ANKARA YILDIRIM BEYAZIT UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

ANALYZING OF DISTRIBUTED APPLICATION DEVELOPMENT PLATFORMS ON BLOCKCHAIN TECHNOLOGY

M.Sc. Thesis by

Hilal Nur ISSI

Department of Computer Engineering

December, 2019

ANKARA

ANALYZING OF DISTRIBUTED APPLICATION DEVELOPMENT PLATFORMS ON BLOCKCHAIN TECHNOLOGY

A Thesis Submitted to

The Graduate School of Natural and Applied Sciences of

Ankara Yıldırım Beyazıt University

In Partial Fulfillment of the Requirements for the Degree of Master of Science

in Computer Engineering, Department of Computer Engineering

by

Hilal Nur ISSI

December, 2019

ANKARA

M.Sc. THESIS EXAMINATION RESULT FORM

We have read the thesis entitled **"ANALYZING OF DISTRIBUTED APPLICATION DEVELOPMENT PLATFORMS ON BLOCKCHAIN TECHNOLOGY"** completed by **HILAL NUR ISSI** under supervision of **Dr. AHMET ERCAN TOPCU** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Dr. Ahmet Ercan TOPCU

Supervisor

Dr. Ali Osman ÇIBIKDİKEN

(Jury Member)

Dr. Mustafa YENİAD

(Jury Member)

Prof. Dr. Ergün ERASLAN

Director

Graduate School of Natural and Applied Sciences

ETHICAL DECLARATION FORM

I hereby declare that, in this thesis which has been prepared in accordance with the Thesis Writing Manual of Graduate School of Natural and Applied Sciences,

- All data, information and documents are obtained in the framework of academic and ethical rules,
- All information, documents and assessments are presented in accordance with scientific ethics and morals,
- All the materials that have been utilized are fully cited and referenced,
- No change has been made on the utilized materials,
- All the works presented are original,

and in any contrary case of above statements, I accept to renounce all my legal rights

Date : **Signature:** …….

Name&Surname: Hilal Nur ISSI

ACKNOWLEDGMENTS

Firstly, I would like to express my sincere gratitude to my supervisor, Dr. Ahmet Ercan TOPCU for his support and motivation during my study. I, also, would like to Dr. Ali Osman ÇIBIKDİKEN for his support and motivation during the writing process of my thesis. Their guidance assisted me all the time in my research and while writing this thesis.

I would like to express my sincere feeling to my family for their emotional and physical supports while I am working on this research. In this hard and long study time, my family always gives me support whenever I need them always near me.

December, 2019 **Hilal Nur ISSI**

ANALYZING OF DISTRIBUTED APPLICATION DEVELOPMENT PLATFORMS ON BLOCKCHAIN TECHNOLOGY

ABSTRACT

In the last decade, the most important research area is the blockchain technology because of its distributed consensus, decentralized, anonymity properties, and peer to peer transaction. Problems such as regulatory and technical challenges can be covered by blockchain technology. In other words, blockchain can provide a secure, easily accessible, and tamper-proof network in the distributed ledgers. It is a published record of transactions, all over a network of users. Mohanta (2018) writes that Satoshi Nakamoto expresses peer to peer cash transaction in distributed system in 2008, and after the idea of cryptocurrency grew rapidly. Currently, there are 1639 different types. There is no limit for using areas in blockchains such as the pharmaceutical industry, smart contracts, logistics, banking, and cybersecurity.

More than three-quarters of researches on blockchain-related are focused on the financial part of blockchain like Bitcoin. The remaining part of researchers is trying to research the smart contract based blockchain platforms and how these innovations can affect daily life. This thesis primarily focuses on the blockchain platforms which are used a smart contract system. To identify the goal, a comparison of platforms with each other in terms of specific and innovative features is used as a purpose. Another purpose of this thesis is that giving an idea of which platform is appropriate for what kind of problems and sectors. To reach these goals, the first technic is used by this thesis is a literature review. We look at the literature on what is going on the academia in terms of our aims. Then, we look at the example of real-time applications or proposed by researches for improving the current daily living standards. The last method we use is collecting all this information in one common environment and analyzing it. Our conclusion of this research is given the flowchart of six common blockchain platforms in terms of their features for specific problems and sectors. These six smart contract-based blockchain platforms are compared with sickle features to decide which platform is suitable for which sector and problem. All

outputs are represented as a comparison table. During this thesis six common platforms which are Hyperledger, Ethereum, Corda, IOTA, Stellar and Ripple are researched.

Keywords: Distributed ledger, blockchain, smart contract, security, privacy, comparison, consensus.

BLOKCHAIN TEKNOLOJİSİNDE DAĞITILMIŞ UYGULAMA GELİŞTİRME PLATFORMLARININ ANALİZİ

ÖZ

Son on yılda, en önemli araştırma alanı dağıtılmış fikir birliği, merkezi olmayan, anonimlik özellikleri ve eşler arası işlem nedeniyle blockchain teknolojisidir. Düzenleyici ve teknik zorluklar gibi sorunlar blockchain teknolojisi ile ele alınabilir. Başka bir deyişle, blockchain dağıtılmış defterlerde güvenli, kolay erişilebilir ve kurcalamaya dayanıklı bir ağ sağlayabilir. Bu, bir kullanıcı ağı üzerindeki işlemlerin yayınlanmış bir kaydıdır. Mohanta (2018), Satoshi Nakamoto'nun 2008 yılında ve kripto para birimi fikrinin hızla büyüdükten sonra dağıtılmış sistemdeki eşler arası nakit işlemini ifade ettiğini yazıyor. Şu anda 1639 farklı tip var. İlaç endüstrisi, akıllı sözleşmeler, lojistik, bankacılık ve siber güvenlik gibi blok zincirlerindeki alanların kullanımı için herhangi bir sınırlama yoktur.

Blockchain ile ilgili araştırmaların dörtte üçünden fazlası Bitcoin gibi blockchain'in finansal kısmına odaklanmıştır. Araştırmacıların geri kalan kısmı, akıllı sözleşme tabanlı blockchain platformlarını ve bu yeniliklerin günlük hayatı nasıl etkileyebileceğini araştırmaya çalışıyor. Bu tez öncelikle akıllı bir sözleşme sistemi kullanılan blockchain platformlarına odaklanmaktadır. Hedefi belirlemek için platformların belirli ve yenilikçi özellikler açısından birbirleriyle karşılaştırılması amaç olarak kullanılır. Bu tezin bir diğer amacı, hangi platformun ne tür sorunlar ve sektörler için uygun olduğuna dair bir fikir vermektir. Bu hedeflere ulaşmak için bu tez tarafından kullanılan ilk teknik bir literatür derlemesidir. Akademide neler olup bittiğine dair literatüre amacımız açısından bakıyoruz. Ardından, mevcut günlük yaşam standartlarını iyileştirmek için gerçek zamanlı uygulamalara veya araştırmalar tarafından önerilen örneğe bakıyoruz. Son kullandığımız yöntem tüm bu bilgileri tek bir ortak ortamda toplamak ve analiz etmektir. Bu araştırmanın sonucuna, altı yaygın blok zincir platformunun belirli sorunlar ve sektörler için özellikleri açısından akış şeması verilmiştir. Bu altı akıllı sözleşmeye dayalı blok zincir platformu, hangi platformun hangi sektör ve sorun için uygun olduğuna karar vermek için orak özellikleri ile karşılaştırılır. Tüm çıktılar bir karşılaştırma tablosu olarak temsil edilir. Bu

tez sırasında Hyperledger, Ethereum, Corda, IOTA, Stellar ve Ripple olmak üzere altı ortak platform araştırılmıştır.

Anahtar Kelimeler: Dağıtık defter, Blok zincir, Akıllı sözleşme, Bilgi güvenliği, Kişisel verilerin korunması, Karşılaştırma, consensus.

NOMENCLATURE

Acronyms

DLT	Distributed Ledger Technology
SMs	Smart Contracts
PoW	Proof-of-Work
PoS	Proof-of-Stake
p2p	Peer--to-peer
IoT	Internet of Things
IIoT	Industrial Internet of Things
DNS	Domain Name Service
DApps	Decentralized Applications
TEE	Trusted Execution Environment
KYC	Known-your-customer
EVM	Ethereum Virtual Machine
JVM	Java Virtual Machine
NIST	National Institute of Standards and Technology
SBFT	Simplified Byzantine Fault Tolerance
MSP	Membership Service Provider
PoET	Proof of Elapsed Time
PBFT	Byzantine Fault Tolerant
M2M	Machine-to-Machine
DAG	Directed Acyclic Graph
SCP	Stellar Consensus Protocol
FBA	Federated Byzantine Agreement

LIST OF TABLES

LIST OF FIGURES

CONTENTS

CHAPTER 1

INTRODUCTION

The idea of a fully independent, self-contained, autonomous, self-validating application that is not immediately or ultimately linked to network communication becomes almost incredible. In the past, it was dependent on providing isolated defenses like keeping something safe, usually placing it in a physical vault or otherwise isolating it from external access.

According to the Gartner Hype Cycle for Emerging Technologies, blockchain technology considers as a mature, adaptive, and use of specific technology, and located in fifth-order between technologies [10, 13]. The innovative combination of existed computer paradigms creates blockchain technology. Blockchain has 2500 patents and gets around $1.3 billion investment form 25 different countries. Klaus Schwab, Founder and Executive Chairman of the World Economic Forum, defines blockchain technology is a ledger system that is secure, shared, and programmable ledger that no single user controls and which can be inspected by anyone. And they represent their ideas about the blockchain in (Figure 1.1)

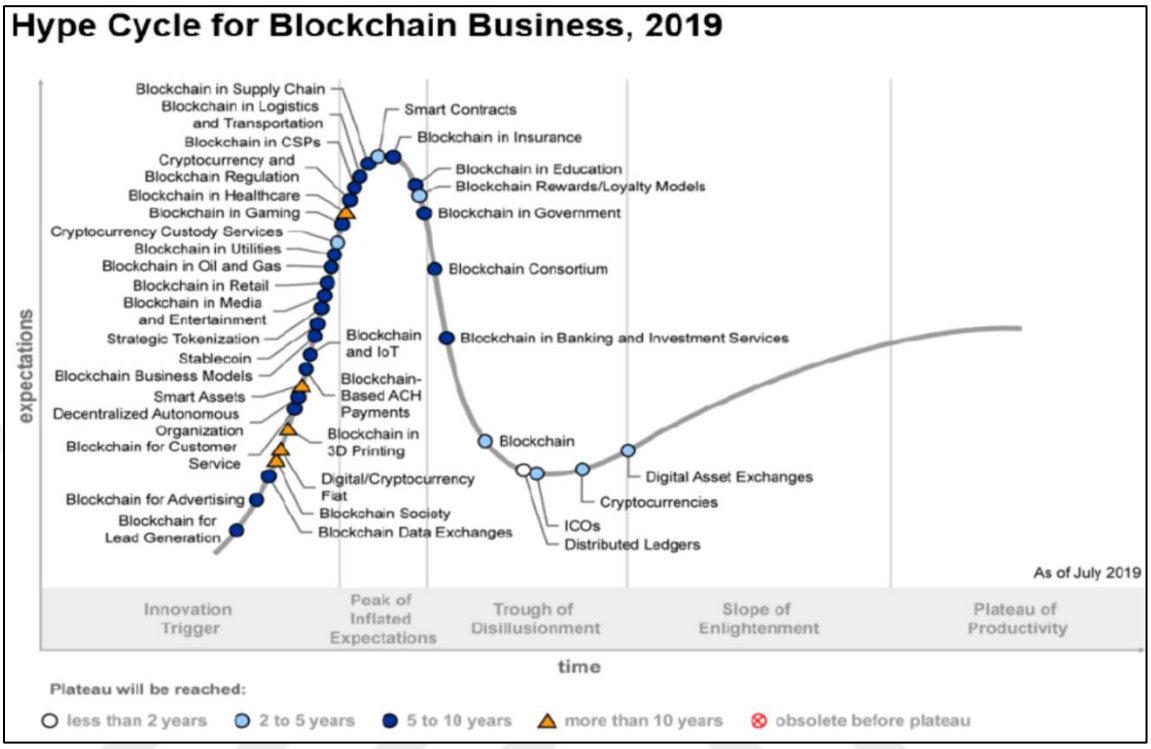


Figure 1.1. Gartner hype cycle for blockchain technologies

Blockchain is peer-to-peer networks technology that uses distributed and decentralized public ledger. The main point of blockchain is that all nodes have a distinctive and timestamp a cryptographic signature. The previous block's information is located in the next block in the chain. As a result, blockchain ensures that all blocks have the same set of transactions (Figure 1.2.) This way transactions can be traced, immutable and auditable. Blockchain has received considerable attention recently. The origin of blockchain technology is coming from the first cryptocurrency Bitcoin which is announced by Satoshi Nakamoto in 2009. A possible use case of blockchain is exceeded the financial and cryptocurrency assets.

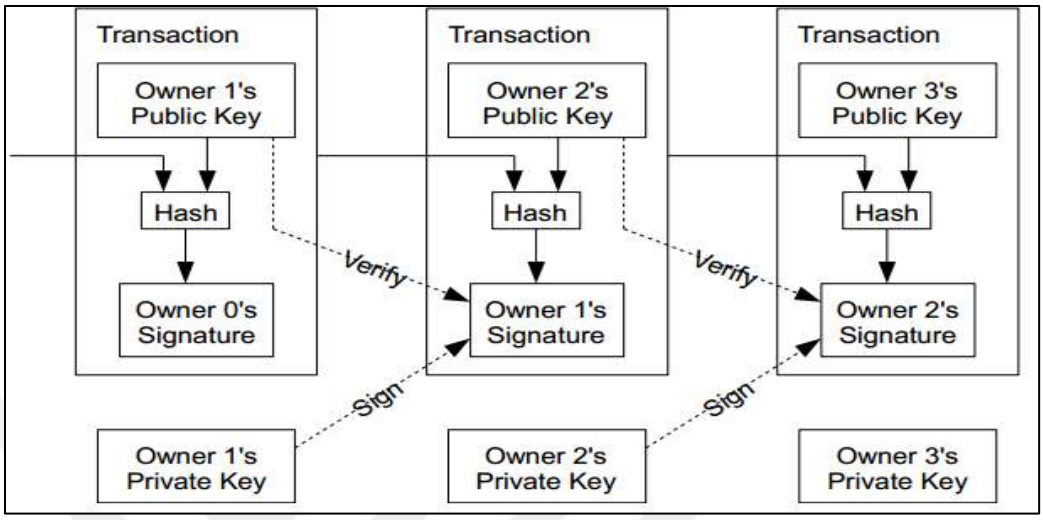


Figure 1.2. Blockchain's main working mechanism

Taylor et.al. (2019) recently, academicians, developers, and researches are interested in blockchain technology because of its secure, private, reliable and unique characteristics. There is no limit for using areas in blockchains such as the pharmaceutical industry, smart contracts, logistics, banking, and cybersecurity [23].

According to researchers, there are three stages in the development of blockchain technology in the literature: blockchain 1.0, blockchain 2.0 and blockchain 3.0.

In the blockchain 1.0 stage, the primary focus is cryptocurrency. Bitcoin is the first cryptocurrency, but after that blockchain environment has become a host over 700 types of cryptocurrencies like Dogecoin, Litecoin. The entire market capitalizations of them are over 26 billion US$.

In the blockchain 2.0 stage, blockchain can use the smart contracts (SCs) which are known as Turing-complete programming languages. Szabo explains the idea of Smart Contract in 1994 as a contract can achieve terms and computerized transaction protocol [30], provides an ambiance for implementing terms of traditional contracts [30]. Smart contracts with Blockchains decentralized consensus mechanism provide shared trusting users to complete data exchange or processing without the need for any third-party trusted

authority. It, also, supply a less costly implementation of some real-world problems and makes the more flexible platform. Figure 1.3 shows the how blockchain uses the smart contract.

