access management system.

Management Modification

This system supports multiple numbers of managers controlling the same device. There are multiple ways in the system to transfer the management control from one manager to another or to add or delete several managers from the system. Besides that, no one can remove a manager from the system but itself. In addition, a manager is permitted to remove himself from an IoT device as long as the IoT device is under the control of at least another manager node. Otherwise, the smart contract will not allow the operation.

Policy Definition

Managers can define access control rules for the resources of their IoT devices. The permissions can be defined in many ways. However, the permissions in our implementation list the devices entitled to access a particular resource. Thenceforth, managers not only need to know the address of the devices under their control but also the address of the devices authorized to access their IoT devices. Managers can enforce the policy by creating a transaction toward the smart contract with all that information.

Policy Modification

Similar to the policy definition, managers can modify and delete policies at any time. The method is similar to the method described in the policy definition. If a manager adds an existing policy using the Add Access Control operation, that policy gets modified automatically.

Part one

When two devices, device “A” wish to access a resource hosted by another device “B”, a CoAP message request sent the request of the access control information of A passe through the management hub. Before an IoT device can connect to the closest management hub, the device first needs to discover the hub’s IP address.

Part two

The management hub then translates the device’s message into an RPC message and sends it to the miner on the blockchain network attached to it. The operation queries the information from the blockchain stored in the miner. Once the miner informs about the access policy of A to the management hub, the management hub translates the answer back to “A”. An act accordingly depending on the information received by the management hub, and therefore,” A” sends the information of the resource to “B”.

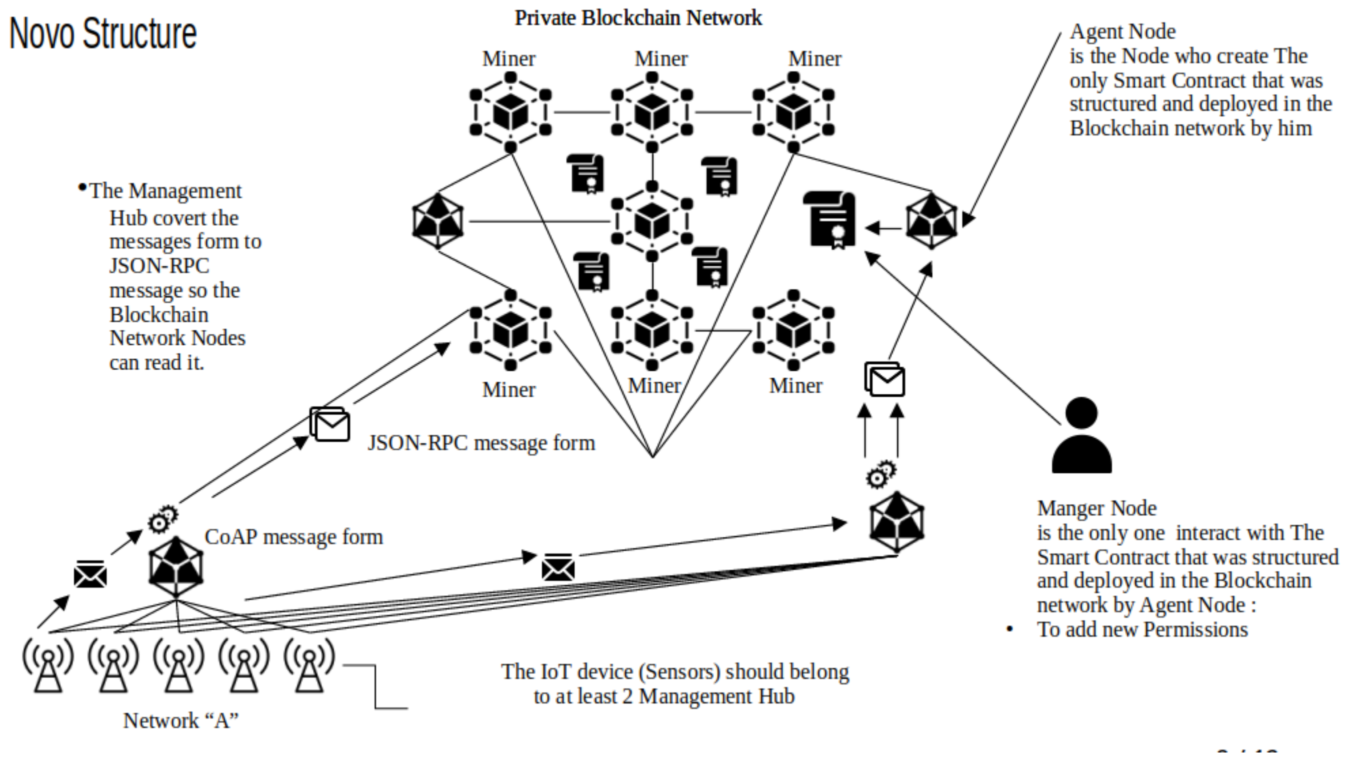

Novo Structure
Private Blockchain Network
Miner
Miner
Miner
Agent Node
is the Node who create The only Smart Contract that was structured and deployed in the Blockchain network by him
•The Management Hub covert the messages form to JSON-RPC message so the Blockchain Network Nodes can read it.
Miner
Miner
Miner
JSON-RPC message form
CoAP message form
Manger Node
is the only one interact with The Smart Contract that was structured and deployed in the Blockchain network by Agent Node :
• To add new Permissions
The IoT device (Sensors) should belong to at least 2 Management Hub
Network “A”

Figure 18 – Novo Structure functioning

2.7 CapChain

2.7.1 Overview

In this section of chapter 2, we will give a brave study of the CapChain framework [12] who proposed a model that an access control framework based on blockchain that allows users to share and delegate their access rights easily to IoT devices publicly, To protect privacy, by adapting multiple techniques from anonymous crypto-currency blockchain systems to hide sensitive information, including users’ identities and related information. They also build a test model as a proof of concept. They implement blockchain technology to perform and serve the privacy for users’ data and credentials, by avoiding the one point of failure. , moreover, this targeted goals is preformed by using the blockchain exchange key that carried out via transactions method with that the man-in-the-middle attacks can be avoided, they also specified in the model the device’s usage should only be visible to users within their private networks, in contrary public blockchains suffer from a privacy problem since all can access data on the blockchains[111].

2.7.2 CapChain a walk throw

They assume that every IoT device in CapChain has one or several ultimate owners who have full control over the device and can generate capabilities based on its own access control policies. It's can be delegated to other users via transactions on a public blockchain that serves as an immutable ledger that records delegation. To grant access to a certain user, the device needs to verify the existence of the relevant transaction on the blockchain. System delegation follows such characteristics:

- Each user's capability has an expiry date for auto revocation. Of delegation, a receiver's capability cannot expire later than the expiry date of the sender's capability.

- Besides auto-expired capabilities, users can still track or revoke the entire chain of delegation originated from themselves if necessary.

- Identities of sender and receiver and transaction information are protected.

- Users need only one master account to receive capabilities from different domains.

In detail the system builds under various conditions :

Capability

Refers to a token that represents some access right to an IoT device, and is encrypted by a secret key shared between the device and its owner, the owner initializes all capabilities associated with his devices and sends them to the blockchain via transaction message contained publish instruction and transferred between users via transactions to. In CapChain, the rule is transferred capabilities cannot have a longer lifetime than the original ones. Thus, the expiration time can be treated similarly to the amount of money in cryptocurrency systems. If we ignore the context of capability.

Blockchain and capability transactions destinations

In this phase blockchain stores all of the capability transactions. It serves as an access control list that records the proof that a user is holding a certain capability and when it will be expired. Use the 3 types of transactions: txpublish , txdelegate , and txconfirm, in terms of delegation, it involves 3 types of public keys

- User's primary address: each user joining the blockchain has a public key as his/her primary address.

- Onetime sub address: an address that is derived from primary address. A transaction will 2 addresses: the use and the domain the contains the device.

- Domain's address: a public key that represents a domain/organization. The corresponding private key is known to both the local proxy and all devices within the domain.

2.7.3 Authorization workflow

The CapChain address 3 entities in the network:

IoT devices

hat have low computation and low storage. The device may or may not have direct access to the Internet, it has to rely on a local proxy to look for transactions on the blockchain.

Proxy

a more powerful device that acts as an actual node on CapChain.

Mobile devices

receive and transfer capabilities. When a user request access, they can prove his/her capability possession by signing the corresponding transaction. The device then will inquire to the blockchain (either directly or via local proxy) for the transaction and the capability and grant access accordingly.

Transaction linkability The users should be able to control all of the delegations made by their successors and revoke them if necessary, unlike the current anonymous crypto-currency systems where there is no way for the sender to trace if their sent money will be spent further.

2.8 UniquID

2.8.1 Overview

UniquID is a decentralized authentication platform that manages identity access management that based on the Proof-of-conccept, it targets to secure the authenticate and authorized access between IoT devices. By generating and providing a digital Key that makes the IoT wondering devices access to different networks without third-party intermediaries. That means to make the device-independents and facilitate the IoT devices authentication. Plus the need of dealing with the increasing problems specifically the device-centered paradigm. On contrary, the traditional identity access management (IAM) frameworks and authentication old mechanisms were not sufficient to deal with IoT challenges[112].

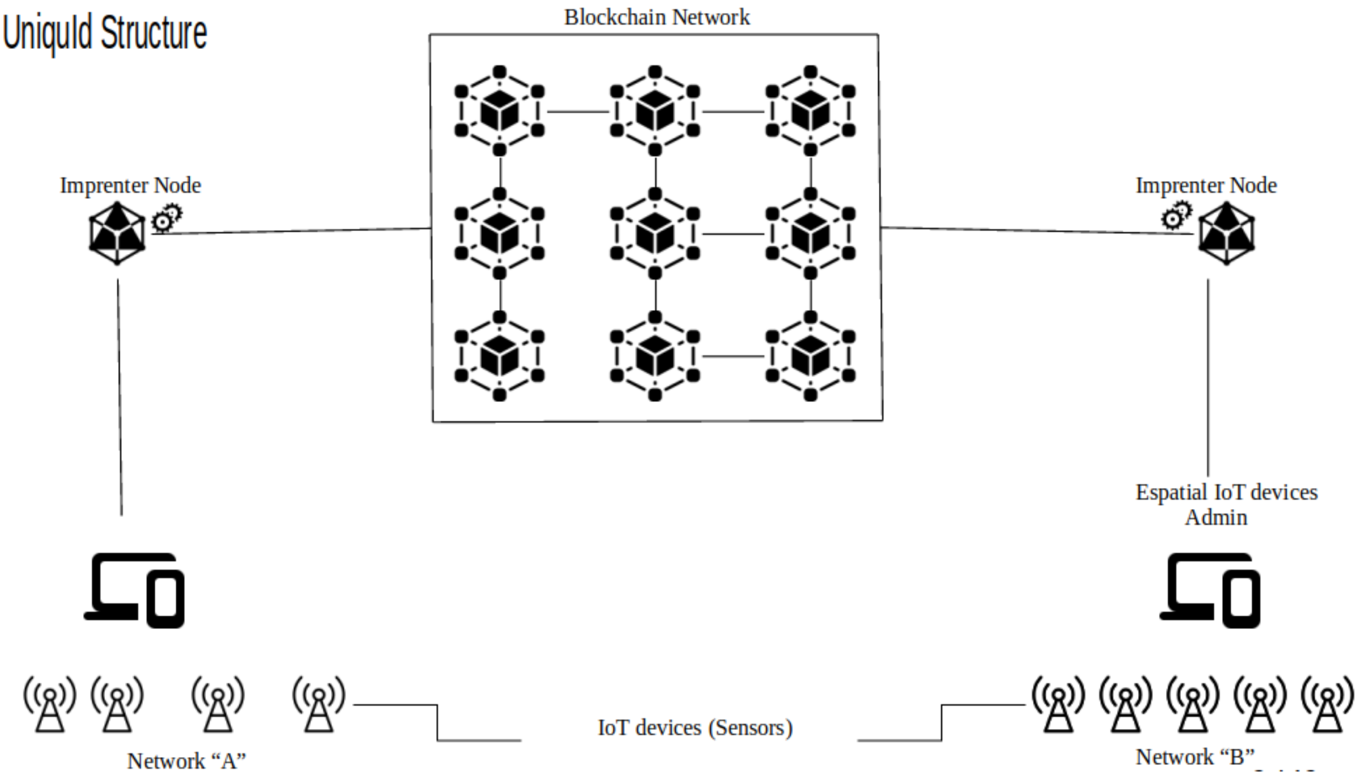


Figure 19 – UniquId Structure

2.8.2 UniquID a walk throw

in UniquId wight paper [112] the publishers explained the difference between the old methods that depend on third-party intermediaries and whom to provide and ensure safe access to a specific platform services ,therefore , the conventional IAM systems are essential for traditional local networks and businesses, but not well-suited for large networks of complex, highly distributed devices, such as the combination of Internet of Things (IoT) and machine to machine (M2M) communication. as well as considering the PKI is one of the key technologies for dealing with security issues and enabling trust among parties [20]. But adoption of the technology never took off as envisioned, due to critical issues such as privacy and liability concerns, management complexity, and high costs, besides that it lacks the flexibility needed for IoT and M2M, whereas certificate-based authentication is well-suited for these uses. Publishers also explained the soled base of this platform by relying upon the blockchain technology and take the advantage of certification infrastructure to overcome the difficulties in reconciling IoT credentials and across-domain IAM, their main goal is

- UDescribing a cheaper and simpler alternative to traditional IAM systems.

- Illustrating the implementation of cross-domain identities for IoT devices to circumvent account reconciliation.

- Showing how the proposed design removes single points of failure from the trust structure.

- Demonstrating direct peer-to-peer (P2P) authentication and authorization among IoT devices.