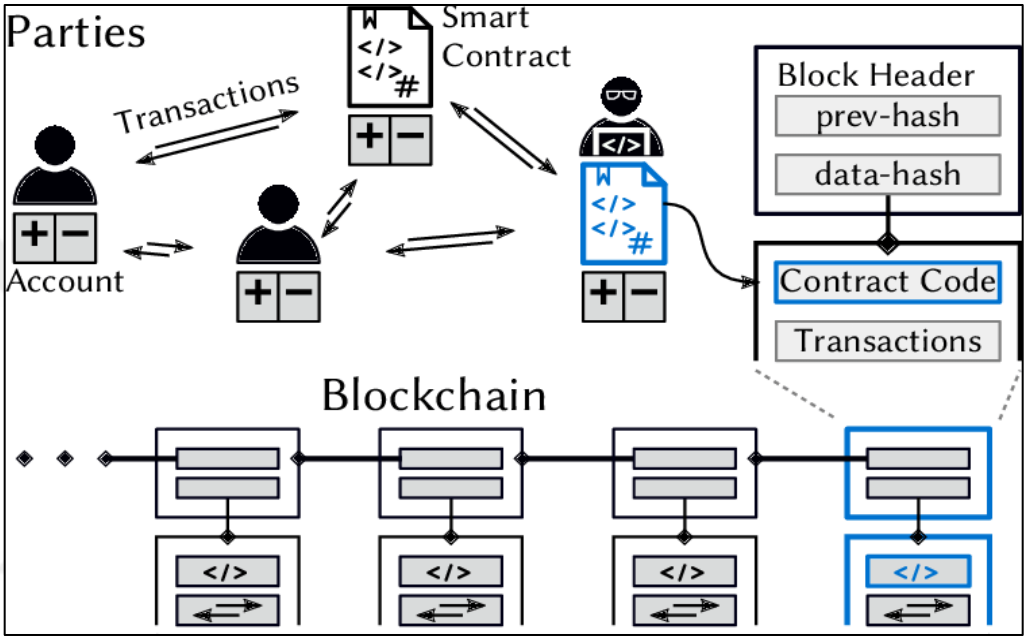


Figure 1.3. Blockchain smart contract working mechanism

Smart contracts supply automated, deterministic program units for handling various modules in a specific way and triggering related events. The primary structure of the blockchain is that each transaction is confirmed by the nodes and transactions are secured by cryptography hash function. While in blockchain previous transactions can be seen openly in the system, no one can delete or modify these transactions. With this feature, Blockchain is a transparent system. In the traditional approach in blockchain systems, all nodes have the same information on the blockchain database. Thus all peers are in consensus in terms of stored data.

In the blockchain 3.0 stage, blockchain technology together with the previous two stage runs various areas such as health, IoT, science, and government.

Chen et al. (2019) showed that in the industry, the growing capacity of blockchain is the main problem. Many people try to resolve it from different aspects, like Lightning Network, sidechains, Hard Fork, SegWit, etc. The main ideas of solving problems are to bypass the restrictions and keep the existing ceiling unchanged [9].

For more secure, reliable, transparent, and self-regulating networks, developers can use the digital ledger database. The blockchain system makes the supply chain sector more trustful and reliable, everything is nowadays in the open system in a distributed manner.

On the organizing and lawful side, many issues have been raised in terms of risk, security, and privacy. It is main that the true balance is achieved between the quick development and legal stability of Blockchain technology, assuring that the organizing and lawful format do not obstruct discovery in this space.

CHAPTER 2

LITERATURE REVIEW

The article, published by W. Scott Stornetta and Stuart Haber in 1991, explains how to use documents with crypto signatures and time stamps. Additionally, the article which is published by Ross Anderson in 1996 describes a decentralized storage system where saved updates cannot be deleted. In the peer-to-peer networks, records for blockchain transactions are located at various distributed nodes. Each separate node is the part of verifying and protection the blockchain. These distributed networks are no longer vulnerable in terms of centralized databases or files. Figure 2.1 shows the main architecture of Central, decentral and distributed networks.

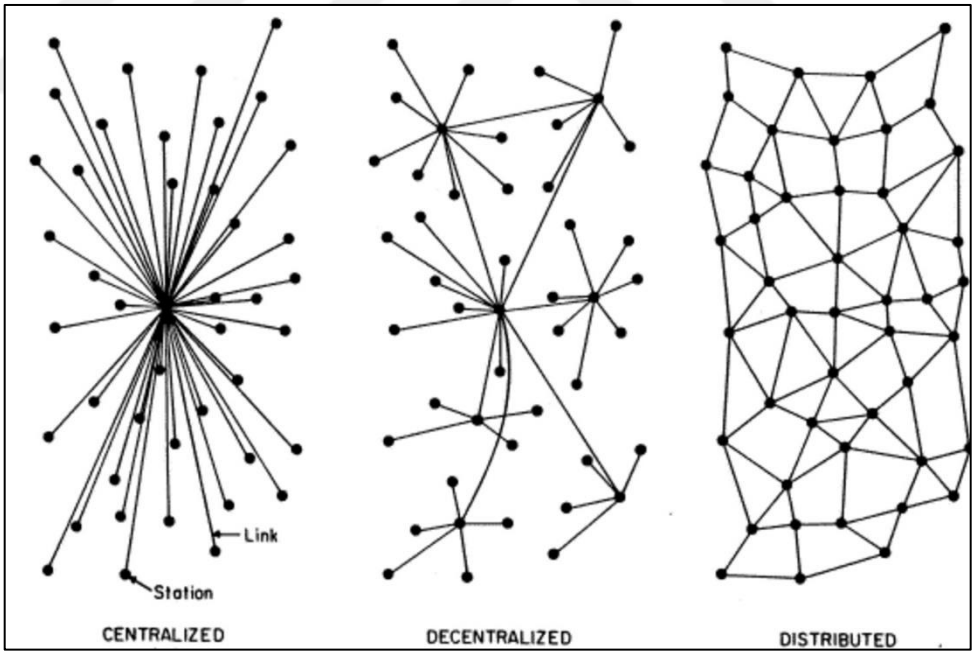


Figure 2.1. Architecture of Centralize, Decentralized and Distributed networks

The digital store up platform and confirm the entire background of transactions between users across the network is Blockchain. The blockchain technology presents an extraordinary success, in that it mediatize the idea of the sequentially connecting archive

in a fixed “hash-chain” with anti-spam algorithms and novel economic incentives, in a way that let the users to transfer signs between themselves while refraining from central authorities and censorship tools. From a technical point of view, Blockchain is “a database that consists of chronologically coordinated bundles of transactions familiar as blocks,” against which any recommended the transaction can be checked with reliance on the integrity of any particular block. Once recorded, the data can never be changed or deleted. It has been defined as together with a database and a network, provides built-in internal integrity and security. On the theoretical side, Blockchain technology has the potential to change trust-based transactions based on mathematically defined and mechanically applied rules.

To start the transaction, participants create and "sign off" the transaction using the agents' private keys. This marks the process as original. This event has broadcast the network and timestamped. Identify the pending transaction node is not easy to process. To create a new block is so hard because network has to ensure that new blocks have to publish nearly every 10 minutes. Once the nonce solution is known, verifying that the “winner” node is computationally fast. Provided that the transactions contained within the block are valid, the recently created block is then attached to the blockchain by the winning node (Figure 2.2.) The process increases the blockchain's size. Distributed ledger technologies (DLTs) use a number of various consensus processes such as proof of stake (PoS) and proof of work (PoW). In this way, blockchain ensure that it can block the malicious attack and provide a secure platform.

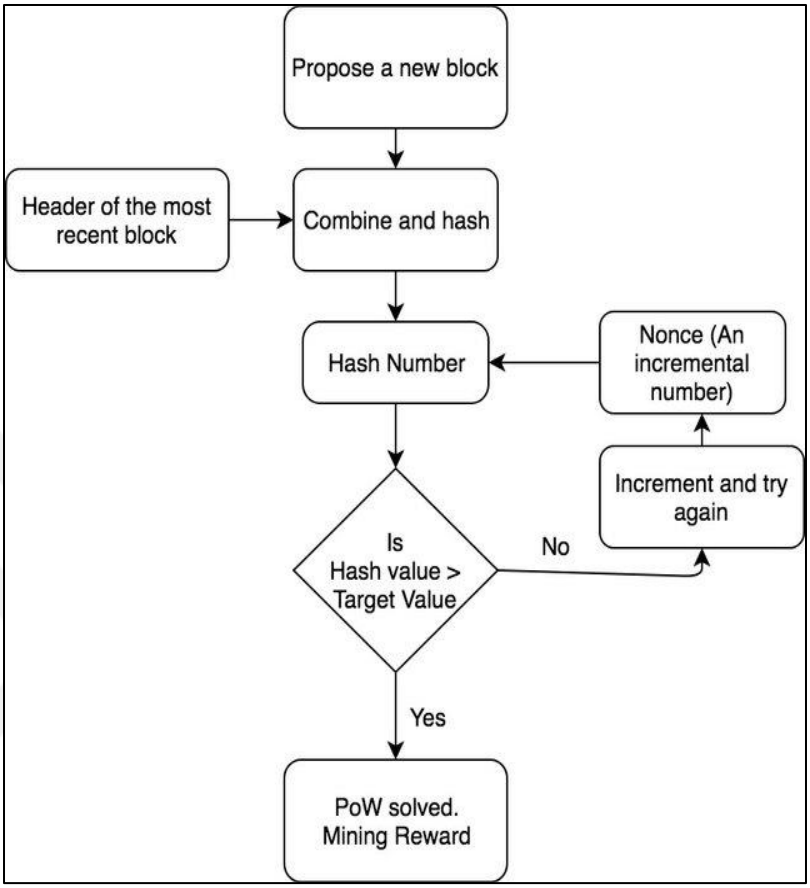


Figure 2.2. Algorithm of proof-of-work consensus protocol

Nash (2018) said that the results of the International Data Corp. Distribution shows while the market value of Blockchain is $945 million in 2017, Blockchain technologies value in the market reached $2.1 billion ends of 2018. According to Gartner survey, more than half of the answerer thought that in the future, blockchain can be a platform for plan investment and business disruption [28]. In 2016, there are 26,000 blockchain projects are running and this is the only 8% of the whole possible projects. This number is growing rapidly in 2017 [3]. The main problems of developing projects are scalability, technological uncertainty, and cost of development. The technology seems far from reaching its impute potential. The symptoms of the Internet in the 2000s years, becoming the most acceptable platform between people, can be seen in blockchain nowadays.

In 1994 Nick Szabo announce the idea of smart contract, which has tamper-resistant properties, self-executing, and self-verifying. To reduce the cost and ensure the security in real-time applications in blockchain, smart contracts are used. This way, code does not need to third parties' confirmation. For development, integration of smart contract in the blockchain is the primary focus area because database and peer to peer transactions can be located in the public environment without any security problems. Smart contracts are unalterable, trackable and irreversible. Blockchain technology together with smart contracts can provide secure and low costly real-time application platforms.

Mainly symposiums and conferences are the platforms for publishing the blockchain papers. Ernst thought that conferences are considered as a most environment for respectable publications and these publications can determine the way of computer science in the future [5]. International Conferences, IEEE-hosted conferences, ACM hosted conferences, Financial Data Security and Cryptography or symposiums are the source of paper which have high cited rates. Another source for paper is the journals. Topics among the most respected are Cryptology, ACM, Computer Networks, Communications and Cryptography [8].

In GitHub is home around 6,500 blockchain projects in 2018. These projects developed for different purposes and used technology, protocols, platforms, consensus, privacy and programming languages to show differences between the projects. A study by Credit Suisse (2016) clearly expresses the goals of blockchain leaders. These aims are the reduction in the costs of stock, lower settlement time, decrease of operational costs, and new revenue opportunities [22]. As a result, this innovation is the center of increasing interest [42]. Almost one-third of C-suite administrators announce that they already adjust the blockchain or are thinking the way of using that [33]. Developers and researchers are informed of the capabilities of the new technology and discover a variety of implementation across a wide range of industries [11]. Many industrial companies and academicians have lots of predictions for blockchain technology. Chen (2018) said that well-known companies, including Google, and Alibaba already have published a project run on the blockchain so, in the future, the blockchain will be a very factual technology.

Yli-Huumo et al. managed an SLR in 2016 to decide what results of research were published on the communal idea of blockchain technology. This research showed while the fourth of five papers focus on privacy and security topics in Bitcoin applications, only 20% of papers discussed the smart contract and blockchain applications. However, this trend changed after 2016, developers started to use different types of blockchain platforms for various purpose.

Finance is still the most popular area in blockchain applications. Blockchain is supposed to play a critical part in bringing advantage to consumers, the sustainable improvement of the global economy, conducting advantages for the whole society in general and the current banking system [20]. Some applications such as Factom, digital document management platform, Maidsafe which is a distributed data network, Binded- copyright protection system- and ADEPT that is autonomous decentralized P2P telemetry for IoT is developed a focus on integrity and invariance blockchain properties [10].

Wang et al. (2019) analyze the effect of blockchain on the supply chain direct meetings with supply chain experts. Experts believe that creating a secure, transparent, and confident supply chain is possible with blockchain [43]. According to Deloitte survey (2016) [15], around half of the companies in manufacturing and consumer goods decided to invest more than $5 million on the blockchain technology in 2017. Ying, Jia, and Du (2018) [23] managed a study on going blockchain-enabled e-commerce platform in a holding and said that blockchain enables corporations to publish their cryptocurrencies and protect delicate information. To improve the transparency and efficiency in the supply chain, some example blockchain projects have been started. These projects are increasing day by day [27]. The collaboration of Nestlé and Walmart with IBM implement projects on food traceability and safety is running on blockchain platforms. UPS, Maersk, and FedEx are planning to develop a project for shipping. Mackey and Nayyar (2017) [16] discuss how they can discover the counterfeits in the pharmaceutical supply chain with different common and innovate technologies like Blockchain. They claim that literature has not enough source on this subject nevertheless, some industrial and governmental

actions promise the answers for the pharmaceuticals industry using blockchain such as Parexel [42], iSolve [37], and Blockverify [39, 44].

Some researches specifically focus on the data-intensive and decentralized features of blockchain for using controlling big data in a decentralized fashion [26] and IoT [18, 24, 29] According to researches [23, 34], in 2017 the rate of using blockchain for security mechanisms in the IoT rose from 9% to around 19%. Near the end of 2016, Conoscenti et al. managed an SLR focussing on the adaptability and use of blockchain particularly regarding IoT and other peer-to-peer devices. Smith and Hardjono (2016) [21] recommend a privacy-preserving system that uses blockchain and IoT networks to indicate resource generation without third-party certification. Blockchain can get better working efficiency and productivity of IIoT (Industrial IoT) owing to a smart contract that gives permission machines to manage themselves. Nearly a quarter of the answerer said that the most suitable solution for proving IIoT devices security is the blockchain applications [21, 33]. Xage [28] is the world's first industrial Internet of Things (IIoT) platform derived from blockchain technology. It can get better operational efficiency and productivity through this kind of random p2p machine communication, providing machines to control themselves. With the distributed ledger of the blockchain in which a single corporation has no control, different attention of members in a supply chain can be placed in a public registry. Today's problems of accountability and revelation can be reduced by blockchain [19].

To improve reliability and security via the hardware and software solutions in distributed networks can be used Blockchain technology [17, 24, 30]. For example, SIRIN LABS [20] is the pioneer inventor of the first blockchain-based smartphone, capable of supplying secure, fee-lees, fast and reliable transactions. Another project is the antimalware blockchain-based solution, BitAv, which recognize virus pattern distribution [17]. To provide security against malicious attacks or single point of failure, In Axon (2015) [6] which is a privacy-sensitive public key infrastructure is implemented. Liang et al. (2018) [7] propose the idea and implementation of a distributed blockchain-based conservation framework to increase the security of contemporary power systems against cyber-attacks.

All these applications are developed on different blockchains without common standards. The International Organization for Standardization determines the ISO/TC 307 global standard for blockchain [39].

Personal information administration has always been an inevitable part of human society's work and life. It has covered various areas such as school students and teachers, national credit information systems, registration the airplanes and hotels, and file management of the government employees and company. Governments and companies started to think about how they can store these huge data with high security [22, 26, 31]. To provide combine social, physical, and business infrastructures in the idea of a smart city, blockchain platforms could use [21, 26, 29]. Barnett (2016) [4] is identifying various uses of blockchain in the construction industry. These scenarios of use can be listed like Multisignature Transactions, keep digital property records, Smart Contracts, timestamping transactions or acts, and Smart Oracles, a real-world repository of knowledge to be used in concurrence with smart contracts. The use of blockchain in smart cities [8], automated dispute resolution and real estate investment [7, 9] has also been predicted. The Blockchain for Cities research tries to make up the 'people's layer', which does not exist in the city today, using blockchain technology as an integration mechanism. The Canadian government supports to work with blockchain frameworks and starts a platform for marijuana surveillance [23]. In 2014, McMillan proposed a system The World Citizen project is a project for decentralized passport service to recognize citizens from all over the world [10, 17]. Some governmental services can be implemented in blockchains like marriage records, income taxation systems, and patent administration [17]. The same UNEP (2016) and other authors confirm that blockchain applications tested in West have some positive outcomes in the global perspective [27, 28].

In the healthcare industry, Blockchain technology could play a crucial role with various applications in areas like automated health claims adjudication, drug counterfeiting, public healthcare management, user-oriented medical research, longitudinal healthcare records, clinical trial, sharing patients' medical data, precision medicine, and online patient access [6, 9, 11, 17, 23, 25, 29, 36]. Researches aspect that endpoint switching, selective

publication, missing data, patients' informed consent, and data dredging can be solved by using blockchain and smart contracts together[23, 27]. A healthcare platform is announced in Estonia. This platform developed using blockchain together with Guardtime Company. With this platform, Estonian healthcare providers, citizens, and health insurance companies can get entire medical treatments performed in Estonia [7, 11].

Namecoin is a decentralized and open-source form of DNS which uses blockchain technology [15, 17]. Alexandria ensures a decentralized, open-source, secure, and blockchain-based platform for a kind of library [19]. This two systems may be improved usage of digital personality services which can affirm personal identities, allowing anonymity and security in a standardized verification model [17, 23].

With the help of Blockchain, privacy, security and vulnerability concerns can solve in the case of universal learning environments [8] and educational records related to prestige prize can be stored safely [12, 17, 29]. Sharples and Domingue (2016) [12] recommend the use of a blockchain-based distributed system for academic prestige and record. Dennis and Owen, 2015 [12] and Carboni (2015) [13] show similar reputation systems.

The research by Ying, Jia, and Du (2018) documents the innovation in China. Hainan Airlines (HNA) group implemented commercial blockchain applications. This e-commerce system using blockchain provides an environment for employees getting their needs directly from third-party suppliers [22]. After started using this system in February 2015, it takes attention from other researchers and consider as a successful innovation [24, 29].

Another area for using blockchain is Blockchain as a service (BaaS), which is expected increase productivity. Amazon, IBM, and Microsoft Azure are the service provider of the distributed systems and to adopt the blockchain as a Service idea is easier for them. According to a survey by Gartner (2016), ‘‘23 percent of CIOs said that blockchain requires the newest skills to implement any technology area, while 18 percent said that blockchain skills are the most difficult to find’’.

Furthermore, how to cope with the countless legal requirements in all the different countries is still unclear. With the innovation of blockchain, academician started to discuss how data should be stored in the blockchain in terms of security, privacy, and transparency. They, also, talked about which data should be stored in system by law? [17, 19].

In most blockchains, the SHA-256 algorithm which would need 2128 operations to crack using Grover's algorithm with the help of a quantum computer, is used for the hash algorithm. The ECDSA algorithm will break when a quantum computer is installed large enough to render almost all blockchains unsafe. Currently, post-quantum cryptographic primitives are the newest discussion topic between scholars [23, 26].

CHAPTER 3

BLOCKCHAIN SMART CONTRACTS PLATFORMS

Over the last few years, blockchain architecture has started to promote smart contracts which are the Turing-complete codes run on the blockchain [21]. The success of Bitcoin in the academic and practical platforms can proof that blockchain technologies have promised huge research potential. Hildenbrandt et al. (2018) showed that the blockchain-based systems can set up approach a wide range of various problems, such as academic research focus on consensus protocols, distributed storage, currency and more. Luu et al. (2019) said that in contrast to classic distributed platforms, smart contract platforms run in open or permissionless networks into which random candidates join.

3.1. Ethereum

Guo, Meamari, and Shen (2018) explained Ethereum which is a distributed computing platform highlighting smart contract functionality is proposed by Vitalik Buterin, a cryptocurrency programmer and researcher, in 2013. Ethereum development was invested by an online crowded sales event between July and August 2014, and the official system was released on July 30, 2015 [5, 8]. It has reached 1 billion dollars since its launch in July 2015.

Valenta and Sandner (2017) explain the general working criteria of Ethereum which builds the generalized technology, or technology on which all process-based state machine concepts can be built. Furthermore, it provides to the end-developer a firmly integrated end-to-end system for implementing the application on a hitherto unique computer pattern in the mainstream: a trustful object messaging computer framework [11]. The open blockchain platform of Ethereum allows execution, creation, and using decentralized applications (DApps). Similar to Bitcoin, network contributors broadcast operations on the network and are then grouped into blocks with different nodes, called miners and

connected to the blockchain using a proof of work (PoW) consensus mechanism [15, 16]. Together these features, this platform can develop state-of-art transactional applications that ensure transparency, trust, and accountability, while the application's core focuses on legal constraints and business processes. The Ethereum leans on a proof-of-work mining process and developed for higher standards of security against denial of service attacks. Ethereum uses Ether as a cryptocurrency. All ether equilibria and values are indicated in Wei units: 1 ether is 1e18 Wei.

Rapid development time has been developed with special emphasis on the safety of applications and the ability to communicate effectively with different applications. To support this, Ethereum provides a platform for promoting a “Turing complete” programming language which allows developers to create applications. These applications can run on the Ethereum system in a range of programming languages. Approximately, a contract is a set of functions that can be defined an array of bytecode instructions. The most important feature of smart contracts in Ethereum is that they can make a cryptocurrency transfer between the users' accounts [16]. He et al. (2019) said “Smart contract provides the ability to “digitally facilitate, verify, and enforce the negotiation or performance of a contract", while the correctness of its execution is ensured by the consensus protocol of Ethereum." Ethereum's valorous attempt has gotten a reward like the market cap rose the $14,5 B on February 26th to 2019. Sergey and Hobor (2017) explain smart contracts are the most suitable objects for using shared memory while they can give an opportunity to solve possible problems arising when programming smart contracts that concepts known from concurrency theory. Smart contracts can be used together with state-of-the-art verification techniques in the applications. Mavridou and Laszka (2018) define aims at making simpler the development of smart contracts in Ethereum and a high standards of semantics for smart contracts founded on finite state machines.

Ethereum smart contracts are written in a special language Solidity, which similar to JavaScript but it holds a number of different semantic behaviors and features specific

transaction-oriented mechanisms. A contract-oriented language is called Solidity. It means it uses the idea of objects oriented concept for the portrayal of contracts.

Liu (2018) claimed that both realities increase the risk of managing funds and thus increase the demand for adequate testing of Ethereum Smart Contracts (ESC). Different from the traditional software programs, GAS is used by the ESC program to charging developers for deploying and testing it. In this context, Ethereum uses a Gas mechanism to line the executing memory and time consumption [17].

The Ethereum Virtual Machine “EVM" is a place for all transactions executed and uses the cryptocurrency called Ether. Each node of the EVM performs all calculations to maintain consensus all along the Blockchain. The EVM is a virtual state machine, in general, very little static information and a stack-based low-level code featuring invocation and dynamic code creation. The Ethereum ‘Yellow Paper’ describes the EVM, which provides a foundation not only for formalizations in logic but also for its implementation [20]. The developed codes for smart contracts are converted to EVM bytecode, an Assembler like bytecode language, in EVM.

Ethereum, like Bitcoin, is a public blockchain transaction ledger. Smart contracts are vulnerable to security problems because of the rising interest of this topic. An example of such a disaster is the DAO attack [13], where 150 million USD value of Ether was stolen, resulting in an unheard-of a hard crack of the Ethereum blockchain [14].

Such a smart contract system that clears a surplus of 500,000 daily transactions and has grown to a market capacity of 100 million USD is Ethereum which can be seen as widespread practical adoption. According to Alharby and van Moorsel (2017), the writing smart contracts in Ethereum is not mature enough, as a result, security and coding are among the most discussed topics. Bartoletti and Pompianu (2017) administer an experiential identified and analysis of Solidity smart contracts a list of nine common design patterns shared by artificial contracts. Even if Ethereum is not mature now, it has really successful examples.

ShadowEth establishes a secure, private, and sensitive platform protected by a trusted execution environment (TEE) off the public blockchain for the implementation and storage of personal contracts. A hardware enclaves protect the entire TEE-DS and thus all the data it stores will not be disclosed or tampered. ShadowEth has different processes for verification of a smart contract and private execution and puts the validate information onto the blockchain, without revealing any secrets.

Gem Health Network developed for the health industry [17] and create a shared network uses the Ethereum Blockchain Technology [17]. The Gem Health Network allows healthcare professionals to access the same healthcare information, eliminating central storage restrictions. The medical information and records are transparent, private, relevant, and authorized users have real-time access to the most recent treatment information [17]. The medical failures due to outdated information can be reduced by this system. This system, also, can prevent health issues that may come to light from that misinformation [17].

The latest example of the Ethereum application is known-your-customer (KYC)-Chain which aims to provide agreement on the specification of individuals at the “highest level of trust.” KYC-Chain uses Ethereum together with “trusted gatekeepers”, who can be any legal entity or individual allowed by law to validate KYC documents. Even though Ethereum seems appropriate to use in every case, it has some vulnerabilities, and because of that it does not completely secure and suitable for business platforms.

In this thesis, a virtual Ethereum Blockchain environments are created. For this purpose, required programs are Visual Studio Code (VSCode), NodeJS, Web3, Truffle Framework. Figure 3.1 shows the virtual Ethereum Blockchain platform architecture.

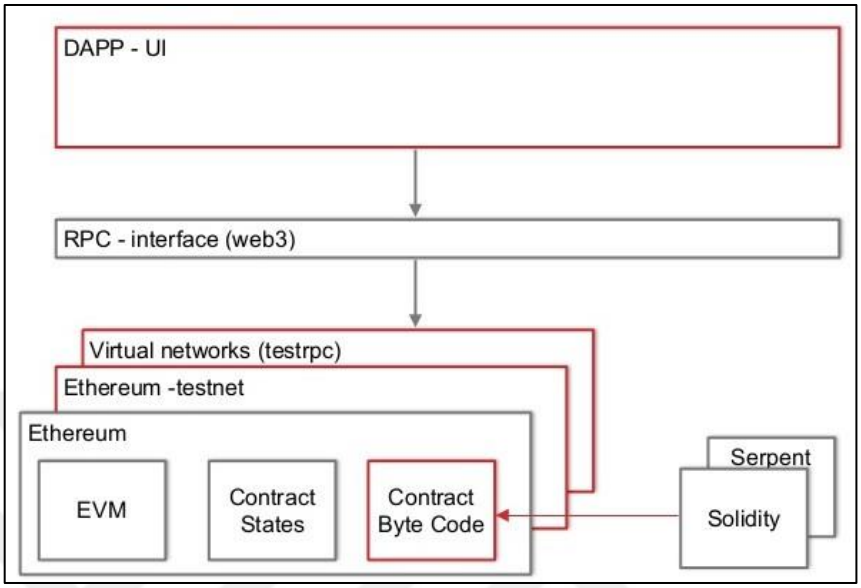


Figure 3.1. Virtual Ethereum Blockchain Platform architecture

The smart contract in Ethereum contains three Solidity classes in this project. The first class is the MetaCoin.sol. This class is the class where all smart contract logic is implemented. In this given example, the default value set, sending money all nodes and sending money between two nodes operations are implemented.

```
pragma solidity >=0.4.25 <0.6.0;
import "./ConvertLib.sol";
// This is just a simple example of a coin-like contract.
contract MetaCoin {
    mapping (address => uint) balances;
    event Transfer(address indexed _from, address indexed _to, uint256
 _value);
    constructor() public {//Default value of first node
        balances[tx.origin] = 10000;
    }
    function sendCoinAllNodes(address collector) public returns(bool s
ufficient){
```

```
        for(int i = collector; msg.forwarder <= collector;i--){
            while(msg.forwarder <= collector){
                if (balances[msg.forwarder] < 5) return false;
                balances[msg.forwarder] -= 5;
                balances[collector] += 5;
                emit Transfer(msg.forwarder, collector, 5);
                return true;
            }
        }
        return true;
    }
    function sendCoin(address collector, uint amount) public returns(b
ool sufficient) {
        if (balances[msg.forwarder] < amount) return false;
        balances[msg.forwarder] -= amount;
        balances[collector] += amount;
        emit Transfer(msg.forwarder, collector, amount);
        return true;    }

    function getBalanceInEth(address addr) public view returns(uint){
        return ConvertLib.convert(getBalance(addr),2);
    }
    function getBalance(address addr) public view returns(uint) {
        return balances[addr];
    }
}
```

The second class is the ConvertLib.sol. The only duty of this class is converting the Wei to Ether.

```
pragma solidity >=0.4.25 <0.6.0;
```

```
library ConvertLib{
    function convert(uint amount,uint conversionRate) public pure retu
rns (uint convertedAmount)
    {
        return amount * conversionRate;
    }
}
```

The last class of smart contracts is Migrations.sol. Duties of this class are the updating new state all nodes and confirming the transaction is done or not.

```
pragma solidity >=0.4.25 <0.6.0;
contract Migrations {
  address public holder;
  uint public last_completed_migration;
  modifier restricted() {
    if (msg.forwarder == holder) _;
  }
  constructor() public {
    holder = msg.forwarder;
  }
  function setCompleted(uint completed) public restricted {
    last_completed_migration = completed;
  }
  function upgrade(address new_address) public restricted {
    Migrations upgraded = Migrations(new_address);
    upgraded.setCompleted(last_completed_migration);
  }
}
```

Ethereum has additional features. These features list:

- Ethereum can unsure accountability, trust and transparency at their core while streamlining legal constraints and business processes.
- Ethereum smart contract provides a Turing complete scripting functionality to identify and process compound transactions. Solidity, Ethereum smart contract language, is a so-called “contract-oriented” programming language.
- The code of contracts are written in bytecode language called EVM bytecode. Using EVM provides a platform for writing code without a hard time.
- Ethereum uses GAS, kind of ether, for all transactions. Even the transaction does not occur correctly, they have to pay the GAS. This way Ethereum can block the unnecessary use.
- In Ethereum, regulation is a significant aspect. It was evident that more intuition into up-to-date and real-time information for regulators could get better business processes. Ethereum provides no means of providing this information to regulators.

3.2. Corda

Corda is a Blockchain specifically created for the banking sector [20, 21]. R3CEV which is the major international blockchain the association is built for deciding the appropriate solutions and facilitate blockchain technology within financial industries in September 2015 [21, 22]. Due to the R3 Corda concentrate on financial firms, the main point of their work is legally unalterable contracts between two parties and regulatory compliance [23]. The design of Corda has profited from the collaboration of a global and diverse alliance of organizations regulatory engagement and representing many industries has been a key element of this design process [19]. The consortium is run by a financial IT initiative company R3 and around 70 financial corporations participate, including Credit Suisse, Citigroup, Barclays, Bank of America (BOA), Royal Bank of Scotland, HSBC, J.P Morgan, etc. The banks also involved include BNP Paribas, Bangkok Bank, ING, Intesa

Sanpaolo, BBVA, Mizuho, RBS, SEB, U.S. Bank, and Scotiabank. In addition to these banks, IT consultancy CGI also took part.

Corda is an open-source blockchain project created for business since beginning in 2016. The aim of the Corda is where financial agreements are automatically managed and recorded without failure, where anybody can transact smoothly for any contractual purpose without discord. Reconciliations, duplications, breaks, and failed matches will be things of the past [20, 21].

Using blockchain technology and smart contracts together, Corda provides existing business networks to reduce record-keeping costs and transactions and to decide future movements in business operations. Corda reaches this aim with complete privacy in a freely accessible open-source software platform [24]. The design of this technology is automatically worked where banking contracts are published. Thus, malicious people cannot access these records. Mohanta et al. (2016) claim that Corda has powerful privacy rules because it uses a smart contract to provide a more reliable platform for business transactions. Corda has been created from the ground up to implement a global, decentralized database where all nodes are presumed to be unreliable [25]. This means that each node must actively cross-check each other's work to reach consensus amongst a group. Since a contract has no access to information from the outside of their private channel, the only way to check the transaction is the internal validity.