- Showing how an IoT device, empowered to locally read a smart transaction, deals with partitioning issues as defined by the CAP Theorem.

In detail, the hierarchical structure of the UniquId platform shows the different layer of it, blockchain layer connected to the IoT network devices and manage the access throw several actors who have specific roles ,

Blockchain

It a public decentralized tamper-proof network, each one of its nodes store a copy of the smart contracts that deployed by the imprinter node instead of tokens in the traditional systems.

IoT network

It's interconnecting sensors that refer to groups of IoT devices, that contain a simple sensor and special ones.

Imprinter

Its special node belongs to blockchain network functioning by creating and deploying special smart contracts in a way to the survey authentication process in the UniquID model.

IoT devices Admin

Referring to sensors that connect with other sensors through threw IoT network and special sensors that have high-performance hardware comparing to other basic devices, it is named admin device. as a special node in UniquID architecture. Its have his owne data structure named Merkel-Tree that stored the Imprinting Contraccts who created and deployed by the Imprinting Node to authonticate the outsider devices base on them.

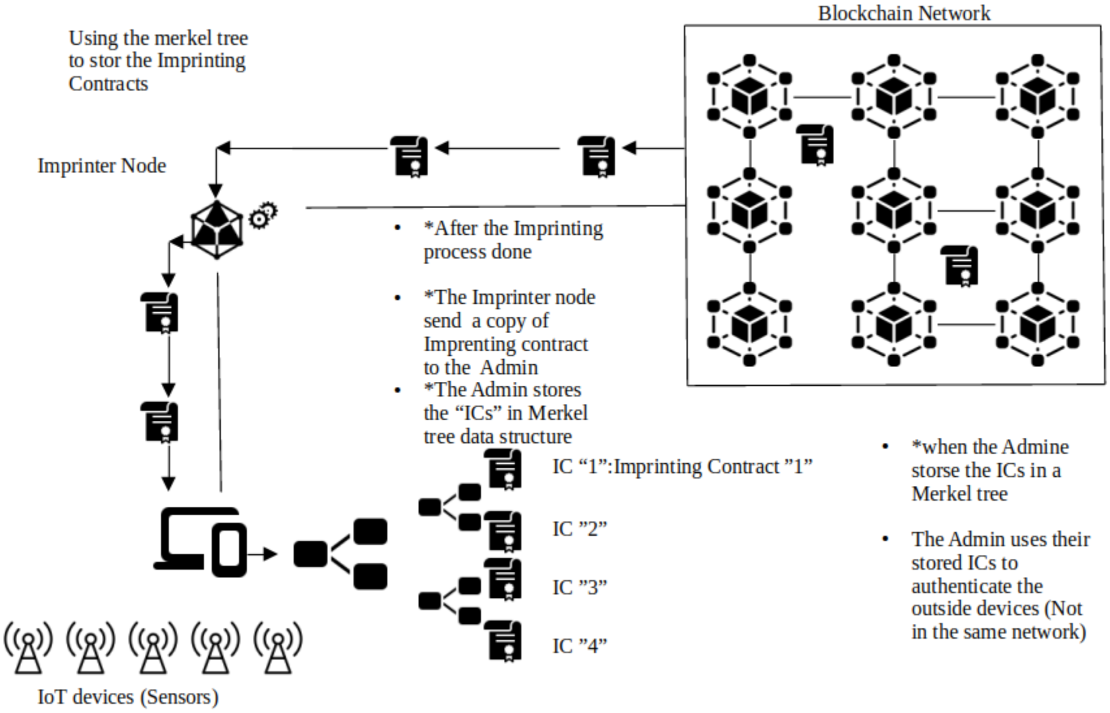

Using the merkel tree
to stor the Imprinting
Contracts
Blockchain Network
Imprinter Node
• *After the Imprinting process done
• *The Imprinter node send a copy of Imprenting contract to the Admin
• *The Admin stores the "ICs" in Merkel tree data structure
IC "1":Imprinting Contract "1"
IC "2"
IC "3"
IC "4"
• *when the Admine storse the ICs in a Merkel tree
• The Admin uses their stored ICs to authenticate the outside devices (Not in the same network)
IoT devices (Sensors)

Figure 20 – (Using the merkel tree to stor the Imprinting Contracts

How it works together These mentioned actors functioning in two different ways each one of them surveys a particular needed goal, in detail each node of the IoT network ether a part of entity A or B, generates its own public key which is directly exchanged with other devices in the same local network. The identities are stored in a blockchain through the imprinting process, the imprinter generates a special smart contract, the imprinting contract (IC), which links the device to the public key of its administrator. Once the generation is done, the imprinter collects the ICs and announces them to the blockchain, After this phase is complete the two scenarios mentioned earlier serve different goals:

- first scenario

- is when two entities try to communicate with each other, entity A wants to negotiate resources from entity B ,in this case the authentication works based on the strored of imprinting contracts in the merkle tree parallel with the update from the blockchain(in case a new device is added to platform or deleted from it). This latter scenario serves CP consistency and partition-tolerance in terms of CAP theorem as the quality goal and security purpose that guaranty by blockchain technology.

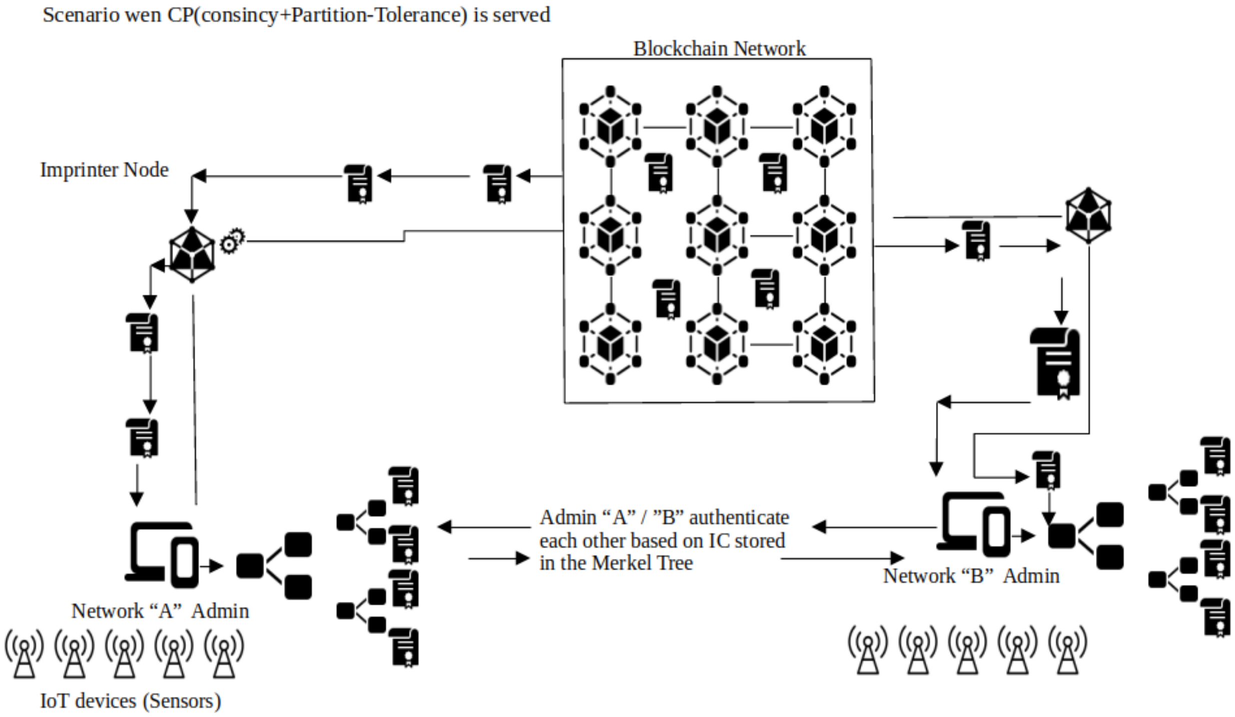

Scenario wen CP(consincy+Partition-Tolerance) is served
Blockchain Network
Imprinter Node
Admin “A” / ”B” authenticate each other based on IC stored in the Merkel Tree
Network “B” Admin
Network “A” Admin
IoT devices (Sensors)

Figure 21 – Scenario when CP(consincy+Partition-Tolerance) is served)

- Second scenario

- is when two entities try to communicate with each other, entity A wants to negotiate resources from entity B without the need to Update the Imprinting Contracs that stored in the Merkel Tree, each one of the entities has stored hash trees and locally confirm certificate validity thanks to the Merkle tree data structure. This latter scenario serves availability and partition tolerance in terms of CAP theorem as quality goal and scalability by ignoring the security purpose by the blockchain technology.

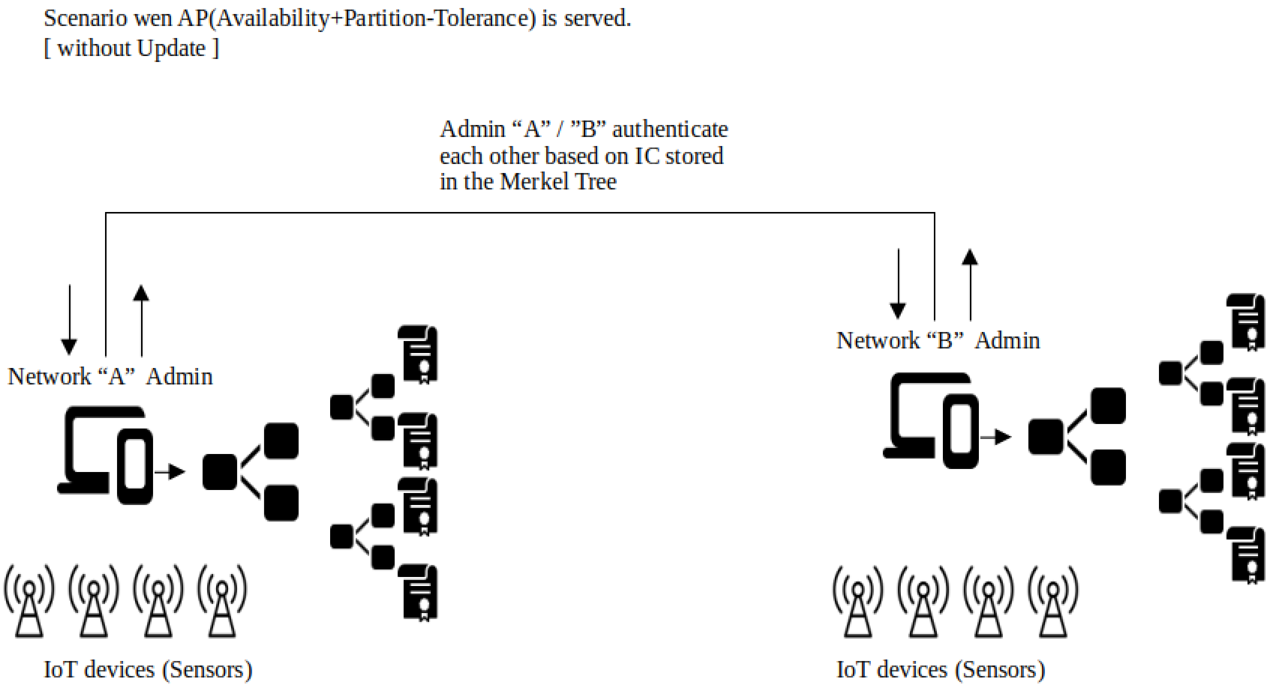

Scenario wen AP(Availability+Partition-Tolerance) is served.
[without Update]
Admin “A” / ”B” authenticate
each other based on IC stored
in the Merkel Tree
Network “A” Admin
Network “B” Admin
IoT devices (Sensors)
IoT devices (Sensors)

Figure 22 – Scenario when AP(Availability+Partition-Tolerance) is served

2.8.3 UniquID publichers experimental Evaluation

the experimental results of a UniquID enrolment instance, executed on a cloud service. Even though we measured the performance of the identity generation phase, as well as the imprinting phase, moreover, the small setup we used for our experiments cannot represent a fully operating UniquID network. Considering that experience is to show that our solution is feasible. they created 7 parallel clients, designated to generate 1000 virtual IoT identities and communicate such identities to 1 imprinting node. Every identity is announced as soon as it is created, and the receiving imprinting node is appointed both to create the IC transactions and forward them to the Litecoin Testnet blockchain. Imprinter and clients ran over AWS T2. Micro instances, burstable performance instances equipped with 1 Gb of RAM. As a communication protocol between the imprinter and the clients, they used MQTT (Message Queue Telemetry Transport), an ISO standard (ISO/IEC PRF 20922) publish-subscribe-based messaging protocol, designed for lightweight communications. They also chose Litecoin as a storing public blockchain, which ensures one mined block every 2.5 minutes. Considering that a Litecoin block is 1 Mb and that a UniquID transaction is 400 bytes, this design choice entails a theoretical upper bound of 2500 enrolled devices per 2.5 minutes or 1000 devices per minute. More in general, and defining the theoretical upper bound of enrolments per minute with the following equation:

$$\frac{Block\ Size\ (bytes)}{400\ (bytes)\ \cdot\ Average\ Mining\ Time\ (m)},$$

where 400 bytes are the size of a UniquID transaction, and the other parameters depend on the underlying blockchain.

2.8.4 Identity Generation

The purpose of this phase is to evaluate and measure the time needed to generate a virtual client next to a physical one and to compare them plus conclude the difference between theoretical and actual time and see if the model is feasible :

- In virtual clients, they measure an average time of 6.61 ± 0.03 milliseconds to generate an identity.

- In the physical client they run the experiment with arm 926ejste CPU, 256 MB RAM, and a mlinux 3.3.6 OS, in this particular hardware the generation of the identity took 627 milliseconds, by only using 44.7 percent of the CPU and 0.4 percent of RAM of hardware capacity.