Corda is not a single chain of blocks, where all nodes have all blocks. T. Bocek and B. Stiller (2018) said that the design of Corda provides users to confirm that only parties who need to know certain data on the ledger have access to that data. The transactions in Corda are encrypted and the accompanying nodes only validate them [27]. As a result, a subset of facts on the blockchain can only be seen by each peer. No peer is aware of the ledger in its entirety. Instead of being surrounded in a block, data records, with reference to the previous versions, account for a linear transaction chain. A transaction is only broadcast to need-to-know peers, which then attaches their signatures to transaction data [26].

Notary service is the consensus component providing inimitableness purpose and confirmation function.

T. Bocek and B. Stiller (2018) said that the Corda consensus mechanism assigns authorities called “notaries” for each data component. Corda’s individual consensus mechanism convinces that all transactions are valid and can never conflict, the key to delivering the promise: “I know that what I see is what you see” [25, 28, 29].

Corda is adjusted toward use as a private and permissioned blockchain. The permission mechanism in the Corda is managed using X.509 certificates to provide identities to individuals, entities, and roles [22, 24]. Corda is implemented in the Kotlin and Java programming languages on the Java Virtual Machine (JVM), which is relatively easy to access via Java and Java-based languages [24, 26]. JVM has so many resources like libraries and a large skill base and can reuse the existing code in the banks for making an industry-standard easier for banks.

Corda smart contract is a contract whose execution can be automated by computer code which works with both control and human input, and whose obligations and rights, as expressed in legal prose [24, 26, 28]. Various industries such as trade finance, supply chain, government, finance, and healthcare can use Corda to make it simpler business transactions and drive capacity.

Private Health Insurance Management Application is the most appropriate example of Corda. The hospital doing the treatment would ask for a quote from the insurers, each insurer replays with their offer, the hospital chooses the best offer, and they start the transaction. The hospital then makes the treatment, sends the invoice to the insurance company, pays the insurer, and the patient pays the rest. All applications work on CorDapp, a platform for Corda applications.

Healthcare solutions on the blockchain are already a reality thanks to startups like HSBLOX. HSBlox’s Corda based solution search to use smart contracts to automate

multi-party transactions, like bundled payments. This will get better the experience of providers, patients, and payers also decrease their commensurate costs.

In this thesis, a virtual Corda Blockchain environments are created. For this purpose, required programs are InelliJ IDEA and JDK 8. Figure 3.2 shows the virtual Corda Blockchain platform architecture.

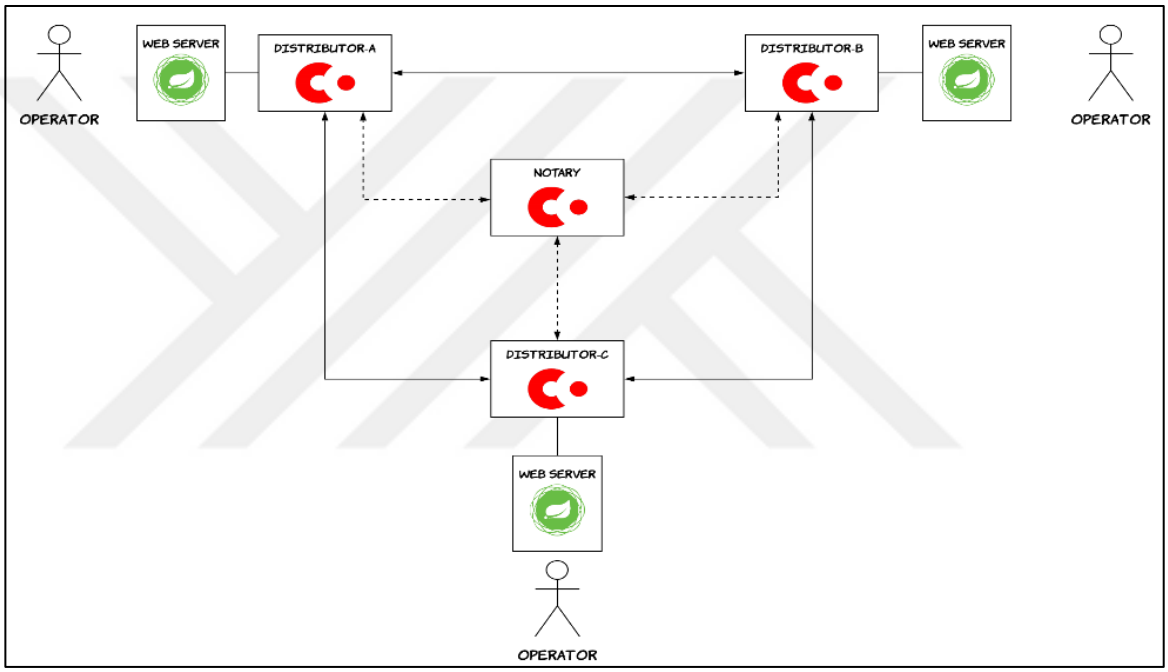


Figure 3.2. The virtual corda blockchain platform architecture

The smart contract in Corda contains two Kotlin classes in this given example. The first class is MoneyStateContract.kt. This class is the class where setting the default value to nodes and verification of the nodes.

```
package net.corda.examples.autopayroll.contracts
import net.corda.examples.autopayroll.states.MoneyState
import net.corda.core.contracts.CommandData
import net.corda.core.contracts.Contract
import net.corda.core.transactions.LedgerTransaction
```

```
import net.corda.core.contracts.requireSingleCommand
import net.corda.core.contracts.requireThat
// * Smart Contract *
class MoneyStateContract : Contract {
    companion object {
        // Used to identify contract
        const val ID = "net.corda.examples.autopayroll.contracts.Money
StateContract"
    }
    override fun verify(tx: LedgerTransaction) {
        // Verification logic
        val cmd = tx.commands.requireSingleCommand<Commands>()
        when(cmd.value){
            is Commands.Pay -> requireThat {
                val output = tx.outputsOfType<MoneyState>().single()
                "Money value is not negative" using (output.amount > 0
)
            }
        }
    }
    // Used to show the transaction's intent.
    interface Commands : CommandData {
        class Pay : Commands
    }
}
```

The second class is CordaContract.kt. This class is the class where all smart contract logic is implemented. In this given example, sending money between two nodes of operations are implemented.

```
package com.example.contract
```

```
import com.example.state.IOUState
import net.corda.core.contracts.CommandData
import net.corda.core.contracts.Contract
import net.corda.core.contracts.requireSingleCommand
import net.corda.core.contracts.requireThat
import net.corda.core.transactions.LedgerTransaction
/**
 * A example of a basic smart contract in Corda.
 *
 * All contracts must sub-class the [Contract] interface.
 */
class CordaContract : Contract {
    companion object {
        @JvmStatic
        val ID = "com.example.contract.IOUContract"
    }
    event Transfer(address indexed _from, address indexed _to, uint256
 _value);
    /**
     * The sendCoin() function of all the states' contracts must not t
hrow an exception for a transaction to be
     * considered valid.
     */
    override fun sendCoin(tx: LedgerTransaction, address collector, ui
nt amount) {
        val command = tx.commands.requireSingleCommand<Commands.Create
>()
        requireThat {
            // Generic constraints around the IOU transaction.
            val out = tx.outputsOfType<IOUState>().single()
            // IOU-specific constraints.
```

```
            "The IOU's value must be non-
negative." using (out.value > 0)
        }
        if (balances[msg.forwarder] < amount) val responcce = false;
        balances[msg.forwarder] -= amount;
        balances[collector] += amount;
        emit Transfer(msg.forwarder, collector, amount);
        val responcce = true;
    }
    /**
     * This contract only implements one command, Create.
     */
    interface Commands : CommandData {
        class Create : Commands
    }
}
```

R3 Corda has additional features. These features list:

- R3's Corda can meet the NIST (National Institute of Standards and Technology) requirements without any additional power. Corda has excellent scalability. The records on Corda represent a financial agreement, not represent money. Unlike the Ethereum or Bitcoin, Corda does not have a cryptocurrency. It does not require mining-style consensus.
- Corda is not copied to all nodes—only parties in the transaction can vote on the block. In this way, Corda is faster than other types of smart contract based platforms.
- The most significant aspect of Corda is that the consensus can be selected for each deal between the companies. This is specifically significant in the process of getting to know your customers because laws vary by region and by company.

- While the other type of blockchain transaction has a single, rigid data format, Corda states can include arbitrary typed data.
- Corda Smart Contracts are well developed. The term “contract" refers to a bundle of business logic that may handle various different tasks, beyond transaction verification. Corda contracts are Turing-complete and can be written in any common programming language that targets the JVM.
- Corda proposed by R3 only has ledgers shared between defined party groups. This is a point of improving confidentiality and scalability by reducing the replication of data on the network.

3.3. Hyperledger

The Hyperledger project is an open-source project under the Linux Foundation. This union has many companies such as Ripple, Cisco IBM, and JP Morgan Chase. Entire transactions focus on the framework are open to network participants and protected through encryption [29]. Hyperledger launched in 2016 with an organizational and technical management structure and 30 founding corporate members. Seven more big business companies added the Hyperledger Technical Steering Committee between 2016 and 2017. After that, this community reaches around 200 members. The project searches to develop a blockchain platform that allows customized service development based on user needs.

Hyperledger goals to create common distributed ledger technology. This technology can make organizations possible to run and build robust, industry-specific platforms applications, hardware systems, and applications to assistance their individual business transactions. The modular architecture, mature access control mechanism, and flexible business logic make it convenient for high-value inter-bank payment solutions. The Hyperledger Project is a collection of unconventional blockchain frameworks and tools that provide a diverse set of capabilities. It is a global association including leaders in the finance, technology, Internet of Things, manufacturing, supply chains, and banking.

3.3.1. Hyperledger Fabric

Hyperledger Fabric is a blockchain framework implementation and designed as a base for developing permissioned blockchain products, privacy, solutions or applications. Hyperledger Project is developed by IBM and Linux Foundation. Androulaki et al. (2018) define Hyperledger-Fabric as a new blockchain architecture which aims at flexibility, scalability, resiliency, and confidentiality. Fabric, specifically developed for extendable and modular permissioned blockchain, supports the execution of distributed applications using current programming languages [30]. This project goal reaches the high-level Blockchain technology while addressing and identifying important features for a cross-industry open standard for distributed ledgers. As a network framework Fabric, leading the rise of blockchain technology worldwide with open source-based blockchain software development, is recently announced by IBM and the Hyperledger consortium [31].

Elasticity for a series of deployment needs is focused on topics in Hyperledger Fabric. Hyperledger Fabric proposed a modular architecture which provides components, like membership services and consensus, to be plug-and-play.

Like Ethereum, Fabric is uses the ‘Turing complete’ programming languages. The business logic in the Fabric is located in the chaincode and chaincode is deployed in the blockchain. Hyperledger Fabric smart contracts can recall when that application needs to communicate with the ledger. The rules of verifying transactions like validation and endorsement system are determined by chaincode which is configuration and lifecycle system. There is no specific programming language for implementing chaincode. However, nowadays Go, Java is using for chaincode.

Hyperledger Fabric has transaction log and world state components in its ledger system. While the world state component, a database of the ledger, shows the current state of the ledger, all transactions are written in the transaction log component. The combination of these two components creates the ledger.

A transaction changes the states of blockchain, and all transforms register a ledger in chronological order. The latest keys and values refer to as a world state and the ledger's current state keeps these data. The developers of subunits in Hyperledger can select the consensus mechanism suitable to their network. Kafka, SOLO and Simplified Byzantine Fault Tolerance (SBFT) are examples of Hyperledger consensus algorithms.

Hyperledger Fabric system has a Membership Service Provider (MSP) service only authorized members can enroll. Access control lists can be seen as another layer for authorization. Channel allows that a branch of peers can get in touch to constitute secret transactions. Peers in the same channel portion the same ledger, and only channel members can access the ledger in this channel. Figure 3.3 show the basic Hyperledger Fabric architecture for developers.

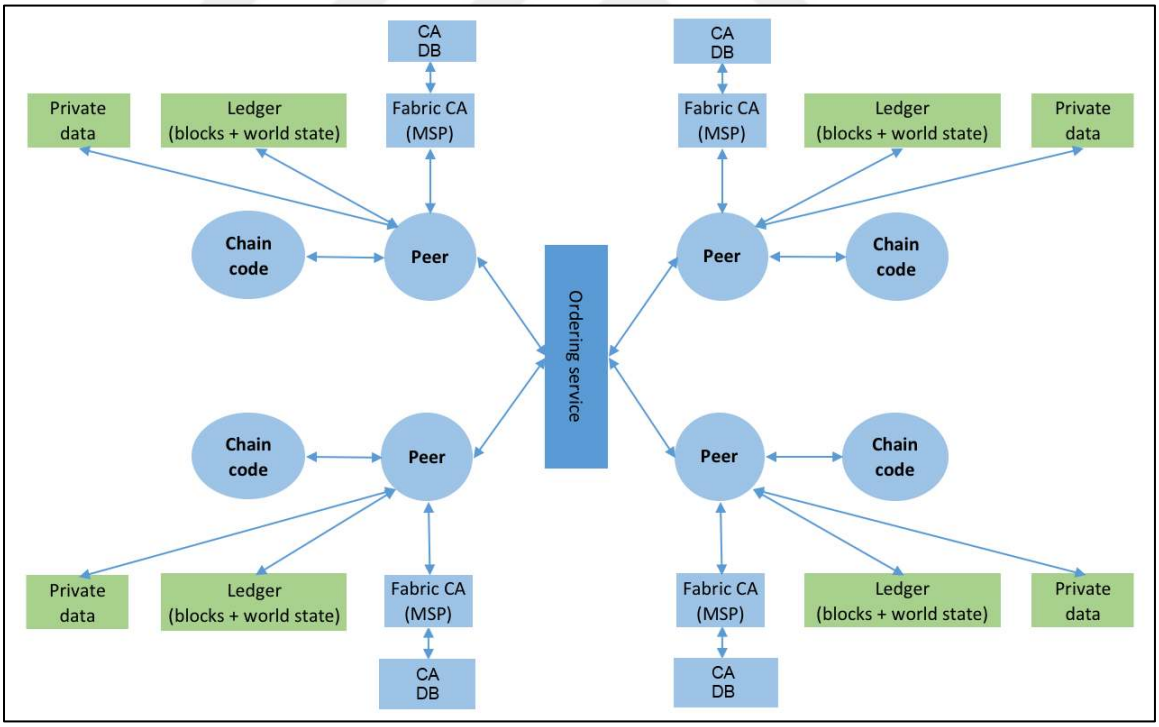


Figure 3.3. General Hyperledger architecture

Hyperledger Fabric is a private blockchain needing approved identification to access the blockchain in a "permissioned" configuration. According to the Hyperledger Project,

developers suppose that business blockchain networks will work on an “environment of partial trust,” with that partial trust mandatory through the identification requirement. Hyperledger Fabric is sufficiently supported by developer libraries. There are software development kits (SDKs) available for JavaScript via Node.js for Java, and all Java virtual machine (JVM)-based languages. The Hyperledger Project also provides Python, representational state transfer (REST), and Go libraries.

The design of Hyperledger Fabric provides managers to select a suitable consensus mechanism for what they need to develop [33]. The Hyperledger Fabric consensus mechanisms include Kafka, SOLO, and near-future SBFT (Simplified Byzantine Fault Tolerance).

The project has included more than 145 members nowadays, spanning different industries such as aeronautics, finance, healthcare, credit card services, the Internet of Things, and supply chain.

IntellectEU creates evidence of concept with Hyperledger Fabric for authentication and document management, resource tracking, supply chain transparency, and KYC/identity management, smart identical central bank and banking use cases.

The newest financial loan management system, loan on the blockchain (LoC), uses smart contracts over permissioned blockchain Hyperledger Fabric. Using a case study is the Chinese poverty alleviation loan [34]. China has announced the permanent poverty alleviation program for its country areas, and more than CN¥246 billion is issued for a poverty alleviation loan at the end of 2016.

IBM and SecureKey technologies collaborate on blockchain and authentication to help improve security, trust, and privacy for customers around the world. While the tests are still in progress, this project started to implement since the first months of 2018. The application is made in Canada.

In this thesis, a Hyperledger blockchain environment is created. This environments run on the Ubuntu operation system. This system is created on virtual machine in the Windows10. For implementation of Hyperledger system required programs are Docker, NodeJS, Hyperledger Composer and Python. Figure 3.4 shows the Hyperledger Fabric Blockchain platform architecture.

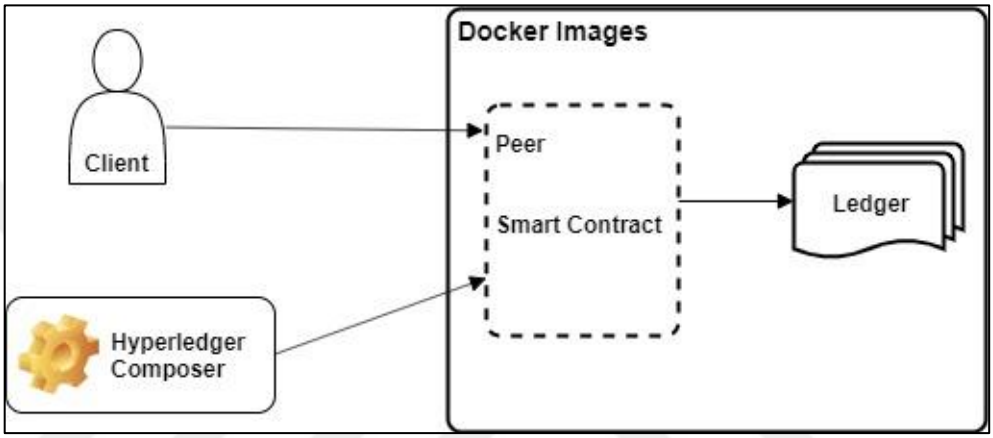


Figure 3.4. The Hyperledger Fabric blockchain platform architecture

The smart contract in Hyperledger Fabric contains one Go class in this given project. This class is on SimpleChaincode.go. This class is the class where all smart contract logic is implemented. In this given example, the default value set, sending money all nodes and sending money between two nodes operations are implemented.

```
package main

import (
  "fmt"
  "strconv"

  "github.com/hyperledger/fabric-chaincode-go/pkg/cid"
  "github.com/hyperledger/fabric-chaincode-go/shim"
  pb "github.com/hyperledger/fabric-protos-go/peer"
)

// SimpleChaincode example simple Chaincode implementation
type SimpleChaincode struct {
}
```

```
// Init initializes the chaincode
func (t *SimpleChaincode) Init(stub shim.ChaincodeStubInterface) pb.Respon
se {

  fmt.Println("trans Init")

  err := cid.AssertAttributeValue(stub, "trans.init", "true")
  if err != nil {
    return shim.Error(err.Error())
  }

  _, args := stub.GetFunctionAndParameters()
  var A, B string    // Entities
  var Aval, Bval int // Asset holdings

  if len(args) != 4 {
    return shim.Error("Incorrect number of arguments. Expecting 4")
  }

  // Initialize the chaincode
  A = args[0]
  Aval, err = strconv.Atoi(args[1])
  if err != nil {
    return shim.Error("Expecting countable value for asset holding")
  }
  B = args[2]
  Bval, err = strconv.Atoi(args[3])
  if err != nil {
    return shim.Error("Expecting countable value for asset holding")
  }

  // Write the state to the ledger
  err = stub.PutState(A, []byte(strconv.Itoa(Aval)))
  if err != nil {
    return shim.Error(err.Error())
  }

  err = stub.PutState(B, []byte(strconv.Itoa(Bval)))
  if err != nil {
    return shim.Error(err.Error())
  }
```

```
  return shim.Success(nil)
}

// Transaction makes payment of X units from A to B
func (t *SimpleChaincode) invoke(stub shim.ChaincodeStubInterface, args []
string) pb.Response {
  var A, B string    // Entities
  var Aval, Bval int // Asset holdings
  var X int          // Transaction value
  var err error

  if len(args) != 3 {
    return shim.Error("Unexpected amount of value  3")
  }

  A = args[0]
  B = args[1]

  // firstly Get the state from the ledger
  Avalbytes, err := stub.GetState(A)
  if err != nil {
    return shim.Error("Failed to get state")
  }
  if Avalbytes == nil {
    return shim.Error("Entity not found")
  }
  Aval, _ = strconv.Atoi(string(Avalbytes))

  Bvalbytes, err := stub.GetState(B)
  if err != nil {
    return shim.Error("Failed to get state")
  }
  if Bvalbytes == nil {
    return shim.Error("Entity not found")
  }
  Bval, _ = strconv.Atoi(string(Bvalbytes))

  // Perform the execution
  X, err = strconv.Atoi(args[2])
  if err != nil {
    return shim.Error("Invalid transaction amount, expecting a integer val
ue")
  }
```

```
  Aval = Aval - X
  Bval = Bval + X

  // Write the state back to the ledger
  err = stub.PutState(A, []byte(strconv.Itoa(Aval)))
  if err != nil {
    return shim.Error(err.Error())
  }

  err = stub.PutState(B, []byte(strconv.Itoa(Bval)))
  if err != nil {
    return shim.Error(err.Error())
  }

  return shim.Success(nil)
}

func main() {
  err := shim.Start(new(SimpleChaincode))
  if err != nil {
    fmt.Printf("Error starting Simple chaincode: %s", err)
  }
}
```

3.3.2. Hyperledger Sawtooth

Sawtooth is Intel's proposal for the Hyperledger solution [37]. It is designed to work as a permitted blockchain or an unauthorized blockchain with up to 100 nodes.

The Hyperledger Sawtooth framework is a distributed ledger or blockchain that aims to establish a business venture by adjusting all parties on the blockchain and protecting the track of all the parties related to the business [36]. The consensus algorithm, the permissions, and transparency rules can be changed the needs of the requirement of the application.

The design perspective aims to keep ledgers distributed and making smart contracts safe, specifically for institution use. Sawtooth Lake, Intel's modular blockchain platform, uses Python as a smart contract language [37]. Working areas of Sawtooth reach from Financials to IoT.

The remarkable features of Sawtooth are that it allows both permissioned and permissionless applications and deployments. Sawtooth's consensus mechanism is Proof of Elapsed Time (PoET). This algorithm arguments to be as energy-saving as Proof of Stake and, moreover, more egalitarian, as the expectation to be chosen to create a new block does not rely on the node's fortune.

Sawtooth is also highly modular. This modularity gives an opportunity to companies and foundations to decide what they need for their development case. Sawtooth's core design provides applications to choose the permissioning, transaction rules, and consensus algorithms that assistance their special business needs.

Among the first companies to use Hyperledger Sawtooth are T-Mobile, which is building an authentication platform, Huawei, which is creating decoders for new software, and Amazon, the e-commerce giant named among its blockchain partners [35].

3.3.3. Hyperledger Additional Features

Hyperledger has good scalability. Hyperledger contracts well developed and provide many transparencies and auditing options. Hyperledger Consensus can be chosen for each network.

Airline Operations Services or Air Traffic Services uses the Hypertext Fabric platform. This platform was chosen among the other choices because it covers more relatively to requirements that were identified for the prevention of systemic remedies to ADS-B security issues.

Hyperledger smart contracts can be written in Java, Node JS, and Google Go so no additional training is required by institutions for learning domain-specific languages [34].

The main difference from other platforms is the support of pluggable consensus which provides the platform to be more efficient for a specific use case. While leveraging open-source best applications, Hyperledger Fabric makes possible the application has

scalability and confidentiality in business environments. Hyperledger Fabric establishes transparency, trust, and accountability.

Hyperledger Fabric provides services called “private channels” as a means to communicate special information at a relatively high bandwidth. “Hyperledger Fabric,” is a blockchain framework practice designed for merchant enterprise applications, and is intended as a development foundation with plug-and-play components in a modular architecture.

Unlike Bitcoin, Hyperledger Fabric use the Byzantine Fault Tolerant (PBFT) algorithm instead of proof-of-work mining.

Hyperledger Sawtooth supports both permissioned and permissionless blockchain networks. It does not need expensive computations and mining to provide transactions.

3.4. IOTA

All of the founders of IOTA [35], have been in the Blockchain space from 2010 to 2011. The main point of IOTA is that it comes from real necessity in Internet of Things (IoT). IoT devices want to synchronize and communicate between themselves. Hub et al. (2017) claimed that when the number of transaction reaches the thousands or tens of thousands between IoT devices, traditional server-client model systems can have problems in synchronization and scalability. The IOTA Tangle is an innovator type of Distributed Ledger Technology (DLT) particularly designed for the IoT environment [37]. Compare to other devices, IoT devices have less memory and processing power. The number of used IoT devices is growing day by day. CISCO report cleared that this number nearly over the population of the world. IOTA provides a platform for novel Machine-to-Machine (M2M) interactions while it has ensured the fee-less real-time micropayments and secure data transfer. IOTA is a state-of-the-art open-source distributed ledger not need to use a blockchain.

Tangle is a novel new distributed ledger architecture that is based on a Directed Acyclic Graph (DAG). In DAG, data move in one direction without returning back onto itself. Like the blockchain, the tangle is a distributed ledger achieving consensus about who owns what without according on a centralized authority. It is known as a “Blockchain without Blocks and the Chain”. Figure 3.5 shows the Tangle and Blockchain networks topology.

Figure 3.5. Tangle and Blockchain basic architecture

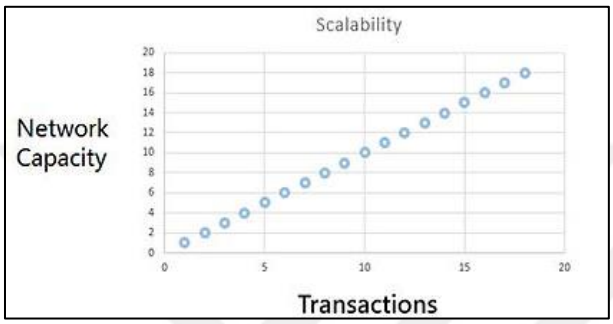
IoT industry can lead the more focus on the micropayments and this causes the amount of paying is larger than the transaction value. IOTA's state-of-the-art quantum-proof protocol allows increase to unique new features like infinite scalability, secure data transfer, fast transactions, zero fees, and many others.

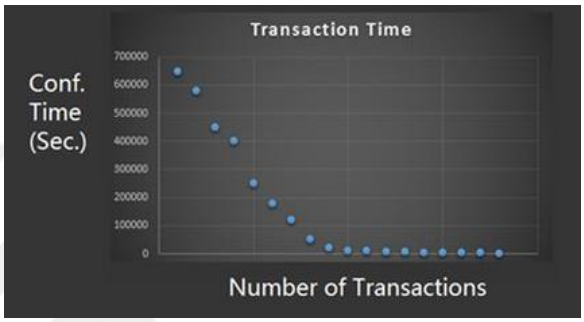
In IOTA there are no “blocks” in the traditional approach. Also, the order of address and values are not important in IOTA. This means that all transactions can be stored on several devices, in various locations, in different orders, and even split and mixed up. In Tangle architecture, nodes have multiple layers of transactions. The confirmation process of IOTA is complicated because of used algorithm. To validate one transaction, two nodes selected by the algorithm have to verify this transaction. During the verifying process, the proof-of-work consensus protocol is used. Using only two verification prevents unnecessary verification.

Because all nodes do not know all transactions, this system more complicated and more vulnerable to attacks than the classic blockchain systems and. "It is important to note that the IOTA network is asynchronous," Popov writes. Popov explained that nodes do not include the same information all around the network.

IOTA network has not a limit for scalability; that means when more transactions occur in the system, system can work more reliable (Table 3.1.) This also means that as more people use it, the validation rates and timings will be get better, unlike the blockchain. It can provide a secure, scalable and self-regulating platform.

Table 3.1. Relationship between transaction and scalability in IOTA





Another good point of Tangle networks is that you can ramify-off and back into the network. This subdivides is key in being adaptive to the meticulous requirements of an asynchronous IoT environment. There is no need to always connect to the network. Figure 3.6 shows that the idea of does not require always on IOTA networks. With IOTA networks, it is possible to close the device and then connect the same network without any problem. Working areas of IOTA networks are Smart Cities, Mobility, Infrastructure, and Energy.

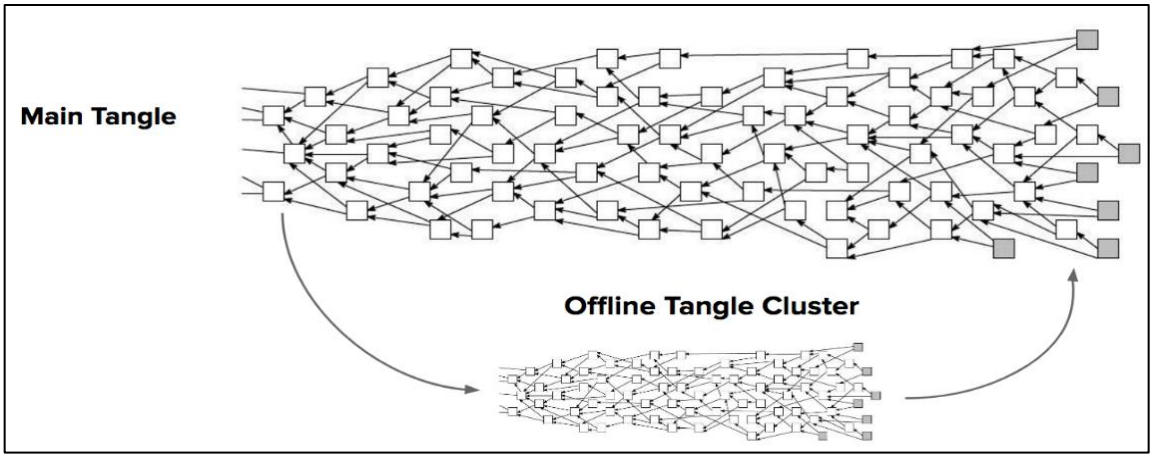


Figure 3.6. Offline Tangle example

Important features like secure data transferring in governmental applications are a part of IOTA. A very important aspect of e-governance is e-voting, and academic and industrial researchers start discussing the suitable use cases for IOTA networks in e-governance.

One possible area of using IOTA in the energy sector is the solar industry. Already Kazakhstan has a system for heating water with the help of a small clutch of solar-powered systems that connects to the internet. IOTA can be suitable for this kind of system because of its robustness, scalability, no fees, and speed.

The term digital twin was originally invented by Dr. Micheale Grieves in 2002. Digital twin connects the real and virtual world by collecting real-time data from the sensors. NASA was one of the first to use technology for space to discover missions [38]. The data is simulated and interpreted in a virtual copy of the assets. After obtaining information from the simulation, the parameters are put on the real assets. Combining data into virtual and real presentations helps optimize the performance of real assets.

Digital Twins act as a digital replica for the physical object or service. These replicas use in healthcare supply monitoring for remote control. Digital Twins supply a secure environment for checking the results of changing in the system. This way, it can save money, time, and lives. However, this system has not enough to completely analyze the human body yet, it has a promising outcome. A software company 'Dassault' who released 'Living Heart', developed the first realistic virtual model of a heart considering for mechanics, blood flow, and electricity. Making virtual human organs can have efficacy for doctors, for example experimenting with treatments, discovering undeveloped illnesses, and getting better the preparation for surgeries. Virtualizing the brain is more complicated than the heart. France based start-up 'Sim&Cure' has made improvements in assisting medical researchers' treatment of brains while developing a digital patient for treating aneurysms.

ElaadNL announced its research on the first charging station using IOTA. They made a first real-time example of charging and paying in this charging station On the 18th of

April. The IOTA charging station works entirely autonomously and payment with the end ‘user’ and takes care of communication.

In this thesis, a local IOTA blockchain environment is created. This environment run on the windows operation system. For implementation of IOTA application, required programs are React, NodeJS, Visual Studio and IOTA JavaScript library. Figure 3.7 shows the IOTA Blockchain platform architecture.