Even tho 627 milliseconds is substantially higher than the one obtained with a virtual client (6.61 ± 0.03 milliseconds) the generating identity under 1 second is still an excellent result.

2.8.5 Imprinting

As the second part of their experiment, they analyzed and measured the necessary time to imprint new identities on a public blockchain, the imprinter has the role to create an IC transaction for each identity and submit all the transactions to the blockchain. The Imprinting process shows that the average time to imprint one identity is 9.06 ± 0.35 minutes. These experiments clearly show that the imprinting took a considerably longer time than the generation of the identities. The former took minutes, whereas the latter took milliseconds.

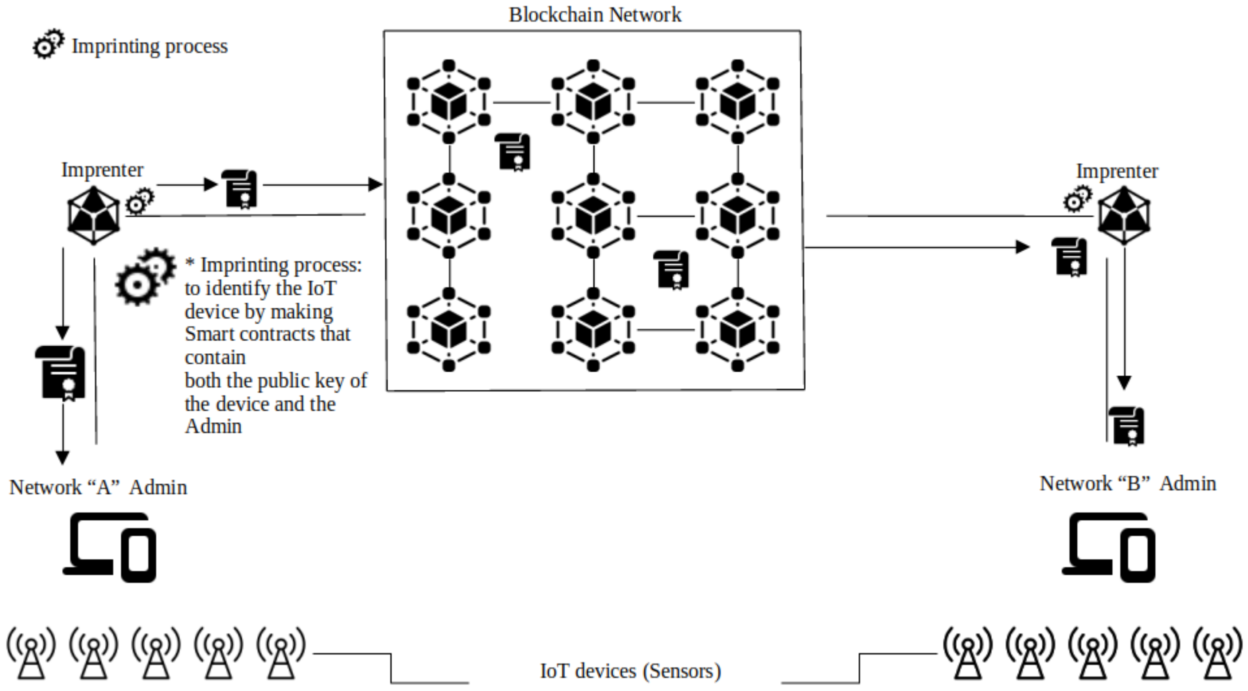

Imprinting process
Blockchain Network
Imprenter
* Imprinting process: to identify the IoT device by making Smart contracts that contain both the public key of the device and the Admin
Imprenter
Network "A" Admin
Network "B" Admin
IoT devices (Sensors)

Figure 23 – Imprinting process

2.8.6 Summing the experiments Enrolment

Their experiments show that, in total, it took around 4.5 hours to automatically enroll (i.e., create, announce, and imprint) 1000 identities, without any human intervention. The reason why this practical result is considerably under the theoretical upper bound of 1000 enrolments per minute, is that our virtual clients on Amazon AWS could open no more than 5 concurrent sockets, per each. This resulted in a bottleneck, where already generated identities were announced with considerable delays. The next Figures shows the magnitude of this bottleneck: on average, it took 115.86 ± 2.19 minutes to announce an identity to the imprinter, which is a significant amount of time compared to the time for identity generation (6.61 ± 0.03 milliseconds) and imprinting (9.06 ± 0.35 minutes).

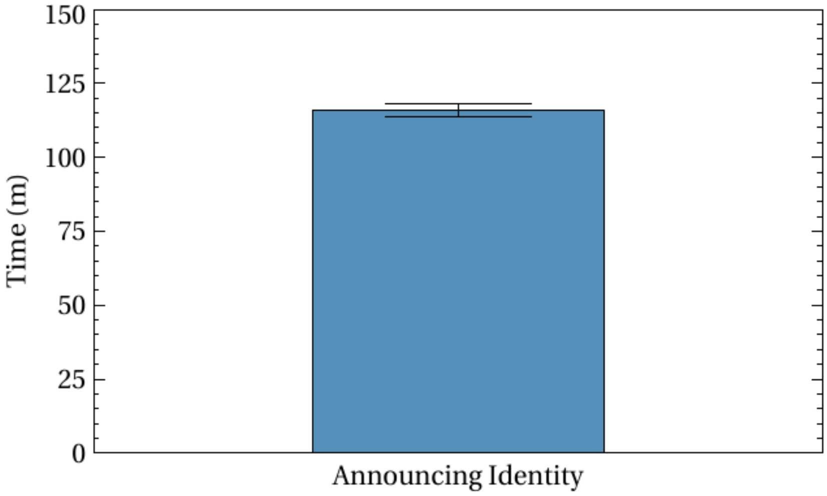


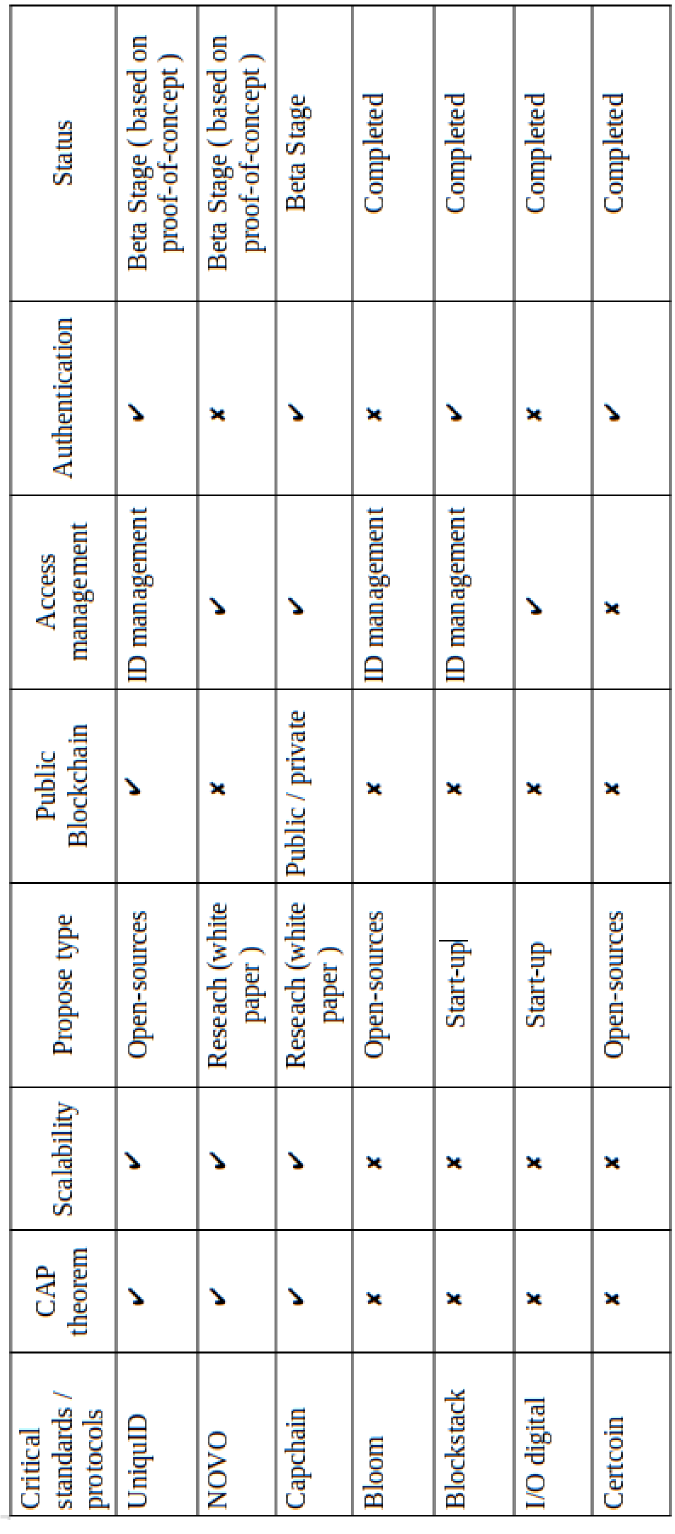
Figure 24 – Average time to announce one identity. Announce time is in minutes

2.8.7 Experimental concluded results

Even after some progression made by the publisher, by add and run the same experiment under 50 concurrent threads per MQTT client, overcoming the communication bottleneck and increasing our capacity to 400 enrolments per minute. Still, at the present stage, UniquID does not enable us to get near the theoretical upper bound, but this is purely due to software limitations that are currently addressed. After all, the better given circumstances enrolled devices no longer need to rely upon PKIs, centralized CA authorities, certificates, nor passwords. This architecture can be feasible without forgetting the applying approach of the proof of concept.

2.8.8 Comparing UniquID with The different proposed approaches

The different approaches proposed in the UniquID architecture and all previous mentioned protocols combine and take advantage of the CAP theorem and IAM effective solution, to gain both sides of the security and scalability, moreover, the reliability and ether Availability/Partition-tolerance. Or Consistency/Partition-tolerance. In specific, comparing with Novo et al, propose blockchain-based access management that utilizes a management hub as a middle-point between IoT devices and the blockchain to get a highly scalable system over a secure one. that avoid the financial bitcoin transactions and introduces new types of transactions that are used to grant, get, delegate, and revoke access. other of these, unlike Novo approach. Comparing to UniquID, the main goal is to serve both scalability and security and show how it provides direct identification and authentication, which in turn enables efficient Machin-ot-Machin resource negotiation. Its worthe of mentioning the other protocoles that have the same goal to authenticate the devices in the IoT like Bloom [113] a Bockchain project for credit scoring and identity management ,BlockStack [114] Decentralized server for identity authentication and storage ,I/O Digital [115]identity management based on the Blockchain,and CertCoin [116] is a decentralized authentication system as shown in figure.



Critical standards / protocols	CAP theorem	Scalability	Propose type	Public Blockchain	Access management	Authentication	Status
UniquID	✓	✓	Open-sources	✓	ID management	✓	Beta Stage (based on proof-of-concept)
NOVO	✓	✓	Reseach (white paper)	✗	✓	✗	Beta Stage (based on proof-of-concept)
Capchain	✓	✓	Reseach (white paper)	Public / private	✓	✓	Beta Stage
Bloom	✗	✗	Open-sources	✗	ID management	✗	Completed
Blockstack	✗	✗	Start-up	✗	ID management	✓	Completed
I/O digital	✗	✗	Start-up	✗	✓	✗	Completed
Certcoin	✗	✗	Open-sources	✗	✗	✓	Completed

Figure 25 – Comparative Protocols Table

2.9 Conclusion

Throw this second chapter we gave an entry to our subject and what technologies involve in it and cites some of the protocols that use these technologies then we did give a brief study of three selected protocols, we selected protocols base on several critical standers that secure the Identity Access Management for IoT devices by combining the new technology of the Blockchain and the CAP Theorem(by combining the best two of Consistency, Availability, and Partition Tolerance), and achieve a Scalability in the system, for each of Novo et al, CapChain, and UniquID.plus a brave mentioning of the Bloom.BlockStack, we did show for each one of them the soled base their creators claimed to have by tested models.

3 CHAPTER: LWU "LIGHT WEIGHT UNIQUID" OUR PROPOSED IMPROVED PROTOCOL FOR UNIQUID PLATFORM

3.1 inroduction

Internet of Things (IoT) devices need to rely on some more powerful protocols/platforms to guaranty and deliver secure access between IoT devices of network and user and his device. Throw our research we passed over various of research in which we narrow the field research with specific conditions to choose what is close to our topic study, these conditions are represented as follow : The model must be open sources, using free access technology (permissionless blockchain), and in its beta-stage, which means the model is not in its theoretical performance, as a result, the model in development rolling, throw this element we select the mentioned protocols as related works and many others to show us the current hot subjects in IT research field. In particular, UniquID is what agrees with our purposes, since it's used both of the two technologies as well as being an open-source project that bases on a proof-of-concept model of research and start-ups, it's the main goal to ensure trusted a secure authentication process that underlying in to control access management refers to Identity Access Management. Our work to improve and get better performance of the proof-of-concept model and implement and enforce the right logic that offers by the blockchain technology and suggest solutions to some security fayes , by adding new conditions and change some actors roles, all that to reach the best implementation of decentralization concept and secure access management platform.

3.2 The misconceptions in the UniquID model

First, the publishers of the UniquID white paper suggest that the protocol relies on a bunch of actors, every one of these actors has his own role and the combination between them makes the platform more secure and scalable than the others platforms/protocols. We will specify and introduce the misconception and the miss collaboration of the technologies that the model relies on them, by explaining the role of each actor and when they collaborate with any of the suggested platforms moreover the logic contradicting processes.

actors and mechanisms that play a big role in UniquID protocol:

3.2.1 Iot devices admin

Is a part of the UniquID platform that generate other simple IoT devices identities, every IoT admin has his own network that has low-performance IoT devices, it's worth mentioning that these special actors are not a node of a blockchain network, a part of his role associate with an imprinter actor to accomplish the registration of simple devices and define it in the blockchain network via a smart contract,in detail exchange his public key+ device key that roled by him, with the imprinting node and aspect from him to create special smart contract and receive a copy to accomplish the authentication process without the need of returning to the blockchain to approve the access.

3.2.2 IoT devices admin issues

The previous explanation of the role of IoT devices admin show the misplacing of this model-actor in the framework, furthermore, IoT devices admin do not need to store smart contract copies to authenticate network outsider, in the case of storing them and executing them without being a member/node of a blockchain network, it means the model returns to a centralized system, it's a logic contradicting, knowing that you can't run them outside the blockchain platform.

3.2.3 The Imprinter actor

It's a node that his exclusive role is to connect the UniquID to the blockchain network by generating a special smart contract that defines IoT devices into the platform model database that is decentralized in a blockchain network. the next part of its job is to get a copy of the deployed smart contract to every device manager.

3.2.4 The Imprinter actor issues

This actor is misplacing, he has no role to run the smart contracts that he structured and deployed earlier to execute them as a result that confirms the access. The white paper of the uniquID framework didn't specify if imprinter converting messages that send by admin devices to make them readable by a blockchain platform. the past action, the imprinter is necessary to have to convert the message encoded in CoAP by the IoT devices into JSON-RPC messages understandable by the blockchain nodes.

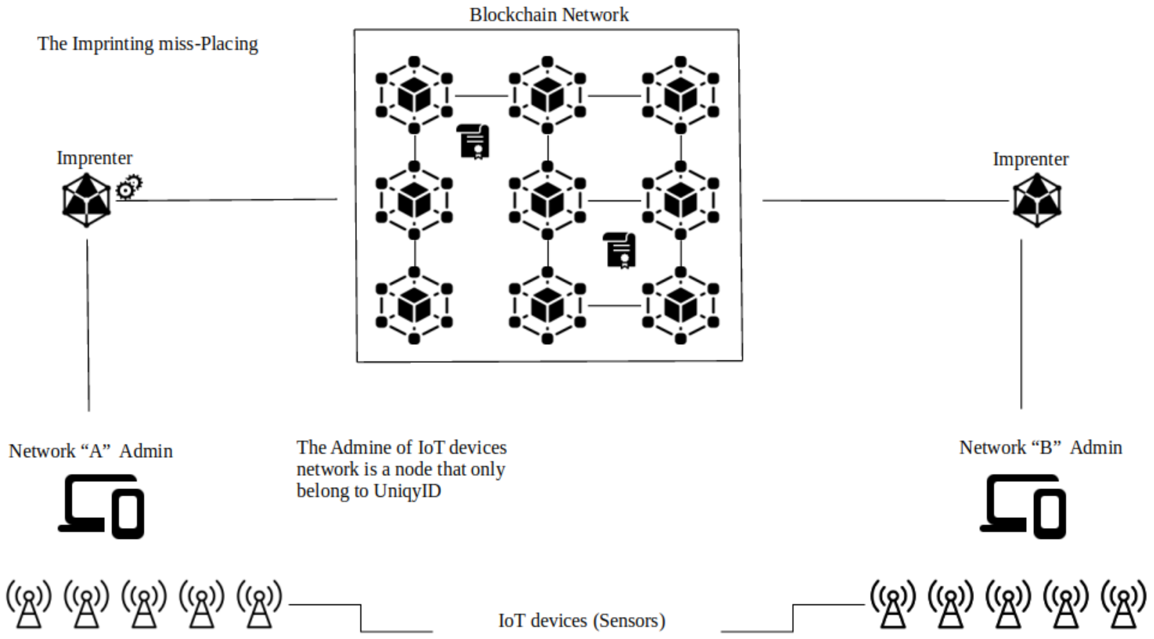

Blockchain Network
The Imprinting miss-Placing
Imprenter
Imprenter
Network "A" Admin
The Admine of IoT devices network is a node that only belong to UniqyID
Network "B" Admin
IoT devices (Sensors)

Figure 26 – The Imprinting miss-Placing

3.2.5 Using Merkle trees mechanisme

The UniquID publishers insert it in entities that are responsible to connect IoT devices so that in case of network failure one of the entities using the smart contracts locally confirms the access, all that is stored in the Merkle tree.

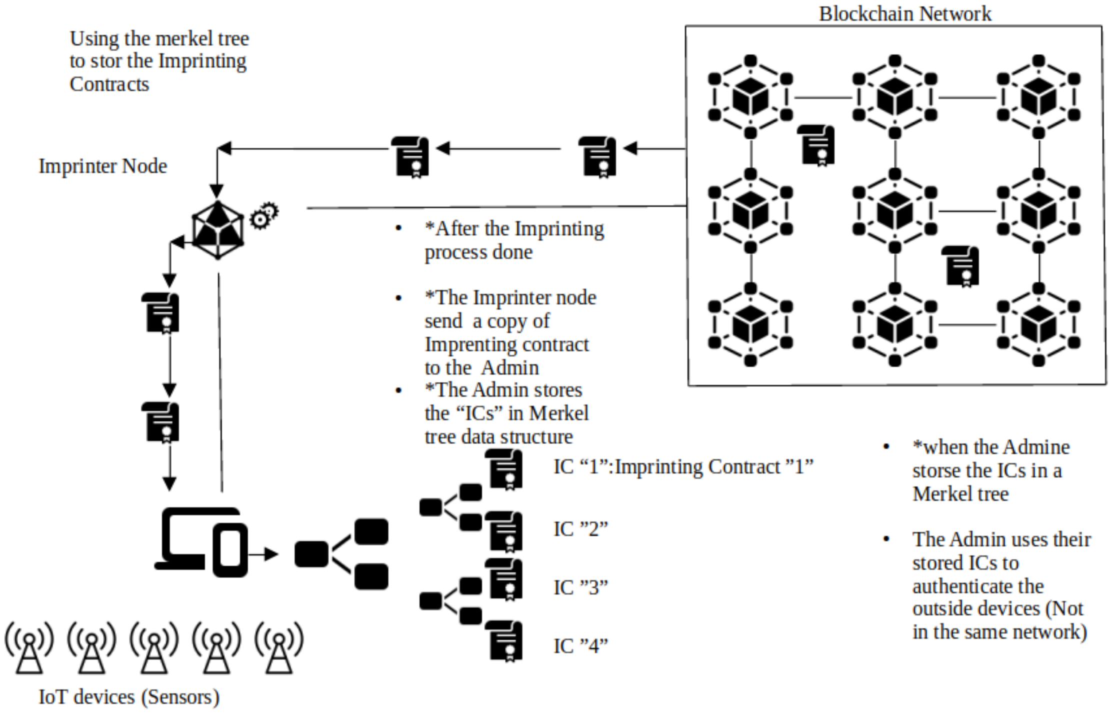
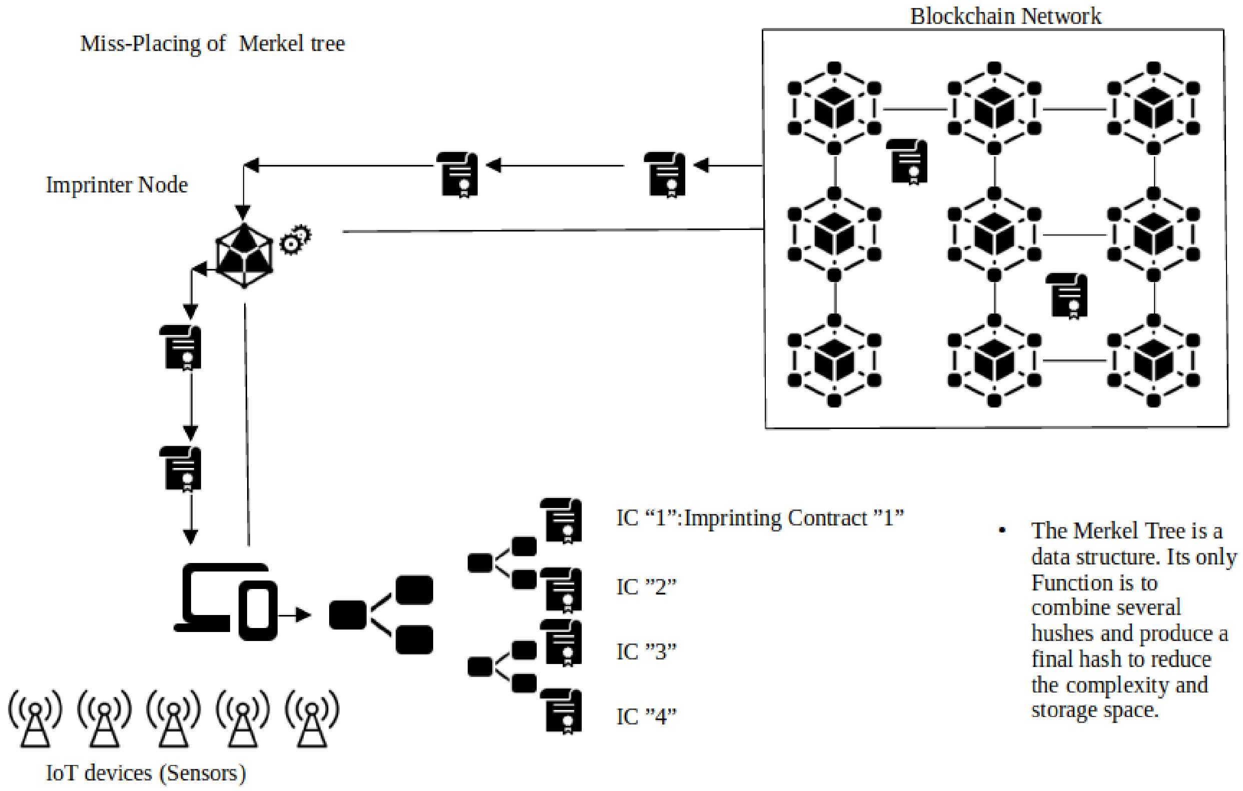

Blockchain Network
Using the merkel tree to stor the Imprinting Contracts
Imprinter Node
*After the Imprinting process done
*The Imprinter node send a copy of Imprenting contract to the Admin
*The Admin stores the "ICs" in Merkel tree data structure
IC "1":Imprinting Contract "1"
IC "2"
IC "3"
IC "4"
*when the Admine storse the ICs in a Merkel tree
The Admin uses their stored ICs to authenticate the outside devices (Not in the same network)
IoT devices (Sensors)

Figure 27 – Using the merkel tree to stor the Imprinting Contracts

3.2.6 Using Merkle trees mechanisme issues

Is a data structure form functioning by only merging a big number of transaction hashes to one hash that contains them all.the publishers using the Merkel tree to store smart contracts to use it later to confirm or denied the request access from outsiders.



- The Merkel Tree is a data structure. Its only Function is to combine several hushes and produce a final hash to reduce the complexity and storage space.

Figure 28 – Miss-Placing of Merkel tree

3.3 Suggestions to Improve and Avoid Misconceptions in the UniquID Model

In the previous title, we cite a few elements that play a big role in our choosing model, we spoke about actors and their functions and structure that are worth mentioning beside we explain their effects on our protocol, after that, we analyze them for discovering some potentials points of failures in which we identified some of them , for this part we want clear the misunderstanding of the technology used in this protocols and set things clear from any problems that we found in the model, what we are going to propose a change that gives this latter what we consider a batter performance.

3.3.1 IoT devices admin improve suggestion By Eliminate the Imprinter Actor

we suggest as improvement of the model structures, that IoT device admin must be node a part of the blockchain network, to avoid the condition to connect directly to blockchain network without the intermediate actor, in this case, the imprinter node, this suggested improvement serves a scalable performance that made the model reliable, and makes the IoT device admin the key of assuring the security and decentralization in the right way,as a result :

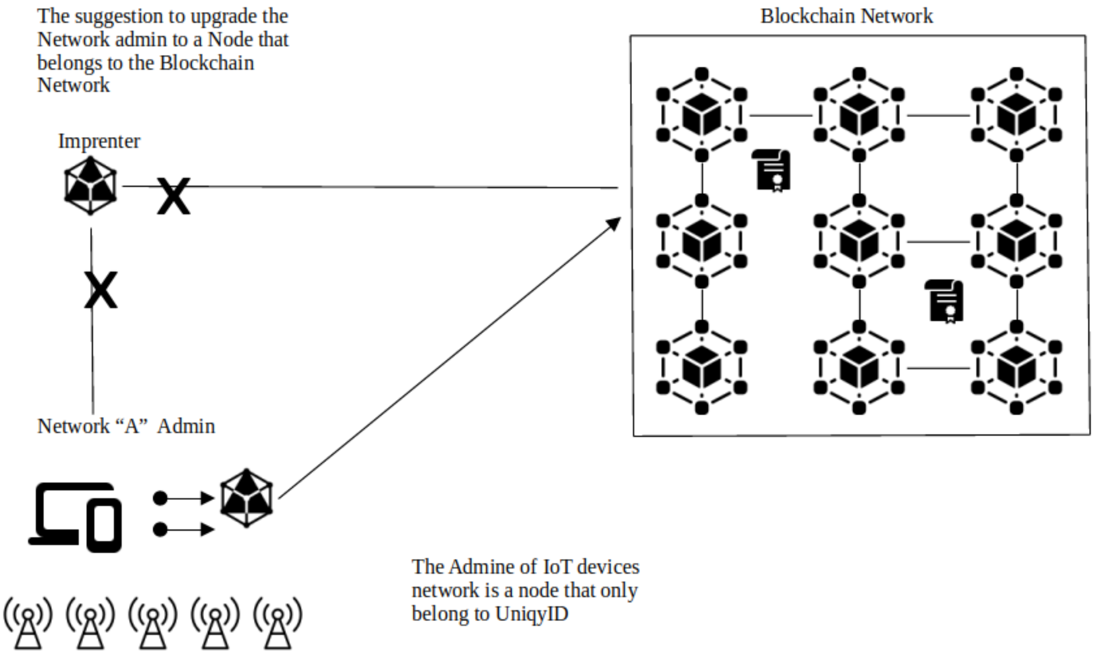

The suggestion to upgrade the Network admin to a Node that belongs to the Blockchain Network
Imprenter
X
X
Network "A" Admin
Blockchain Network
The Admine of IoT devices network is a node that only belong to UniqyID

Figure 29 – The suggestion to upgrade the Network admin to a Node that belongs to the Blockchain Network

By that is means to there is no need for the concept of Merkel-Tree in the model especially when we suggest making IoT admin device node in the blockchain network, even though it was a miss implementation from the beginning that suggestion showed in figure 29.