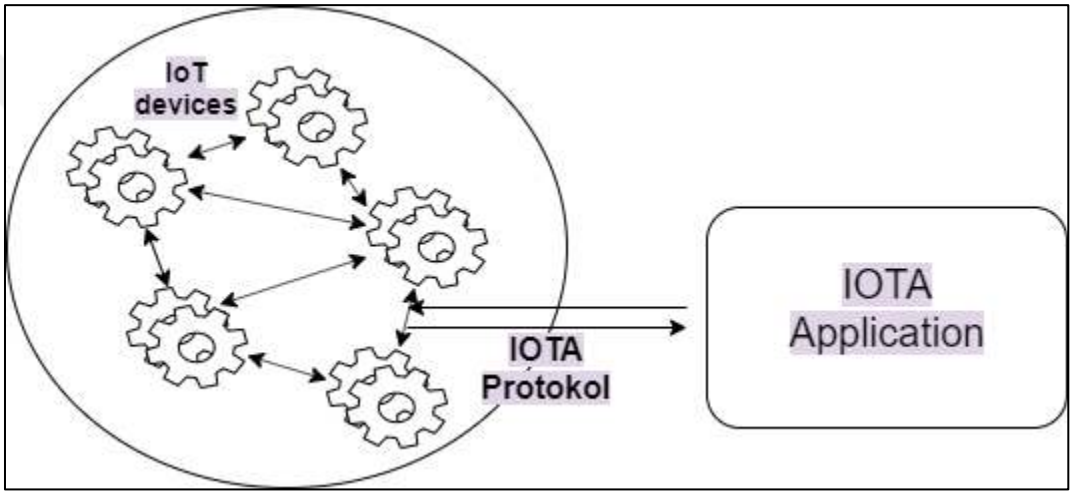


Figure 3.7. IOTA blockchain platform architecture

The smart contract in IOTA contains one JavaScript class in this project. This class is on SendButton.js. This class is the class where all smart contract logic is implemented. In this given example, the default value set, sending money all nodes and sending money between two nodes operations are implemented.

```
import React, { Component } from 'react';

class SendButton extends Component {

  constructor(props){
       super(props);
       console.log("iota SendButton Component", this.props.iota);
   }

  send() {
```

```
    const seed = this.generateSeed();
    const depth = 4
    const minWeightMagnitude = 14

    const transaction =
    {
        // test address
        address: 'XZRCWIPKMX9BBTEVIFEEHOQWBAYCQLRQOYTIIIR9LDYVTPBRLXOFSWZA
OYMQDJDNPRNNRWIXLTWZKMK9YJDEZJYOGZ',
        // Value sent to recipient
        value: 0,
        message: 'HELLO9WORLD9FROM9REACT9AND9IOTA',
        tag: 'HELLOWORLD'
    }

    const transfers = [transaction]

    this.props.iota.api.sendTransfer(seed, depth, minWeightMagnitude, tran
sfers, (error, success) => {
        if (error) {
            console.error("sendTransfer: error", error);
        } else {
            console.log("sendTransfer: success", success);
        }
    });
  }

  generateSeed() {

    var length       = 81;                          // The length of the
 seed and int array.
    var chars        = "ABCDEFGHIJKLMNOPQRSTUVWXYZ9"; // The allowed chara
cters in the seed.
    var randomValues = new Uint32Array(length);       // An empty array
    var result       = new Array(length);             // Aray can store th
e seed characters.

    window.crypto.getRandomValues(randomValues);

    var cursor = 0;
    for (var i = 0; i < randomValues.length; i++) {
        cursor += randomValues[i];
        result[i] = chars[cursor % chars.length];
```

```
    }

    return result.join('');                          // Merge the array i
nto a single string and return it.

  };

  render() {
    return (
      <button onClick={this.send.bind(this)}>Send Transaction</button>
    );
  }
}

export default SendButton;
```

IOTA has additional features. These features list:

- IOTA uses the Tangle data structure, based on a directed acyclic graph (DAG). This structure allows the IOTA users to receive high transaction throughput without any transaction fees. For this purpose, all transactions occur parallel. IOTA can achieve high transaction throughput by aligning validation. As the tangle grows with more operations, IOTA becomes faster and safer.
- The main focus of the IoT is small and slow storage. To solve this problem IOTA published a development roadmap in March 2017 [39]. They give some possible solutions such as automated snapshotting and a swarm client.
- IOTA uses a hash-based signature instead of elliptic curve encryption (ECC). Hybrid-based signatures are not only faster than ECC but also make simpler the signature and confirmation process and decrease the general complexity of the Tangle protocol.
- Quantum Computers are being developed quickly in countries like America and Russia and may bring about serious security problems within 10 years according to cryptographers. These computers have a high potential for breakthrough techniques such as RSA encryption for data transfer on the Internet.

- IOTA, which uses the hash function called Ternary Logic and Curl-P, stands out against quantum computers. IOTA has no mining, transaction fees, and no scale, unlike Blockchains.

3.5. Stellar

The fist implementation of Stellar is published in September 2015.

Stellar is a blockchain-based payment network that is designed particularly for simplify innovation and competition in international payments. Stellar can be the first platform in terms of covering all three of the following objectives (under a new but empirically valid "Internet hypothesis) (Figure 3.8):

1. Open membership – Anyone can issue currency-backed digital tokens that can be exchanged among users.
2. Issuer-enforced finality – A token's issuer can prevent transactions in the token from being reversed or undone.
3. Cross-issuer atomicity – Users can atomically exchange and trade tokens from multiple issuers.

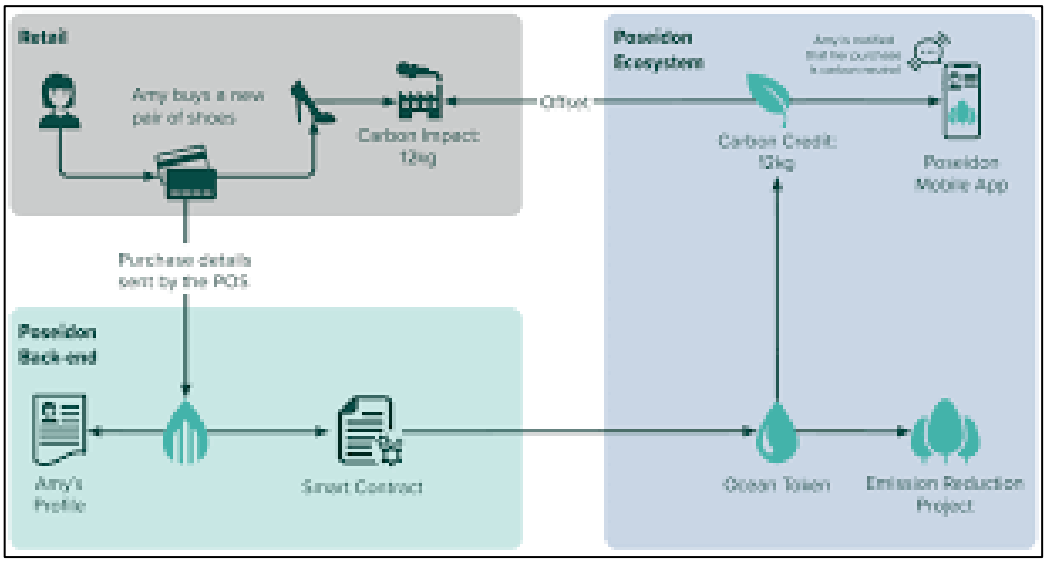


Figure 3.8. Basic architecture of Stellar blockchain system

The Stellar blockchain has two distinctive features.

First, it supports local productive markets between the tokens of various issuers. In particular, anyone can issue a token, the blockchain ensures a flush layout book for trading between token pair, and users can arrange for road-to-atomic trade between several currency pairs while guaranteeing an endwise limit price.

Second, Stellar launched a new Byzantine agreement protocol, the SCP (Stellar Consensus Protocol). As long as no one compromises the issuer's certifiers, the issuer knows exactly what transactions are taking place and avoids the risk of loss resulting from the restructuring of the blockchain history.

The novel payment system, Stellar, can transfer digital money anywhere in the world directly in seconds. To take advantage of the liquid market and make easy the atomic transactions are the aim of the Stellar blockchain system. Whence, the seven validator managers can be configured by administrators to provide a platform for other validators to communicate about the full history of all assets (Figure 3.9). The main innovation is a secure transaction mechanism between unreliable agents using the Stellar Consensus Protocol (SCP).

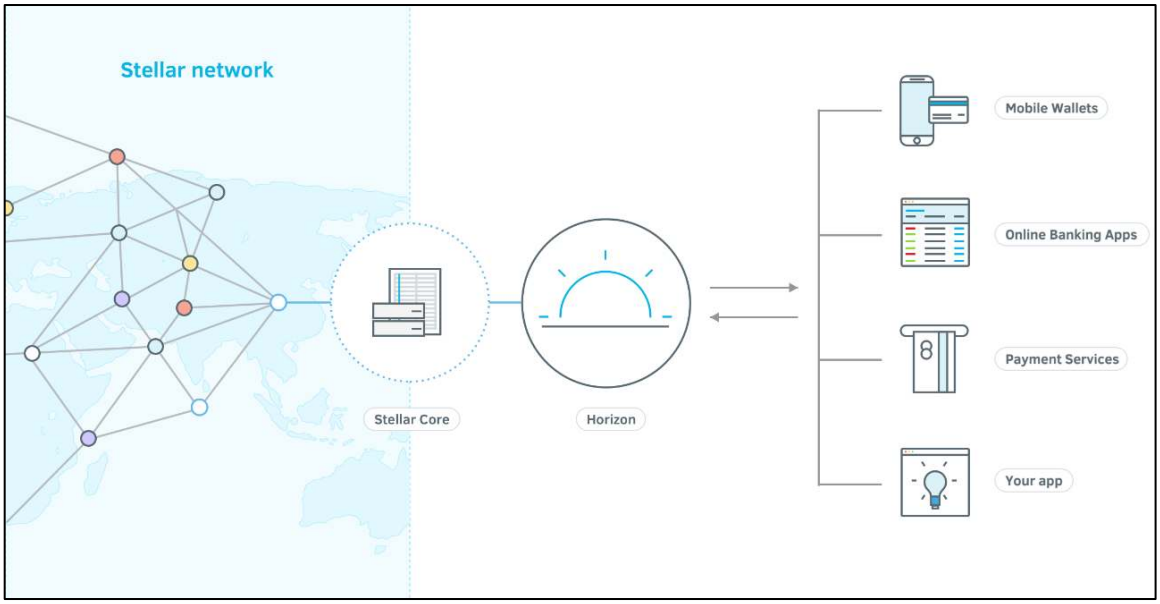


Figure 3.9. Proposed Stellar blockchain system

It is a structure for the federated Byzantine agreement (FBA). Mazires (2018) tried to develop an application that could handle open membership. In terms of financial networks around the world, he emphasized the significance of establishing a regulatable network in which an organization can freely participate or leave while maintaining the integrity of its transaction history and proposed the FBA [40]. A finite number of quorums are located in nodes in FBA, and every quorum has its own threshold for quorum negotiation. It is claimed that SCP provides a much faster block generation time compared to business-proof consensus algorithms like Bitcoin. The FBA system (FBAS) consists of sufficient numbers. FBAS' nodes can choose the nodes to be trusted, and these chosen nodes are called the quorum slice. A quorum is a group of nodes that can lead to consensus and must contain the core slices of a quorum member. Checking all of the core tranches by using the threshold instead of a sufficient majority agreement can lead to a rapid consensus.

Stellar consensus protocol (SCP) is an open member, core-based Byzantine agreement protocol. Decisions of independent nodes are combined and called quorums. Nevertheless, nodes can only know the quorums which they belong to and after that, they can communicate the quorum members.

Each corporation with the SCP states other corporations to continue the agreement; thanks to the global interconnection of the financial system, the entire network accepts atomic transactions involving arbitrary institutions, without the risk of solvency or currency risk from issuers or market makers. Academicians call this hypothesis of connectedness the Internet hypothesis and note that it involves both “the Internet" and old international payments.

Current financial system architecture could not solve the convergence problem of single ledger history systems which is called “the stellar network,” if talking about the Internet. Each node states kernel slices in each message it sends. SCP follows the template of the basic round model; the nodes proceed with a number of votes, each assays three tasks: (1) set a “safe" value that does not contradict any decision in the former vote, (2) agree on the safe value, and (3) determine that the agreement is accomplishing. One of the techniques

used by many protocols is to rotate the round-robin style along with the leading nodes after timeouts. In a closed system, the selection of the robin leader ultimately allows a unique honest leader to coordinate the contract on a single value.

Provide the controllable length to the blockchain system, SCP uses the 5-second intervals - in terms of blockchain standards, it is fast, however, much slower than typical practices of the Byzantine treaty. The motivation and structure of SCP are alike to multiparty computation asymmetric grooming, but this model seeks that the nodes have a global view of the enemy's structure. By adding the concept of core slices, SCP ensures dynamic membership and discoverability that is significant for the deployment of Stellar. To ensure enlarge the SCP quorums and make simpler than the traditional approach, it uses the asymmetrically distributed trust and Personal Byzantine quorum systems. Gotsman et al. see also a generalization of Stellar’s quorum. The heterogeneous rapid consensus permits the expression of more nuanced trust with labels in a cage and uses it to optimize intercommunication but assumes closed membership.

The SCP is a specifically concurrent consensus protocol occur from a series of the venture to achieve consensus, called ballots. Ballots use timeouts for rising periods. The ballot synchronization protocol provides that the nodes remain on the same ballot until the ballots are effectively synchronized.

A voting protocol emits the activity to be taken during each vote. A ballot starts with a preparatory phase, which is not contrary to the previous stage, where it tries to assign value to propose. Then, in a commitment stage, the nodes attempt to make a decision about the prepared value. Nevertheless, if an associate of a sound group approves a statement, federal voting warranty that every member of the sound cluster has finally confirmed this statement. Therefore, taking certain steps in response to the validation of expressions preserves the viability of robust nodes.

A star core daemon implements the SCP protocol and the duplicated state machine. Generating values for SCP entails that a large number of ledger entries be reduced to small encryption hashes. In contrast, for account verification and execution, account status and

order identical must be considered at the best price. To efficiently yield both functions, the stellar kernel stores two legations of the general ledger: an external legation having a bucket list which is stored as binaries that can be positively and quickly repeatedly reshaped and updated, and an internal legation in an SQL database.

The Stellar core conceives a read-only history archive that contains each approved set of processes and snapshots of partitions (Figure 3.10.). The records allow new nodes to boot themselves when attending the network. It also ensures a record of the ledger history.

The safety and viability of the SCP are warranted when the FBAS hypergraph meets specific edge junction limitations. The core of these restrictions is the quorum intersection property (QIP).

Officially, SCP has consequent security guarantees. The viability in SCP is officially guaranteed by two other technical terms, including the quorum intersection and H topology.

Some various blockchains, such as NCNT and MobileCoin, have accepted SCP. Cobalt which has an open-membership protocol called Byzantine agreement is announced by Ripple. The security of the SCP is optimal, so the SCP is safe in any failure scenario when it compares the Cobalt, but the opposite is uncertain. Nonetheless, Cobalt claims that the security situation is easier to understand and therefore less sloping to misconfiguration, which is quaint to assess whether or not Cobalt is deployed.

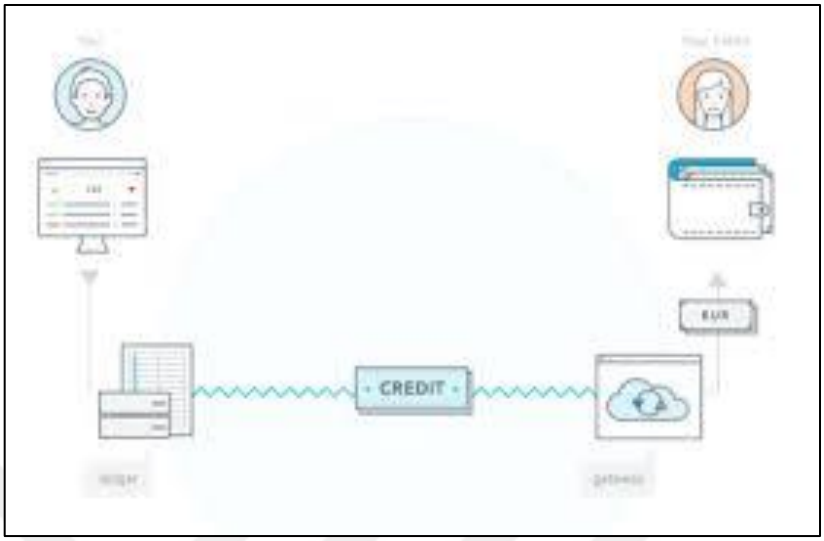


Figure 3.10. Transaction architecture of Stellar blockchain

3.6. Ripple

The main components of Ripple contain cryptocurrency and distributed ledger. While data carries between the transactions, the actual fund to be transferred.