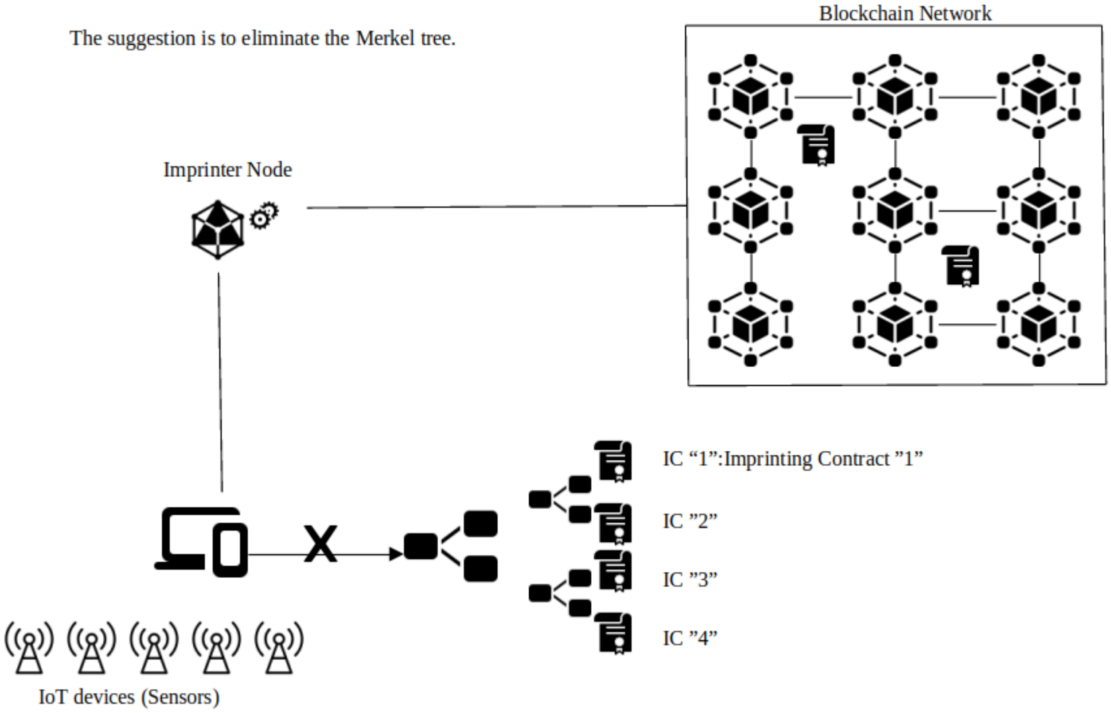
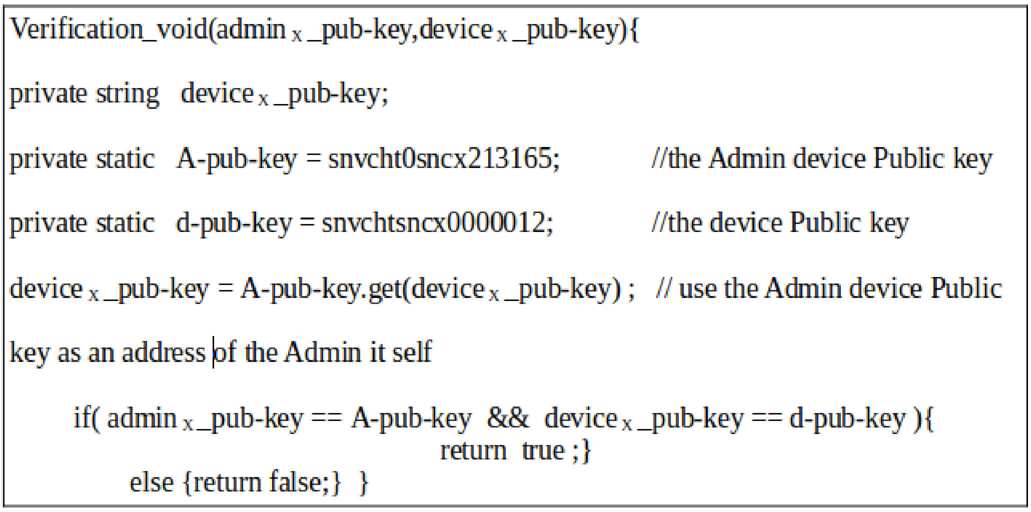

The suggestion is to eliminate the Merkel tree.
Blockchain Network
Imprinter Node
IC “1”:Imprinting Contract ”1”
IC ”2”
IC ”3”
IC ”4”
IoT devices (Sensors)

Figure 30 – The suggestion is to eliminate the Merkel tree

The promoted UniquID Admin node service

Since UniquID is working on ethereum ,we going to use ethereum as platform and for IoT admin device which have high performance soft-wear and hard-wear we suggesting as an example Raspberry PI device .Ethereum platform provides it’s users the chance to create nodes and test them before execute your projects .We going to show an example of how making an IoT admin (Node) device a node in the Ethereum :

- Steps that UniquId perform to add the User device as an Admin Network approved by the Blockchain platform by:
  - Check node configuration, sending a request to the elected admin and see if the device have the proper hardware to join the Blockchain network.
- The blockchain Platform approved on the Admin.
- Install an Ethereum-cli on the Node.
- The UniquID Platform set configuration of the Special Smart Contract Form,that pre-designed in the Platform.



```
Verification_void(admin x _pub-key,device x _pub-key){

private string   device x _pub-key;

private static   A-pub-key = snvcht0sncx213165;          //the Admin device Public key

private static   d-pub-key = snvchtsncx0000012;          //the device Public key

device x _pub-key = A-pub-key.get(device x _pub-key) ;  // use the Admin device Public

key as an address of the Admin it self

      if( admin x _pub-key == A-pub-key  &&  device x _pub-key == d-pub-key ){
                                  return  true ;}
           else {return false;}  }
```

Figure 31 – Special Smart Contract Form

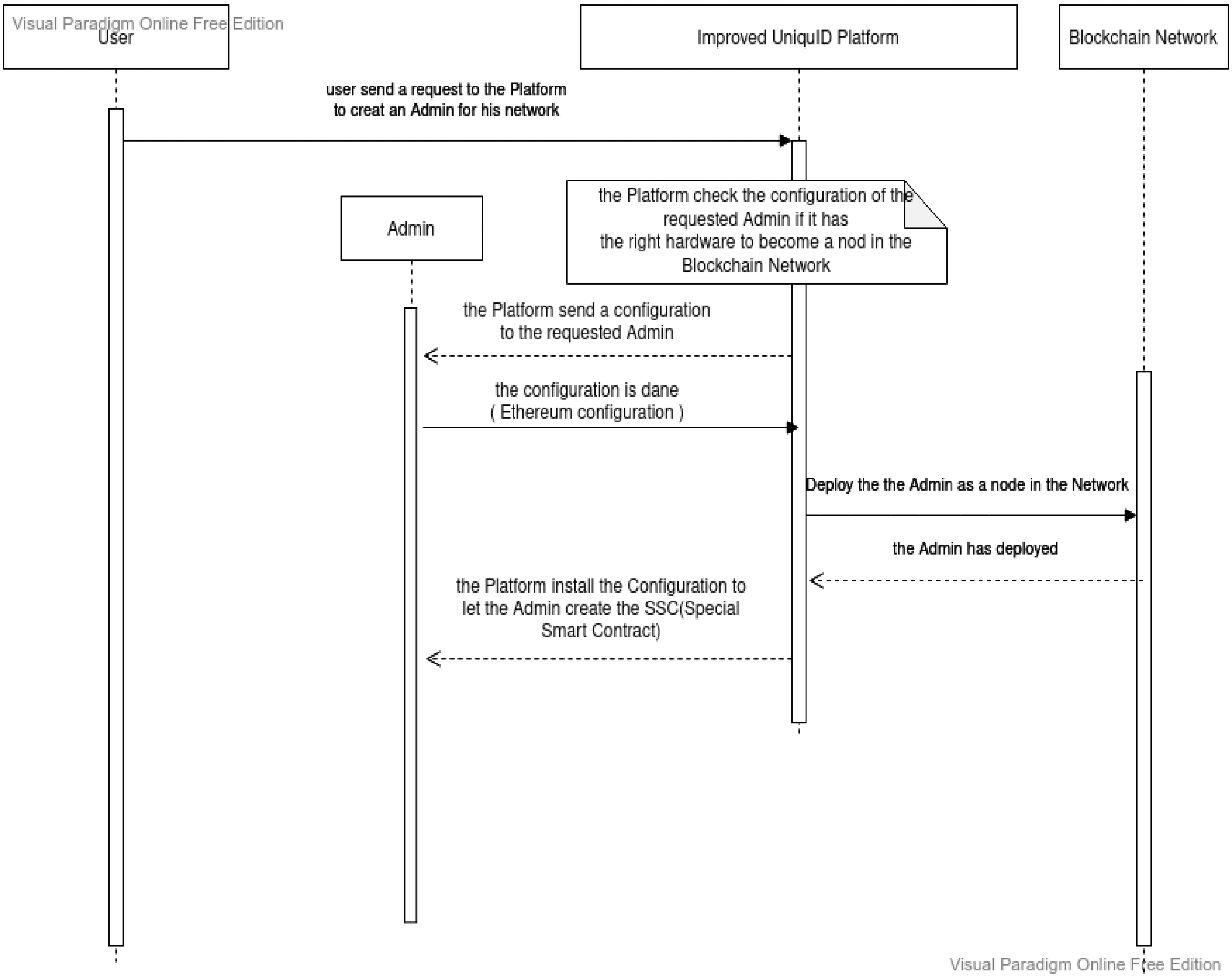
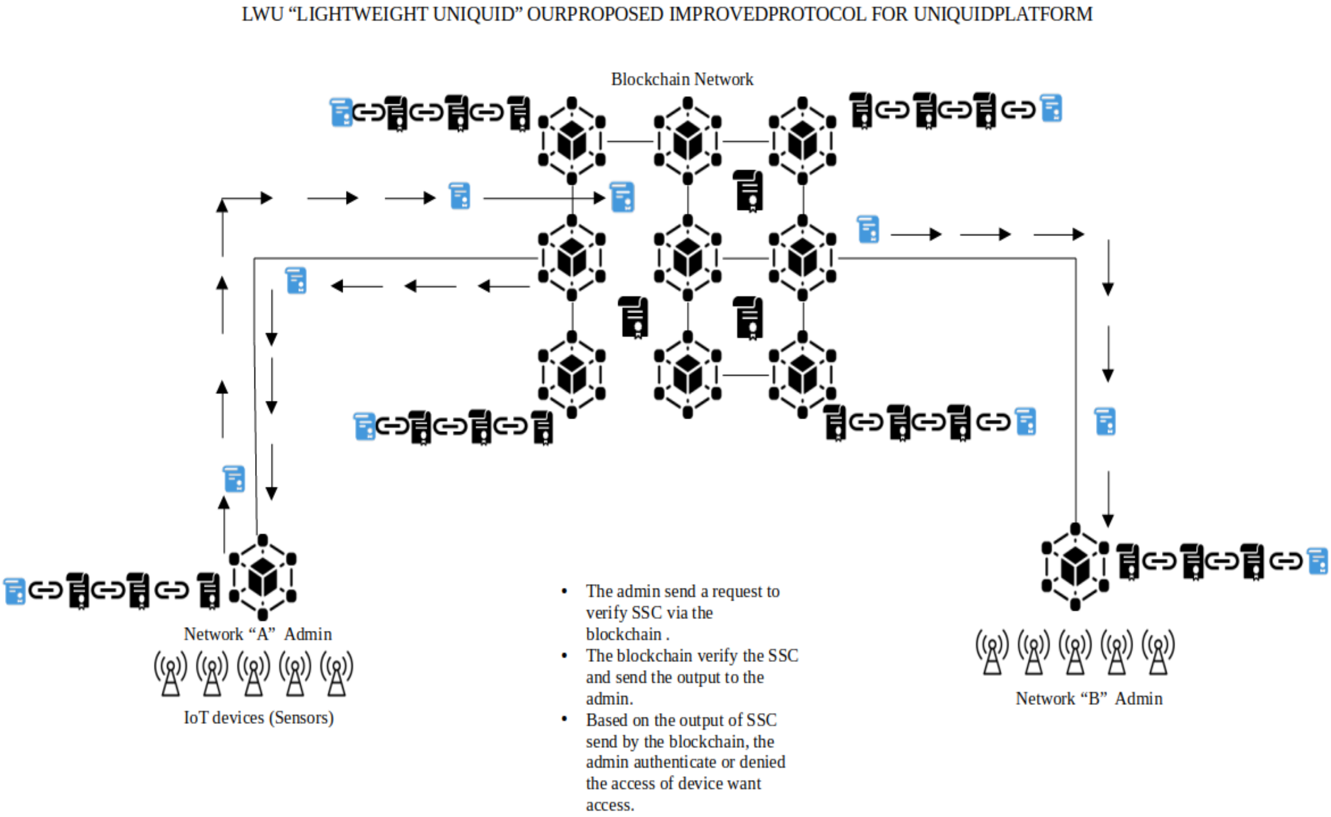

Visual Paradigm Online Free Edition
User
Improved UniqID Platform
Blockchain Network
user send a request to the Platform
to creat an Admin for his network
Admin
the Platform check the configuration of the
requested Admin if it has
the right hardware to become a nod in the
Blockchain Network
the Platform send a configuration
to the requested Admin
the configuration is dane
(Ethereum configuration)
Deploy the the Admin as a node in the Network
the Admin has deployed
the Platform install the Configuration to
let the Admin create the SSC(Special
Smart Contract)
Visual Paradigm Online Free Edition

Figure 32 – Sequence Diagram that shown who the Platform user request to add new Admin,and the approval process


LWU “LIGHTWEIGHT UNIQUID” OURPROPOSED IMPROVEDPROTOCOL FOR UNIQUIDPLATFORM
Blockchain Network
Network “A” Admin
IoT devices (Sensors)
Network “B” Admin

- The admin send a request to verify SSC via the blockchain .
- The blockchain verify the SSC and send the output to the admin.
- Based on the output of SSC send by the blockchain, the admin authenticate or denied the access of device want access.

Figure 33 – LWU “Light Weight Uniquid” Ourproposed Improvedprotocol For Uniquidplatform

3.4 The services Provided by the Admin

Considering the suggested solutions, the Admin actor in the LWU (light weight UniquID) model can provide several services to assure both of security and scalability goals, comparing withe UniquID first model. the services Admin actor can provide:

- Creating the SSC
  - First the Admin can create the SSC based on the the configuration installed in it(Admin) by the Platform
  - Second the Admin deployed the SSC in the Blockchain Network,in details when the Admin send the request, the Blockchain check if the SSC in the programming langage understandable by the Platform (Solidity in case of Etheruem Platform)

then send a copy to a miner ,after the miner solve the puzzle and find the right hash for it and send back to the Network,finely the Blockchain Platform send a copy to all nodes in the Network including the Admin .

– Next the Admin can authenticate other devices even from outside Network of his own, by verifying the the SSC in the Blockchain Network based on the address of it, plus the addresses of the device and his Admin (@SSC +admin-public-key + device-public-key)

3.5 Check if the suggested solutions can improve the security in UniquID platform

In this section, we going to test the suggested solution in several scenarios to check if they are valid for all possible scenarios:

Scenario one (when the user add a device in his network)

In case of a new device want be added to IoT the network,it send request that contained her public-key to admin device,the admine device generate special smart contract that contained the device public-key,the admine public-key that is already define by UniquID platform after that, the formed SSC deployed in the blockchain platform. The blockchain platform gives the aproval of SSC being added by sending a copy to all nodes in the network, this last give the @address of the SSC to IoT device itself.

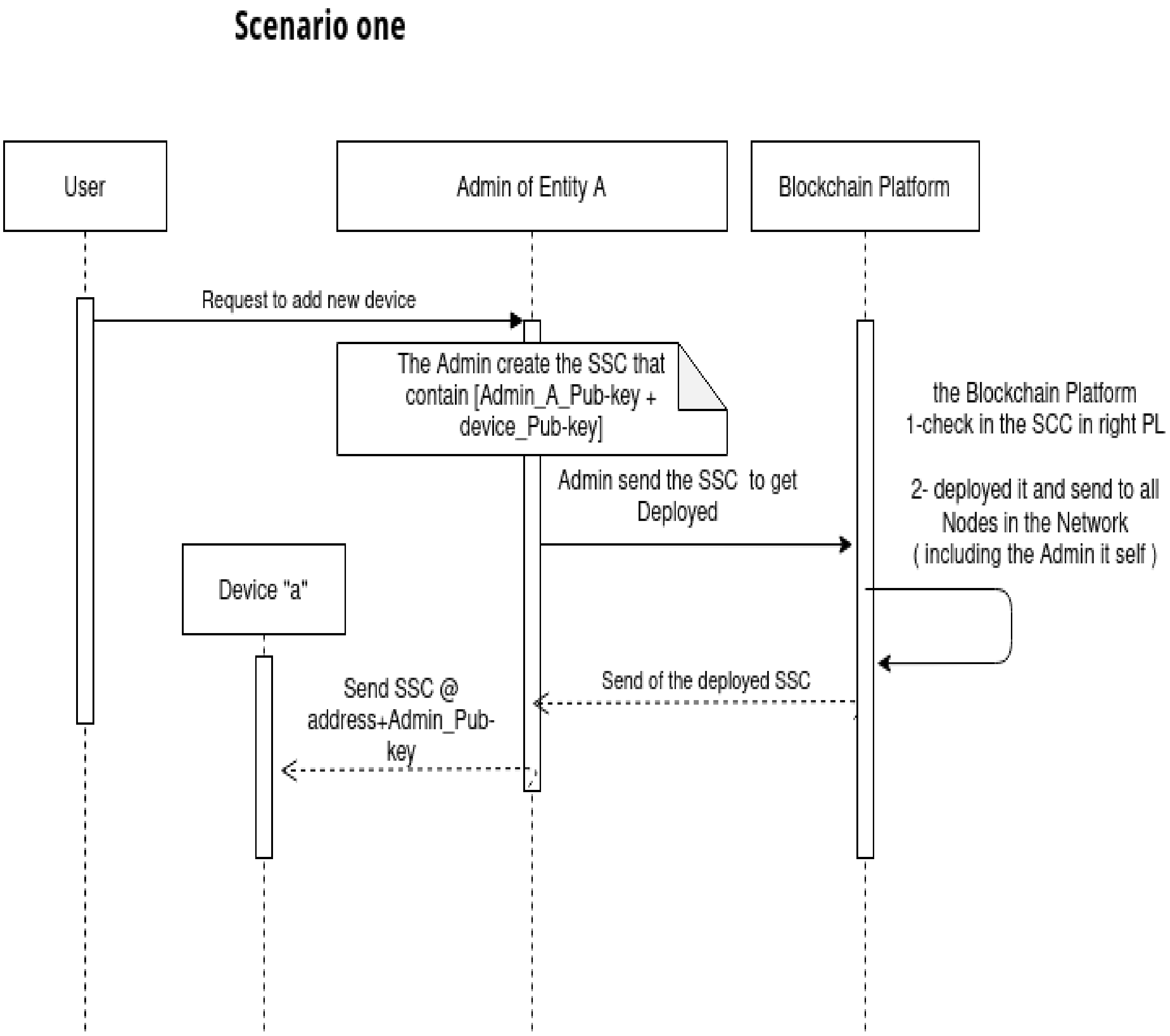

Scenario one
User
Admin of Entity A
Blockchain Platform
Request to add new device
The Admin create the SSC that contain [Admin_A_Pub-key + device_Pub-key]
the Blockchain Platform
1-check in the SCC in right PL
2- deployed it and send to all Nodes in the Network (including the Admin it self)
Admin send the SSC to get Deployed
Device "a"
Send of the deployed SSC
Send SSC @ address+Admin_Pub-key

Figure 34 – scenario how the user send request for Entety Admin to add new device in the network

Scenario two

When a device from entity A want to communicate to device from entity B,the device contact admin(B) by sending request that contained (device public-key,admin(A) public-key,it's smart contract @dress),the admin(B) send the request detail into blockchain platform,the latter verify if nodes agree to this copy,after their agreement ,the platform execute the smart contract that belong to the mention device in order to authenticate her and give her access to communicate with the device that belong to entity B,that can happen if the condition of the smart contract is verifiable,in our case,the SSC contact admin(A) to get the public-key of device and compare it to what it has,if admin(A) have public-key of the device that means it's still belong to his network and the condition is approved,therefore the result of SSC is acceptance and by that the communication between devices is allowed .

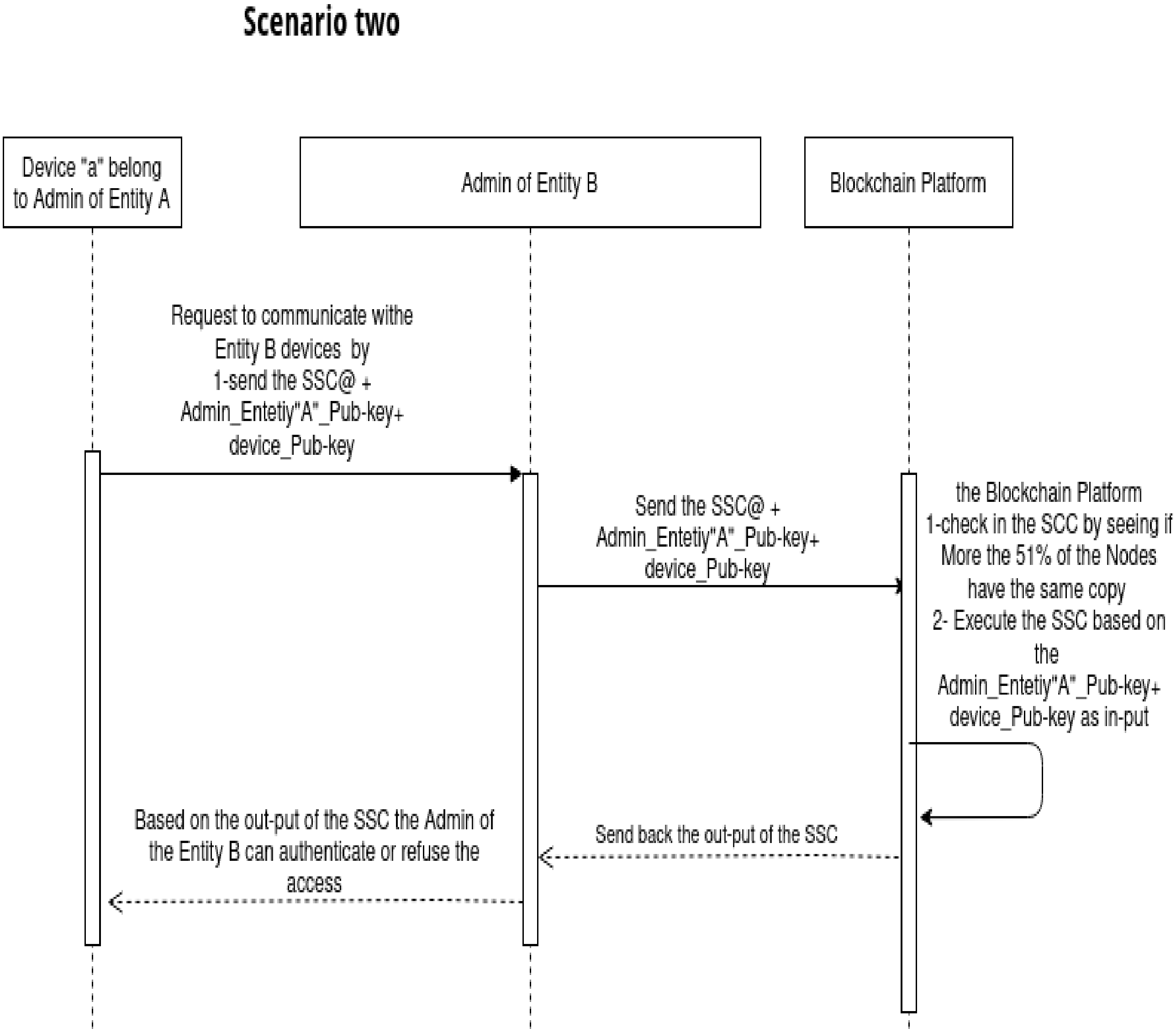

Scenario two
Device "a" belong to Admin of Entity A
Admin of Entity B
Blockchain Platform
Request to communicate withe Entity B devices by 1-send the SSC@ + Admin_Entetiy"A"_Pub-key+ device_Pub-key
Send the SSC@ + Admin_Entetiy"A"_Pub-key+ device_Pub-key
the Blockchain Platform 1-check in the SCC by seeing if More the 51% of the Nodes have the same copy 2- Execute the SSC based on the Admin_Entetiy"A"_Pub-key+ device_Pub-key as in-put
Send back the out-put of the SSC
Based on the out-put of the SSC the Admin of the Entity B can authenticate or refuse the access

Figure 35 – scenario when device who belong to anther Entity Admin request to connect with Entity B admin

Scenario three

If a IoT device is removed from entity A and still want to communicate to one from the other entity,this device send a request which contained(her public-key,admin(A) public-key,@dress of her smart contract),as the mechanism work ,the admin(B) transfer it to blockchain platform ,as the sequence of the event being sad,verification is done by approval of other nodes,as a result execution of SSC of this device,here the result change since the condition in the SSC haven't checked because the device has leave the entity A network,in detail, the blockchain get the device public-key from admin(A), in this scenario, since device is removed from the entity ,the admin delete it's public-key therefore the result from admin(A) is NULL as a consequence the condition in the SSC is false so no authentication for the device request of communication.