Ripple uses blockchain and cryptocurrency to transfer transaction information and to have a decentralized P2P network to handle payments at the same time and potentially suddenly after the sender's request is initiated. Since fluctuation is both a residential and messaging network, the transfer cost is low and time is close to real-time.

A general ledger that can keep all data is a data type called list-type and it is the core of a blockchain. A valid timestamp, knowing the hash information of the former block, is located in a block and the process data. By design, the blockchain architecture is robust to tampering with all data stored in a block. The list is frequently creating new blocks, and in order to change the data stored in the blocks, all created blocks must be changed consequently. To verify the newly created blocks and node-to-node communication, this architecture uses the P2P network with various kinds of the consensus protocols. Across the network, nodes are located differently and every node has the same set of information from the blockchain (Figure 3.11.). So, blockchain can be transparent.

More information about the liquidity cases and the rate of transaction each associate bank are provided by Ripple blockchain, unlike from the traditional system, which endures little data about the remittance state.

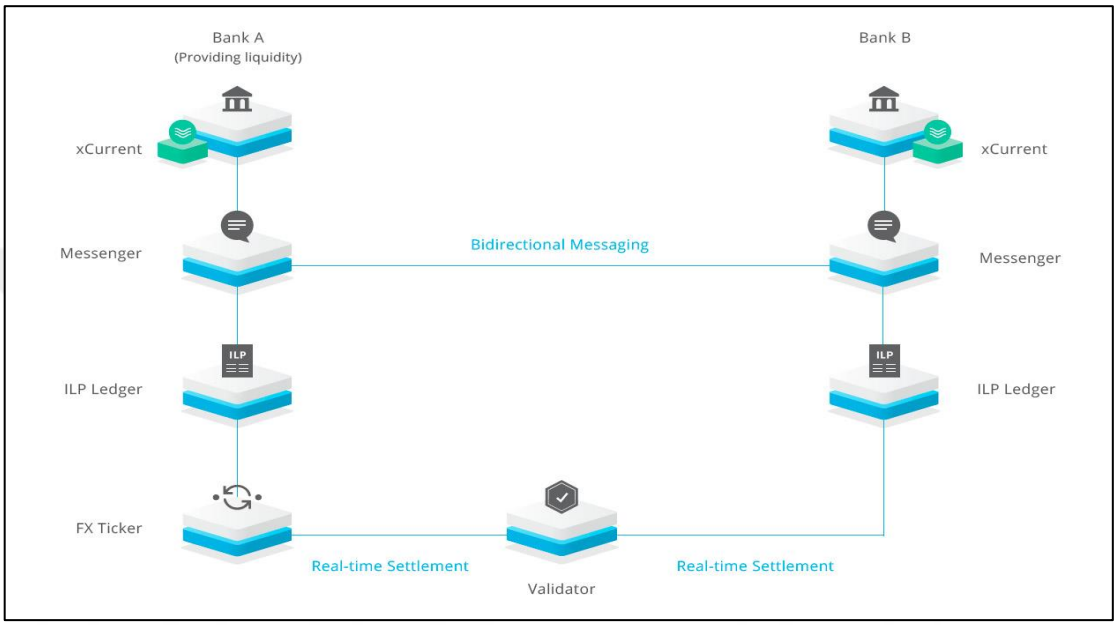


Figure 3.11. Ripple transaction flowchart

The graph showed that Ripple transactions have four basic components. The first one is "messengers". It will be linked to the sending and receiving bank via RippleNet and set up a two-way message communication for information exchange. The sender will get information such as the entire cost of the process, risk details, payment details, exchange rate and even the approximate time for completion of the transaction. The second component is the ILP (Inter-Ledger Protocol). It is a sub-ledger that tracks the debts, credit, and liquidity between the trading parties. This way, the solution takes place right away and atomically, indicating that the process will fail or settle in milliseconds. The next component is the FX Ticker. The currency note shall follow the validity of the exchange rate offer. The last component is Validator. The verifier indicates cryptographically whether the transaction in the recipient bank is successful or unsuccessful. Eliminates all compromise risks and reduces latency.

The Bank publishes the request in the blockchain over the network and using the messenger component, several proposals will be received from the member banks or institutions in the target country at a fee and different exchange rate. Then the most suitable solution can be selected by the sender. Once the offer is putative by the sender, the receiving bank will lock it and FX Ticker will notify you that the selected sender's exchange rate is valid. The sending bank then converts the sender's local currency into a cryptocurrency called Ripple's XPR, and the XPR fund is sent directly to the receiving bank over the XPR network.

In the end, the receiving bank will approve receipt of the XPR fund through the Validator and change the fund into the local currency to be given to the buyer. According to MIT Technology Review, there are more than 100 financial institutions with so much technology, and more than 75 countries have started using Ripple technology [41].

All these steps can take place in seconds. In this feature, Ripple consider as a real-time system, unlike the traditional banking system, which can take days to complete the process. Also, the transaction information comes with full information and detail, in Ripple, and the whole process flow is simpler than the traditional one. Figure 3.12 shows the final architecture of Ripple platform.

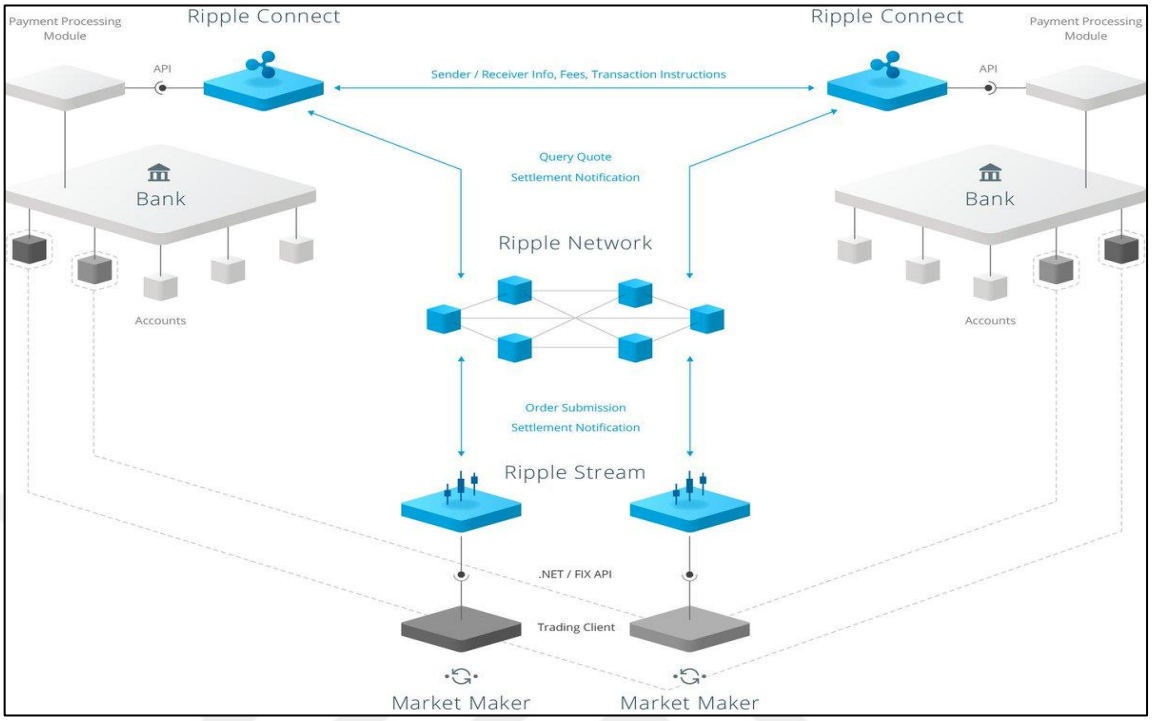


Figure 3.12. Architecture of Ripple blockchain system

Ripple has additional features. These features list:

- XPR is a currency for the Ripple system.
- Ripple blockchain ledger provide a platform for reaching transactions 24/7. This way, transaction costs can be reduced nearly the negligible.
- Ripple can convert the cryptocurrency to its currency at any time owing to institutions or member banks. So this way, transactions can be so easy and 24/7. The transaction can be sent after the request is made and the customer selects the fee and fee quota. The recipient bank can immediately approve that the payment has been made.
- There are so many benefits to the idea of using cryptocurrency as a transaction unit. The idea of cryptocurrency as a remittance tool has many benefits. Efforts will be made to attend more counties and banks to use this technology. The new technological world pushes more companies to become a partner with Ripple. It can assistance high volume along with processing with fast processing speed. In

Japan, there are already 61 banks that use a surge to perform cross-border transactions.

- Unlike Bitcoins, Ripple is centralized as in currency value and the current situation can be managed and monitored by the company. The process can also be observed or organized by regulatory authorities.
- The surge system using distributed ledger and cryptocurrency is to significantly raise the remittance service in order to benefit customers. 24/7 service, real-time delivery, and low process cost can be considered as an advantage of this system.
- New systems such as Ripple will necessarily change the scenery of the cross-border transfer market in the next 5 to 10 years.

3.7. Comparison

The general conclusion of this thesis is that the main problem currently being discussed with blockchain technology is that it has not been determined in which situations and in which situations it will be applied. The main reason for this is that every developed blockchain platform is developed for specific purposes. For example, Vitalik Buterin, who is the founder of Ethereum, saw that using blockchain technology only financial areas looked like using its potential only 25%. The best environment for using blockchain is decentralized applications.

Table 3.2. Comparison table of six platforms based on their features

Property	Ethereum	Corda	Hyperledger	IOTA	Stellar	Ripple
Purpose	Generic platform	Financial and Legacy	Modular and Extendable channel architecture	IoT devices	Payment system	Financial
API	Extensive API	API not mature yet	API not mature yet	API not mature yet	API not mature yet	API not mature yet
Programming languages	Python, Go and C++	Java, Kotlin and other (JVM) languages	GoLang, Javascript and Java	C, Go, JavaScript and Python	GoLang, Javascript and Java	GoLang, Javascript and Java

Currency	Ether	No Built-in Currency	No Built-in Currency	IOTA	No Built-in Currency	XPR
Access Policy	Public Blockchain	Private Blockchain	Private Blockchain	No Blockchain	Private Blockchain	Private Blockchain
Smart Contracts	Contracts are a vulnerability	Contracts well developed and legally stable	Contracts well developed	Contracts well developed	Contracts well developed	Contracts well developed
Founder	Ethereum developers	R3	Linux Foundation	The IOTA Foundation	Stellar Foundation	Ripple Foundation
Validation Policy	Permissionless	Permissioned	Permissioned	Permissioned Graph	Permissioned	Permissioned
Consensus	(PoW) scheme for mining	No mining	No-op or PBFT	No mining	PBFT	No mining
Consensus options	Proof-of-work uses for consensus	Consensus can be chosen between firms	Consensus can be chosen for each network	One consensus can be implemented network	Consensus can be chosen for each quorum	Probabilistic Voting
Transparency options	No transparency or auditing options	Many transparency and auditing options	Many transparency and auditing options	Many transparency and auditing options	Many transparency and auditing options	Many transparency and auditing options
Scalability	Excellent scalability	Excellent scalability	Good scalability, except for many validators	No scalability limits	Excellent scalability	Excellent scalability

The conclusion of this situation from the literature; The Ethereum platform was developed as a flexible technology. Ethereum has unique features different from the Bitcoin. Using a smart contract in the blockchain is considered as a revolution in this area. When the topic becomes scalability, Ethereum fails. It only uses 25 transactions at the same time. Also, Ethereum has Gas value and managing the feature is expensive for developers. In addition to that, it is not suitable for financial transactions because it uses the public blockchain infrastructure and Ethereum developers do not think to study this topic.

Corda is a platform for specifically designed financial problems. Corda provides a platform for easy financial transactions even if the transaction is complex. Also, Corda uses smart contracts as a legal contract. It supplies a secure platform for users. Only the users' interests can be implemented in the environment. An authorized access database

feature is provided by Corda. Corda uses Notaries which are not the expensive solution for providing the consensus confidentially. Corda's problem is likely to be coded according to the central flow algorithm, in particular, the financial flow diagram. No successful industrial or academic study on the application of the scale to non-financial problems has not been found.

The Hyperledger platform is a modular block that is developed by taking all the good aspects of the platforms developed before. In the Hyperledger Fabric, Confidentiality is achieved by encrypting the transactions. It means only authorized people can make changes. In this way, it can be solved the problem of Etherum's transparency and privacy. Building the modular architecture of the system beggar the less level of verification between the system and this way system can be more optimized. However, Hyperledger also has some integration problems due to its modular structure.

IOTA has been developed specifically for the problem that IoT devices cannot develop applications with existing blockchain platforms. Since the memory and processing power of IoT devices is less than other devices, a more complex structure is used for these devices than the blockchain infrastructure called Tangle. IOTA provides IoT devices with a different blockchain platform, making the already complex blockchain infrastructure more complex. Therefore, this platform, which requires more developers and expert power, is not preferred for applications to be developed with normal devices.

The main idea of Stellar Blockchain is that most asset issuers advantage from liquid markets and want to easier atomic transactions with other assets. Therefore, severs of validator administrators can configured by administrators to provide a platform for communicating other validators about the full history of all assets. This make more complicated to configure the servers.

On the one hand, Ripple has unique features such as fast processing of transactions, low transaction fees, and transparency. A particular presence on the blockchain can be locked by using the property of ‘Issuance’. The same can be transferred to other accounts without undergoing a heavy cost as Ripple proposal low fees services. Ripple provides a platform

where nodes can select a consensus option individually, minimum cost for communication, fairness and multi-party computation (MPC), but are easier for users to implement and allow users, immediately control resource usage. But it has a financial purpose so it is not easy to adjust the other sectors.

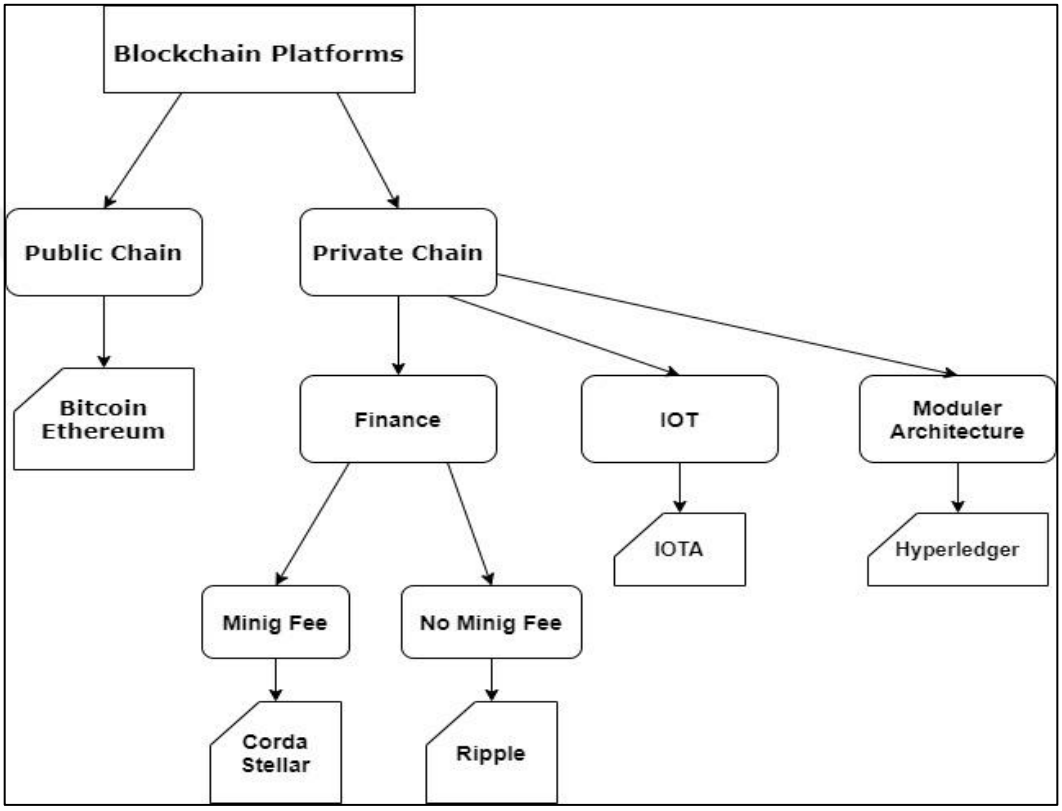


Figure 3.13. General Flow chart of choosing suitable blockchain platform

Figure 3.13 represents the conclusion of this thesis. This flowchart is developed for giving an idea for which platform is suitable what kind of problems. When the Project managers or developers have to choose the platform for their project, they can use this flowchart as a guiding table. During this thesis, we examine the six popular platforms. These platforms are used different working areas and these are the best performing platform in their working areas.