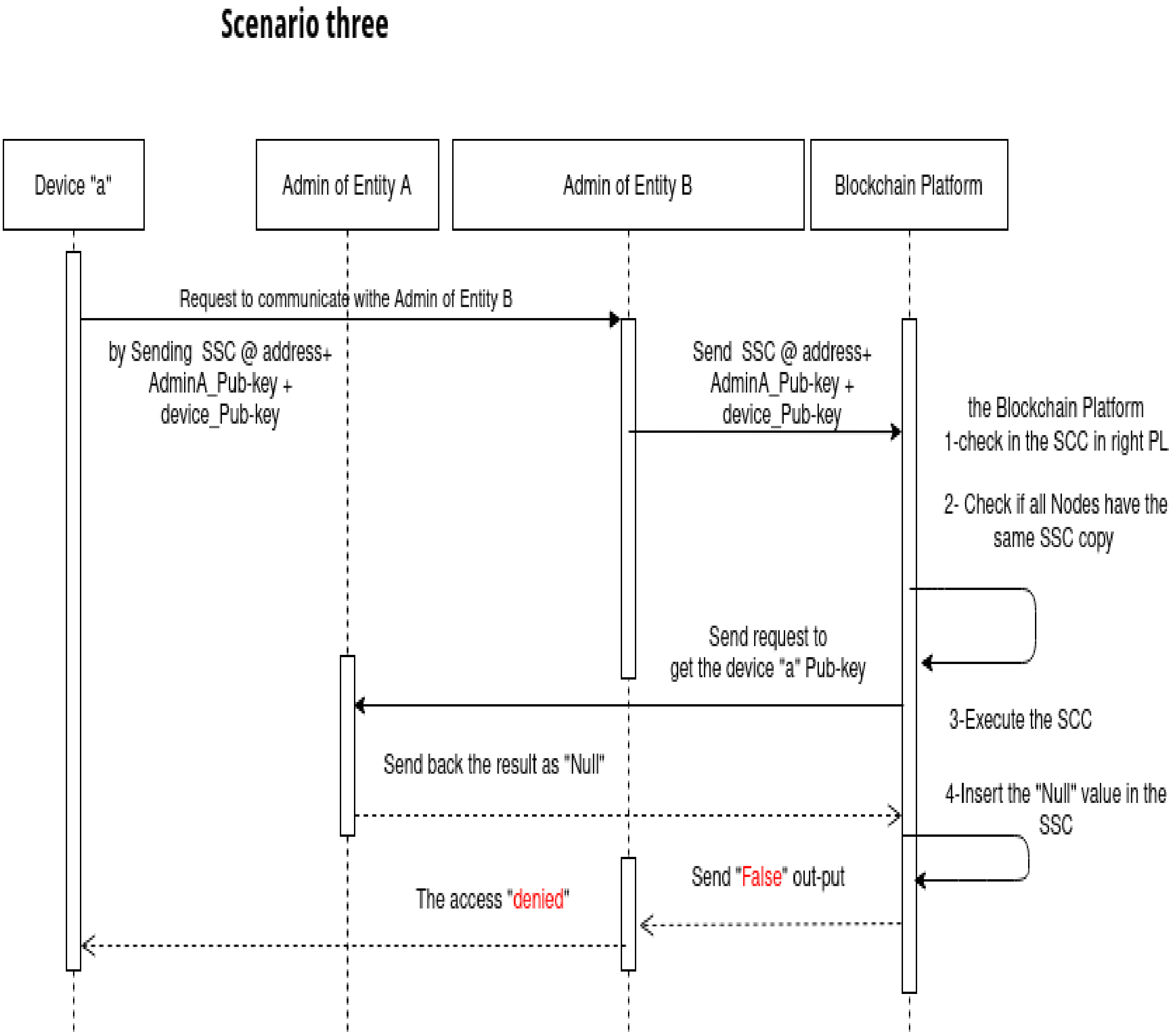

Scenario three
Device "a"
Admin of Entity A
Admin of Entity B
Blockchain Platform
Request to communicate withe Admin of Entity B
by Sending SSC @ address+ AdminA_Pub-key + device_Pub-key
Send SSC @ address+ AdminA_Pub-key + device_Pub-key
the Blockchain Platform
1-check in the SCC in right PL
2- Check if all Nodes have the same SSC copy
Send request to get the device "a" Pub-key
3-Execute the SCC
Send back the result as "Null"
4-Insert the "Null" value in the SSC
Send "False" out-put
The access "denied"

Figure 36 – scenario when the out side device request to connect with Entety B admin

3.6 The advantages of the lightweight UniquID

An improved security

- 1- We promote the admin of IoT network as a node that belong to the blockchain network.
- 2- The authentication check will be happening in the right circumstances that guaranteed as a node in the blockchain network.since the verification of the smart contract by the Blockchain Network, instead being verified by just the Admin it self.
- 3- Avoid the time service between admin node and the imprinter in the UniquID model when the admin send the generated identities to imprinter.
- 4- Reline on blockchain decentralize storage structure instead of the Merkle-Tree.
- 5- Boost the number of blockchain nodes to make a scalable infrastructure.

3.7 Conclusion

In this chapter, we did analyse the protocol by presenting some failures,that can jeopardize and risk the the users data in one side and the working platform in the other side, in this case we did found out the mis-using of merkle-tree as storage structure and the weakness in the imprinting contract verification process,as a solution we eliminate the imprinter node, and promote the admin device as node of blockchain that give us better security performance as well the scalability, which UniquID didn't provided.We suggest the Light weight UniquID as a new extension for UniquID protocol to get the most secure authentication performance that the main platform can provide.

4 CONCLUSION AND FUTURE WORK

Blockchain has proved efficiency in the security and decentralized aspect in different IT domains, he brought a lot of new ideas in the domain of research, and since it's considered a fertile field, researchers attempted to explore this technology, as a result, many protocols have been published all over the world.After exploiting articles we focus our vision by number of critical standards that guided us to choose three types of protocols that suit our goals,comparing them brought UniquID as proper candidate by showing us how to move from the current IAM systems and PKIs who relay on the trusted-third-partie to a decentralised system to avoid the challenges posed by the IoT paradigm and demonstrate how the CAP theorem strongly applies to blockchain-based IAMs. Worth of machining the Blockchain technology is currently evolving consequently smart contract as well. As we hopped in the beginning, we did study this protocol and shown the strong points in it as the publishers specified represented in the merge of both the CAP theorem and the scalability, next to the weak side which were an obstacle to promote the data safety for users. We proposed alternatives to level up the performance, and securing it by removing some mechanism and changing actor roles and designed a special smart contract that able to authenticate IoT devices communication between entities. The LWU "Light Weight UniquID" give the advantage of blockchain features to promoted Node as actor changing roles solution, by giving it the chance to become effective in the network.Moreover, to get the right verification of the Special Smart Contract to assure a better version of security,next to this we did specify the new Node services, throw when and how a simple device can elected and configured to assure us what is meant to serve. With that being sad,the LWU is just an extension serve the main purpose of the UniquID platform which is to authenticate the Internet of Things devices based on blockchain technology, not forgetting the risk of the man-in-the-middle attack that mentioned by the platform publishers.

As future work we want to implement the " Light weight UniquID " model in the real-world, and confirm the working solutions that we suggested will have the same success as our theoretical ambition, in addition to secure the selected platform against the man-in-the-middle abuse and test it for denial-of-service attacks.

REFERENCES

[1] Satoshi Nakamoto, Bitcoin: A peer to peer electronic cash system, 2009 (white paper).https://bitcoin.org/bitcoin.pdf.

[2] Yaga, D. , Mell, P. , Roby, N. and Scarfone, K. (2018), Blockchain Technology Overview, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8202.

[3] Kumar, Randhir, and Rakesh Tripathi. "Secure Healthcare Framework Using Blockchain and Public Key Cryptography." (2020): 185-202.

[4] Ouaddah A, Elkalam AA, Ouahman AAIT. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In Europe and MENA Cooperation Advances in Information and Communication Technologies. Springer International Publishing, 2017; 523–533.

[5] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in: 2017 IEEE International Congress on Big Data (BigData Congress), IEEE, 2017, pp. 557–564.

[6] B.-K. Zheng, L.-H. Zhu, M. Shen, F. Gao, C. Zhang, Y.-D. Li, J. Yang, Scalable and privacy- preserving data sharing based on blockchain, Journal of Computer Science and Technology 33 (3) (2018) 557–567. doi:10.1007/s11390-018-1840-5.

[7] M. Conoscenti, A. Vetro, J. C. De Martin, Blockchain for the internet of things: A systematic literature review, in: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), IEEE, 2016, pp. 1–6.

[8] L. Lotti, Contemporary art, capitalization and the blockchain: On the autonomy and automation of art's value, Finance and Society 2 (2) (2016) 96–110.

[9] C. Hammerschmidt, Consensus in Blockchain Systems. In Short, Available: https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe.

[10] Tschorsch, F., Scheuermann, B.: Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutor. 18(3), 2084–2123, 3rd Quart. (2016).

[11] Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfede, S.: Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press (2016).

[12] Tschorsch, F., Scheuermann, B.: Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutor. 18(3), 2084–2123, 3rd Quart. (2016).

[13] Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfede, S.: Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press (2016).

[14] Tschorsch, F., Scheuermann, B.: Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutor. 18(3), 2084–2123, 3rd Quart. (2016).

[15] Kingslin, S.; Zahra, R. An Effective Randomization Framework to POW Consensus Algorithm of Blockchain (RPoW). Int. J. Eng. Adv. Technol. 2019, 8, 1793–1797.

[16] Chaudhry, N.; Yousaf, M.M. Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities. In Proceedings of the 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), Lahore, Pakistan, 19–21 December 2018.

[17] Sharkey, S.; Tewari, H. Alt-PoW: An Alternative Proof-of-Work Mechanism. In Proceedings of the 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), Newark, CA, USA, 4–9 April 2019.

[18] Sayeed, S.; Marco-Gisbert, H. Assessing Blockchain Consensus and Security Mechanisms against the 51 Attack. Appl. Sci. 2019, 9, 1788.

[19] Leonardos, S.; Reijsbergen, D.; Piliouras, G. Weighted Voting on the Blockchain: Improving Consensus in Proof of Stake Protocols. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019.

[20] Chalaemwongwan, N.; Kurutach, W. State of the art and challenges facing consensus protocols on blockchain. In Proceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018.

[21] Ogawa, T.; Kima, H.; Miyaho, N. Proposal of Proof-of-Lucky-Id(PoL) to Solve the Problems of PoW and PoS. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018.

[22] Kiayias, A.; Russell, A.; David, B.; Oliynykov, R. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. Cryptology ePrint Archive, Report 2016/889, 2016.

[23] Komodo White Paper; Technical Report; Komodo Platform. 2018. Available online: https://cryptorating.eu/whitepapers/Komodo/2018- 02-14-Komodo-White-Paper-Full.pdf

[24] Luo, Y.; Chen, Y.; Chen, Q.; Liang, Q. A New Election Algorithm for DPos Consensus Mechanism in Blockchain. In Proceedings of the 2018 7th International Conference on Digital Home (ICDH), Guilin, China, 30 November–1 December 2018.

[25] Do, T.; Nguyen, T.; Pham, H. Delegated Proof of Reputation. In Proceedings of the 2019 International Electronics Communication Conference on (IECC), Okinawa, Japan, 7–9 July 2019; ACM Press: New York, NY, USA, 2019.

[26] Castro, M.; Liskov, B. Practical byzantine fault tolerance and proactive recovery. ACM Trans. Comput. Syst. 2002, 20, 398–461.

[27] Cho, H. ASIC-Resistance of Multi-Hash Proof-of-Work Mechanisms for Blockchain Consensus Protocols. IEEE Access 2018, 6, 66210–66222.

[28] Lamport, L.; Shostak, R.; Pease, M. The Byzantine Generals Problem. ACM Trans. Program. Lang. Syst. 1982, 4, 382–401.

[29] Kwon, J. Tendermint: Consensus without Mining; Technical Report; Cornell University: Ithaca, NY, USA, 2014.

[30] State Machine Replication in the Libra Blockchain; Technical Report; The LibraBFT Team, 2020. Available online: https://developers. diem.com/main/docs/state-machine-replication-paper .

[31] Baird, L. The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance; Technical Report; Swirlds, 2016. Available online: https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf .

[32] Androulaki, E.; Manevich, Y.; Muralidharan, S.; Murthy, C.; Nguyen, B.; Sethi, M.; Singh, G.; Smith, K.; Sorniotti, A.; Stathakopoulou, C.; et al. Hyperledger fabric. In Proceedings of the Thirteenth EuroSys Conference on—EuroSys'18, Porto, Portugal, 23–26 April 2018; ACM Press, New York, NY, USA, 2018.

[33] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains," in Proceedings of the Thirteenth EuroSys Conference, 2018, p. 30.

[34] X. Chen, K. Zhang, X. Liang, W. Qiu, Z. Zhang, D. Tu, Hyperbsa: A high-performance consortium blockchain storage architecture for massive data, IEEE Access 8 (2020) 178402–178413.

[35] S. Omohundro, Cryptocurrencies, smart contracts, and artificial intelligence, AI matters 1 (2) (2014) 19–21.[122] .

[36] A. Berentsen, F. Sch¨ar, The fallacy of a cashless society, in: Beer C., Gnan E., and UW Birchler (Hg.), Cash on Trial, SUERF Conference Proceedings, Vol. 1, 2016, pp. 14–19.

[37] T. Don, T. A. B. Revolution, How the technology behind bitcoin is changing money, business, and the world, Information Systems (2016) 100–150.

[38] R. B ¨ohme, N. Christin, B. Edelman, T. Moore, Bitcoin: Economics, technology, and governance, Journal of Economic Perspectives 29 (2) (2015) 213–38.

[39] G. Prisco, Estonian government partners with bitnation to offer blockchain notarization services to e-residents, Bitcoin Magazine 30 (2015).

[40] J. Liebenau, S. Elaluf-Calderwood, Blockchain innovation beyond bitcoin and banking, Available at SSRN 2749890 (2016).

[41] G. Zyskind, O. Nathan, et al., Decentralizing privacy: Using blockchain to protect personal data, in: 2015 IEEE Security and Privacy Workshops, IEEE, 2015, pp. 180–184.

[42] K. Delmolino, M. Arnett, A. Kosba, A. Miller, E. Shi, Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab, in: International Conference on Financial Cryptography and Data Security, Springer, 2016, pp. 79–94.

[43] F. Idelberger, G. Governatori, R. Riveret, G. Sartor, Evaluation of logicbased smart contracts for blockchain systems, in: International Symposium on Rules and Rule Markup Languages for the Semantic Web, Springer, 2016, pp. 167–183.

[44] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, J. Kishigami, Blockchain contract: Securing a blockchain applied to smart contracts, in: 2016 IEEE international .

[45] Y. Cai, D. Zhu, Fraud detections for online businesses: a perspective from blockchain technology, Financial Innovation 2 (1) (2016) 20.

[46] G. Wood, et al., Ethereum: A secure decentralised generalised transaction ledger, Ethereum project yellow paper 151 (2014) (2014) 1–32.

[47] M. Khazraee, I. Magaki, L. V. Gutierrez, M. Taylor, Asic clouds: Specializing the datacenter, IEEE Micro (2017).

[48] S. Ali, G. Wang, B. White, R. L. Cottrell, A blockchain-based decentralized data storage and access framework for pinger, in: 2018 17th IEEE International Conference

on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), IEEE, 2018, pp. 1303–1308

[49] S. Raval, Decentralized applications: harnessing Bitcoin's blockchain technology, " O'Reilly Media, Inc.", 2016.

[50] N. Z. Aitzhan, D. Svetinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, IEEE Transactions on Dependable and Secure Computing 15 (5) (2016) 840–852.

[51] Genaro,Torija.A, Ramos-Ridao,Requena,Ruiz, Zamorano, M.:A neural network based model for urban noise prediction. J. Acoust. Soc. Am.128(4), 1738–1746 (2010)

[52] M. Chung, J. Kim, The internet information and technology research directions based on the fourth industrial revolution., KSII Transactions on Internet Information Systems 10 (3) (2016).

[53] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, W.-C. Hong, A survey on decentralized consensus mechanisms for cyber physical systems, IEEE Access 8 (2020) 54371–54401.

[54] /T. M. Fernandez-Carames, P. Fraga-Lamas, A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories, Ieee Access 7 (2019) 45201–45218.

[55] A. Badzar, Blockchain for securing sustainable transport contracts and supply chain transparency-an explorative study of blockchain technology in logistics (2016).

[56] Y. Guo, C. Liang, Blockchain application and outlook in the banking industry, Financial Innovation 2 (1) (2016) 24.

[57] A. Bahga, V. K. Madisetti, Blockchain platform for industrial internet of things, Journal of Software Engineering and Applications 9 (10) (2016) 533.

[58] S. A. Abeyratne, R. P. Monfared, Blockchain ready manufacturing supply chain using distributed ledger (2016).

[59] J. Basden, M. Cottrell, How utilities are using blockchain to modernize the grid, Harvard Business Review 23 (2017).

[60] P. K. Sharma, S. Y. Moon, J. H. Park, Block-vn: A distributed blockchain based vehicular network architecture in smart city., JIPS 13 (1) (2017) 184–195.

[61] A. Ekblaw, A. Azaria, J. D. Halamka, A. Lippman, A case study for blockchain in healthcare:“medrec” prototype for electronic health records and medical research data, in: Proceedings of IEEE open big data conference, Vol. 13, 2016, p. 13.

[62] KAMATH, Reshma. Blockchain for Women Next Generation for Sustainable Development Goal 5. Journal of Poverty Alleviation International Development, 2018, vol. 9, no 1.

[63] M. Haferkorn, J. M. Quintana Diaz, “Seasonality and Interconnectivity Within Cryptocurrencies – An Analysis on the Basis of Bitcoin, Litecoin and Namecoin”, Springer International Publishing, Cham, 2014, pp. 106–120.

[64] L. Cocco, A. Pinna, M. Marchesi, “Banking on blockchain: Costs savings thanks to the blockchain technology”, Future Internet, 9 (3), 2017, p. 25.

[65] H. M. Gazali, R. Hassan, R. M. Nor, H. M. M. Rahman, “Re-inventing PTPTN study loan with blockchain and smart contracts”, In: ICIT 2017–8th International Conference on Information Technology, Proceedings pp. 751–754.

[66] G. Papadopoulos, “Blockchain and Digital Payments: An Institutionalist Analysis of Cryptocurrencies”, 2015, pp. 153–172.

[67] J. Dai, M. A. Vasarhelyi, Toward blockchain-based accounting and assurance. J. Inf. Syst. 31 (3), 2017, pp. 5–21.

[68] D. Cawrey, “37Coins Plans Worldwide Bitcoin Access with SMS-Based Wallet”, Online Available: http://www.coindesk.com/37coins-plans-worldwide-bitcoin-access-sms-basedwallet/.

[69] P. Rizzo, “How Kipochi Is Taking Bitcoin into Africa”, Online Available: http://www.coindesk.com/kipochi-taking-bitcoin-africa/.

[70] J. Liu, T. Zhu, “Application of Blockchain Technology in Cultural and Creative Design Education”, International Journal of Emerging Technologies in Learning, 16 (4), 2021.

[71] H. Sun, X. Wang, X. Wang, X, “Application of Blockchain Technology in Online Education” International Journal of Emerging Technologies in Learning, 13(10), 2018.

[72] P. Ocheja, B. Flanagan, H. Ogata, “Connecting decentralized learning records: A blockchain based learning analytics platform,” in Proc. ACM Int. Conf. Ser., 2018, pp. 265–269.

[73] Y. Xu, S. Zhao, L. Kong, Y. Zheng, S. Zhang, Q. Li, “ECBC: A high performance educational certificate blockchain with efficient query,” in Theoretical Aspects of

Computing– ICTAC (Lecture Notes in Computer Science). Cham, Switzerland: Springer, 2017, pp. 288– 304.

[74] M. S. M. Pozi, G. Muruti, A. A. Bakar, A. Jatowt, and Y. Kawai, "Preserving author editing history using blockchain technology," in Proc. 18th ACM/IEEE on Joint Conf. Digit. Libraries (JCDL), New York, NY, USA, Jun. 2018, pp. 165–168.

[75] T. Nugent, D. Upton, M. Cimpoesu, "Improving data transparency in clinical trials using blockchain smart contracts," F1000Research, vol. 5, Oct. 2016, Art. no. 2541.

[76] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," Information, vol. 8, no. 2, p. 44, Jun. 2017.

[77] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," Health Inform. J., doi: 10.1177/1460458218769699.

[78] S. M. Idrees, M. Nowostawski, R. Jameel, "Blockchain-Based Digital Contact Tracing Apps for COVID-19 Pandemic Management: Issues, Challenges, Solutions, and Future Directions", JMIR Medical Informatics. 2021 Feb 9;9(2): e25245.

[79] Idrees, S. M., Nowostawski, M. (2020). Mobile Phone Based Contact Tracing Applications for Combating Covid-19 Pandemic. Biomedical Journal of Scientific Technical Research, 32(4), 25194-25197.

[80] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in Proc. 2nd Int. Conf. Open Big Data (OBD), Aug. 2016, pp. 25–30.

[81] Archa, B. Alangot, and K. Achuthan, "Trace and track: Enhanced pharma supply chain infrastructure to prevent fraud," in Ubiquitous Communications and Network Computing (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering). Cham, Switzerland: Springer, 2017, pp. 189–195.

[82] Idrees SM, Nowostawski M, Jameel R, Mourya AK. Security Aspects of Blockchain Technology Intended for Industrial Applications. Electronics. 2021; 10(8):951.

[83] M. Haferkorn, J. M. Quintana Diaz, "Seasonality and Interconnectivity Within Cryptocurrencies – An Analysis on the Basis of Bitcoin, Litecoin and Namecoin", Springer International Publishing, Cham, 2015, pp. 106–120.

[84] The Decentralized Library of Alexandria, 2015. Online Available, http://www.alexandria.io/.

[85] J. Liu, P. Jiang, J. Leng, “A framework of credit assurance mechanism for manufacturing services under social manufacturing context,” in Proc. 13th IEEE Conf. Automat. Sci. Eng. (CASE), Aug. 2017, pp. 36–40.

[86] M. Król, S. Reñé, O. Ascigil, I. Psaras, “ChainSoft: Collaborative software development using smart contracts,” in Proc. 1 st Workshop Cryptocurrencies Blockchains Distrib. Syst. (CryBlock), New York, NY, USA, 2018, pp. 1–6.

[87] W. Ying, S. Jia, W. Du, “Digital enablement of blockchain: Evidence from HNA group,” Int. J. Inf. Manage., vol. 39, 2018, pp. 1–4.

[88] P. Y. Chang, M. S. Hwang, C. C. Yang, “A blockchain based traceable certification system,” in Security with Intelligent Computing and Big-data Services (Advances in Intelligent Systems and Computing). Cham, Switzerland: Springer, 2017, pp. 363–369.

[89] K. Toyoda, P. T. Mathiopoulos, I. Sasase, T. Ohtsuki, “A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain,” IEEE Access, vol. 5, 2017, pp. 17465–17477.

[90] A. Schaub, R. Bazin, O. Hasan, O. L. Brunie, “A trustless privacy-preserving reputation system”, In IFIP International Conference on ICT Systems Security and Privacy Protection, 2016, pp. 398-411 Springer, Cham.

[91] Conti, M., Sandeep Kumar, E., Lal, C., Ruj, S.: A Survey on security and privacy issues of bitcoin. IEEE Commun. Surv. Tutor. 20(4), 3416–3452, Fourth quarter 2018.

[92] Ertem Osmanoglu - Identity and Access Management Business Performance Through Connected Intelligence-Syngress (2013).

[93] M. Samaniego, R. Deters, “Blockchain as a Service for IoT”, In: Proceedings – 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, iThings-GreenComCPSCom-Smart Data 2016, pp. 433–436.

[94] Oxford Dictionaries, Definition of “Internet of Things”. https://www.lexico.com/en/definition/internet-of-things.

[95] Muccini, H. and T. Moghaddam, M. (2018). IoT Architectural Styles, pages 68–85. 12th European Conference on Software Architecture, ECSA 2018.

[96] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys Tutorials, 17(4):2347–2376.

[97] Pan, J. and McElhannon, J. (2018). Future edge cloud and edge computing for internet of things applications. IEEE Internet of Things Journal, 5(1):439–449.

[98] Cisco (2014). The Internet of Things reference model. http://cdn.iotwf.com/resources/71/IoT Reference Model White Paper June 4 2014.pdf.

[99] Ray, P. (2018). A survey on internet of things architectures. Journal of King Saud University - Computer and Information Sciences, 30(3):291 – 319.

[100] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., and Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5):1125–1142.

[101] Alshohoumi, F., Sarrab, M., Al-Hamdani, A., and Al-Abri, D. (2019). Systematic review of existing iot architectures security and privacy issues and concerns. International Journal of Advanced Computer Science and Applications, 10.

[102] Wu, M., Lu, T.-J., Ling, F.-Y., Sun, J., and Du, H.-Y. (2010). Research on the architecture of internet of things. In 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), volume 5, pages V5–484. IEEE.

[103] Sethi, P. and Sarangi, S. (2017). Internet of things: Architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017:1–25.

[104] Pisching, M., Pessoa, M., Junqueira, F., Santos Filho, D., and Miyagi, P. (2018). An architecture based on rami 4.0 to discover equipment to process operations required by products. Computers and Industrial Engineering.

[105] Durán-Sánchez, A., et al. (2017) Sustainability and Quality of Life in Smart Cities: Analysis of Scientific Production. In: Sustainable Smart Cities. Creating Spaces for Technological, Social and Business Development, Springer, Berlin, 159-181.

[106] Kshetri, N.: Can blockchain strengthen the internet of things? IT Profes- sional 19(4), 68–72 (2017). https://doi.org/10.1109/MITP.2017.3051335, doi. ieeecomputersociety.org/10.1109/MITP.2017.3051335.

[107] Roman, R., Zhou, J., Lopez, J.: On the features and challenges of secu- rity and privacy in distributed internet of things. Computer Networks 57(10), 2266 – 2279 (2013).

[108] Ouaddah, A., Abou Elkalam, A., Ait Ouahman, A.: Fairaccess: a new blockchain-based access control framework for the internet of things. Security and Com- munication Networks 9(18), 5943–5964.

[109] Aafaf Ouaddah, Hajar Mousannif, Anas Abou Elkalam, Abdellah Ait Ouahman,Access control in the Internet of Things: Big challenges and new opportunities,Computer Networks,Volume 112,2017,Pages 237-262,ISSN 1389-1286,

[110] Novo, O.: Blockchain meets iot: An architecture for scalable access manage- ment in iot. IEEE Internet of Things Journal 5(2), 1184–1195 (April 2018).

[111] Le, T., Mutka, M.W.: Capchain: A privacy preserving access control frame- work based on blockchain for pervasive environments. In: 2018 IEEE Interna- tional Conference on Smart Computing (SMARTCOMP). pp. 57–64 (June 2018).

[112] Giaretta A., Pepe S., Dragoni N. (2019) UniquID: A Quest to Reconcile Identity Access Management and the IoT. In: Mazzara M., Bruel JM., Meyer B., Petrenko A. (eds) Software Technology: Methods and Tools. TOOLS 2019. Lecture Notes in Computer Science, vol 11771. Springer, Cham. https://doi.org/10.1007/978-3-030-29852-4-20

[113] esse Leimgruber, A.M., John Backus, Bloom Protocol: Decentralized credit scoring powered by Ethereum and IPFS. 2018.

[114] M. Ali, R.S., J. Nelson and M. J. Freedman, Blockstack: A New Internet for Decentralized Applications (Whitepaper). 2017.

[115] Digital, I.O., I/O Digital Application Based Blockchain Whitepaper. 2016.

[116] Conner Fromknecht, D.V., Sophia Yakoubov CertCoin: A NameCoin Based Decentralized Authentication System. 2014.