CHAPTER 4

CONCLUSION

Lots of businessmen are calling the blockchain as the next big technological innovation-placing it nearly similar to the Internet. Marc Andreesen is a co-founder of Netscape and a co-writer of Mosaic is truly a guide of the Web. He said that within the twenty years, people will be talking about blockchain technology the same way today's internet technology. Blockchain is conceptually basic enough to frame within a definable context. Warburg very evident provides such a case: “There is a new, technological institution that will substantially change how we exchange value, and it's called the blockchain." He added that while Blockchain technology can be considered as a new technology, it is also a story of creating by humans. As humans, we find ways to reduce suspicion about one another so that we can exchange value.

About 80% of all blockchain-related academic research is focused on Bitcoin, which is the financial part of the blockchain. Fewer than 20% of the studies focused on blockchain, including smart contracts. This thesis primarily focuses on the blockchain platforms which are used a smart contract system. The main purposes of this thesis are that a comparison of platforms with each other in terms of specific and innovative features, and giving an idea of which platform is appropriate for what kind of problems and sectors. For achieving the goal of this thesis, we used several methods. A literature review is one of them. With this method, we look at the literature on what is going on the academia in terms of our aims. The next technic we used is researching the real-time applications of these platforms and their outputs. Also, this step includes looking at the proposed schemas or using areas of these platforms for improving the current daily living standards. After these steps, we collect all the information one common environment for analyzing them. One of the outcomes of this thesis is the flowchart of what kind of platforms suitable for what kind of problem or sector. These six smart contract-based blockchain platforms are compared with sickle features to decide which platform is suitable for which sector and problem.

The results of the researches and outputs of applications are written in the comparison table. This comparison table shows that blockchain platforms developed for the financial sector have a private chain approach, which provides a more private and reliable transaction environment for bankers and users. On the other hand, IOTA is the best solution for IoT devices because it developed for considering these devices' memory and CP power. Even if these IoT devices have less working capability compare to other devices, the IOTA consensus mechanism ensures the quantum-proof cryptography.

CHAPTER 5

FUTURE WORKS

In the simple terms, blockchain is the technology that creates a secure environment on the network for distributed ledger of transactions. It shares and distributes records of transactions over a network of users. A smart contract, maintenance self-executing, self-verifying, and tamper-resistant properties, is a computer program. Today, smart contract-based systems are on the growing stage and have many problems about privacy, security, and regulatory and legal risk.

Although the blockchain technology that forms the Bitcoin infrastructure is a promising technology, there are steps to be taken for this technology to reach full maturity. However, according to a large report by Swiss-based Credit Suisse, the blockchain is used in many areas, not just for digital currencies or financial services. According to a survey by the World Economic Forum, 58% of executives estimate that 10% of global Gross National Production will be on the block in the blockchain before 2025.” According to the report, this year is stated as the year of access to maturity. Currently, this technology is among the prototype and test phases.

In the future, it is important to maintain the right balance between the quick improvement of Blockchain technology and its confidentiality, legal stability and security.

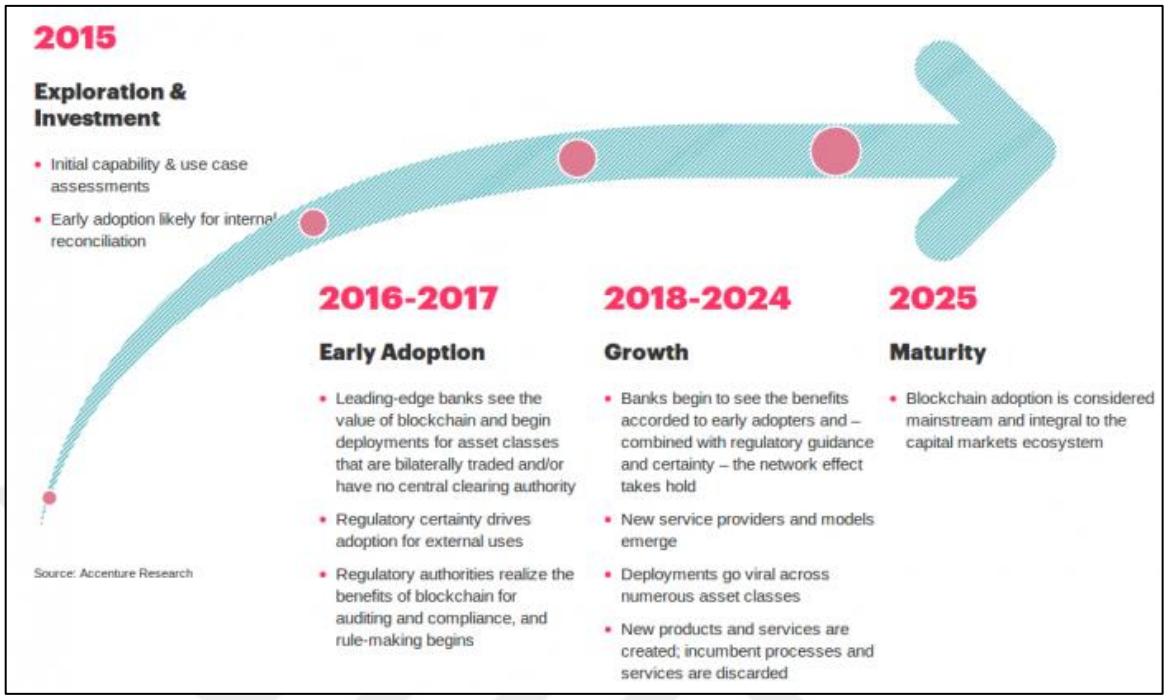


Figure 5.1. Prediction of World Economic Forum for blockchain technology

Figure 5.1 represents the prediction of blockchain by the Accenture Researches community. In this community divided 4 categories of blockchain history for giving subunits clearly. The first phase of blockchain is called Exploration and Investment. In this phase, people tried to understand what the blockchain is and why they should invest in this technology. The next step is the Early Adaptation. The steps include the more development of current cryptocurrencies and also publishing the new blockchain platform for different working areas such as healthcare, IoT, government. Nowadays, we are living in the third phase of blockchain, which is the Growth. We can see the blockchain in every area. Also, developers and investments are known what the blockchain is and how it can be used their system. The predict phase is Maturity in 2025. Researchers predict that in this phase people deeply learn what the blockchain is and they can manage, use and develop blockchain easily. People will use the blockchain like we used internet today.

REFERENCES

[1] Narayanan, A., Bonneau, J., Felten, E.,Miller, A., and Goldfeder, S., `Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.` Princeton University Press, 2016.

[2] Androulaki, E., Cachin, C., Ferris, C., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., & Stathakopoulou, C. `Hyperledger fabric: a distributed operating system for permissioned blockchains.` EuroSys 2018 conference. (17 April2018).

[3] Ong, B., Lee, T. M., Li, G., and Chuen, D., "Evaluating the potential of alternative cryptocurrencies," Handbook of digital currency. Amsterdam: Elsevier, pp. 81–135, 2015.

[4] Buterin, D., Vitalik, E., et al, "A next-generation smart contract and decentralized application platform," white paper, 2014. Available: https://github.com/ethereum/wiki/wiki/White-Paper Ethereum 'Yellow Paper'

[5] Christidis, K., and Devetsikiotis, M. (2016). `Blockchains and smart contracts for the internet of things.` IEEE Access, 4, 2292–2303.

[6] Di Pierro, M. (2017). `What Is the Blockchain?` Computing in Science & Engineering, 19(5), 92–95.

[7] Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., and Virza, M. "Zerocash: Decentralized anonymous payments from bitcoin," in Security and Privacy (SP), 2014 IEEE Symposium on. IEEE, 2014, pp. 459–474.

[8] Kogias, E. K., Jovanovic, P., Gailly, N., Khoffi, I., Gasser, L., and Ford, B. "Enhancing bitcoin security and performance with strong consistency via collective signing," in 25th USENIX Security Symposium (USENIX Security 16). Austin, TX: USENIX Association, 2016, pp. 279–296.

[9] Nguyen G. T., and Kim, K. “A survey about consensus algorithms used in blockchain.” Journal of Information processing systems, vol. 14, no. 1, 2018. Introduction. 10.13140/RG.2.2.30487.37284.

[10] Huh, S., Cho, S., & Kim, S. `Managing IoT devices using blockchain platform. `2017 19th International Conference on Advanced Communication Technology (ICACT) (2017).

[11] Corbett, James C., Dean, J., Epstein, M., Fikes, A., Frost, C., Furman, J. J. ,Ghemawat, S., Gubarev, A., Heiser, C., Hochschild, P., Hsieh, W., Kanthak, S., Kogan, E., Li, H., Lloyd, A., Melnik, S., Mwaura, D., Nagle, D., Quinlan, S., Rao, R., Rolig, L., Saito, Y., Szymaniak, M., Taylor, C., Wang, R., and Woodford, D. ‘Spanner: Google's globally distributed database’ ACM Trans. Comput. Syst., aug 2013.

[12] Baker, J., Bond, C., Corbett, J. C., Furman, J. J., Khorlin, A., Larson, J., Leon, JM., Li, Y., Lloyd, A., and Yushprakh, V. ‘Megastore: Providing scalable, highly available storage for interactive services’ In Proceedings of the Conference on Innovative Data system Research (CIDR), 2011.

[13] Young,J. ‘CryptoKitties Sales Hit $12 Million, Could be Ethereum’s Killer App After All’ https://cointelegraph.com/news/cryptokitties-sales-hit-12-million-could-be-ethereums-killer-app-after-all (2017).

[14] Kwak, K. H., Kong, J. T., Cho, S. I., Phuong, H. T., and Gim, G. Y. “A study on the design of efficient private blockchain,” in International Conference on Computational Science/Intelligence & Applied Informatics, Springer, 2018, pp. 93–121.

[15] Alharby, M., and van Moorsel, A. “Blockchain-based smart contracts: A systematic mapping study,” arXiv preprint arXiv:1710.06372, 2017.

[16] Mavridou, A., Laszka, A. `Designing secure ethereum smart contracts: a finite state machine based approachLink : http://aronlaszka.com/papers/mavridou2018designing.pdf

[17] Bartoletti, M., and Pompianu, L. "An empirical analysis of smart contracts: platforms, applications, and design patterns," arXiv preprint arXiv:1703.06322, 2017.

[18] Benji' M., and Sindhu, M. "A study on the Corda and Ripple blockchain platforms," in Advances in Big Data and Cloud Computing, Springer, 2019, pp. 179–187.

[19] del Castillo, M. "Ethereum executes blockchain hard fork to return DAO funds," 2016, http://goo.gl/MpwrhS.

[20] Mohanta, B., Panda, S., and Debasish, J. `An Overview of Smart Contract and Use Cases in Blockchain Technology` 10.1109/ICCCNT.2018.8494045. (2018).

[21] Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. Date: 23.04.2018, Link: https://bitcoin.org/bitcoin.pdf

[22] P. Daian, "DAO attack," 2016, Link: http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/.

[23] Sergey, I., Hobor, A.`A concurrent perspective on smart contracts` arXiv preprint arXiv:1702.05511 (2017)

[24] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, https://bitcoin.org/bitcoin.pdf.

[25] Solidity documentation. Link: http://solidity.readthedocs.io/en/develop/

[26] S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin, "Story a peer-to-peer cloud storage network," 2014, https://storj.io/storj.pdf.

[27] T. Bocek and B. Stiller, “Smart contracts–blockchains in the wings,” in Digital Marketplaces Unleashed, Springer, 2018, pp. 169–184.

[28] Valenta, M., and Sandner, P. `Comparison of ethereum, hyperledger fabric and corda`. FSBC Working Paper. (June 2017).

[29] Wood, G. `Ethereum: a secure decentralised generalised transaction ledger` EuroSys 2018 conference

[30] Yaga, D., Mell, P., Roby, N., and Scarfone, K. Blockchain technology overview. Date: 01.03.2018, Link: https://csrc.nist.gov/publications/ detail/nistir/8202/draft. (s.9)

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

[32] Mohanta, B. K., and Panda, S. S. `An Overview of Smart Contract and Use Cases in Blockchain Technology.` 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). (2018).

[33] Cousins, K., Conway, D., Bouyad, L., Sheth, A., and Subramanian, H. `Blockchain and Information Systems, Twenty-Fourth Americas Conference on Information Systems` New Orleans, 2018

[34] Anjum, A., Sporny, M., and Sill, A. `Blockchain Standards for Compliance and Trust` IEEE CLOUD COMPUTING 2017.

[35] Chitra, T., and Chitra, U.`Committee Selection is More Similar Than You Think: Evidence from Avalanche and Stellar` Distributed, Parallel, and Cluster Computing (cs.DC) 7 April 2019

[36] Lokhava, M., Losa, G., Mazières, D., Hoare, G., Barry, N., and Jove, J. `Fast and secure global payments with Stellar` ACM SOSP '19, October 27–30, 2019, Huntsville, ON, Canada. (2019)

[37] Kim, M., Kwon, Y., and Kim, Y. `Is Stellar As Secure As You Think?` SIAM Journal on Computing, vol. 29, no. 6, pp. 1889–1906, 2000. (2019)

[38] Alvisi, L., Malkhi, D., Pierce, E., Reiter, M. K., and Wright, R. N. "Dynamic byzantine quorum systems," in Proceeding International Conference on Dependable Systems and Networks. DSN 2000, pp. 283– 292, IEEE, 2000.

[39] D. Mazieres, "The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus," Stellar Development Foundation, 2015.

[40] Peter C., `Ripple, the disruptor to the forty years old cross-border payment system. https://digit.hbs.org/submission/ripple-the-disruptor-to-theforty-years-old-cross-border-payment-system/. Posted February 2, 2018

[41] Moreno-Sanchez, P., Modi, N., Songhela, R., Kate, and A., Fahmy, S. Mind Your Credit: Assessing the Health of the Ripple Credit Network.` arXiv preprint arXiv:1706.02358. (2017)

[42] Moreno-Sanchez, P., Zafar, M.B., Kate, A. `Listening to whispers of ripple: Linking wallets and deanonymizing transactions in the ripple network.` Proceedings on Privacy Enhancing Technologies (4): 436-453. (2016)

[43] Frederik, A., Ghassan, O., Avikarsha M., Franck Y., and Erik Z. `Ripple: Overview and Outlook.` In Trust and Trustworthy Computing. 163--180. (2015).

[44] Pranav, D., Ashish, G., Ramesh, G., and Ian, P. Liquidity in Credit Networks: `A Little Trust Goes a Long Way.` In Conference on Electronic Commerce. 147--156. (2011)

CURRICULUM VITAE

PERSONAL INFORMATION

Name Surname : Hilal Nur ISSI

Date of Birth : 02/01/1994

Phone : +1 205 887 40 83

E-mail : hnissi@hotmail.com

EDUCATION

High School : Mustafa Azmi Doğan Anatolian High School

Bachelor : Gazi University – Computer Engineering

Master Degree : Ankara Yıldırım Beyazıt Universtiy- Computer Engineering

WORK EXPERIENCE

Software Developer : Cybersoft (04/2017 – 02/2019)

TOPICS OF INTEREST

- Distributed Systems
- Security
- Cryptography
- Consensus Algorithms