Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Babylon
College of Information Technology
Software Department

NETWORK FUNCTION VIRTUALIZATION TO DEVELOP A BLOCKCHAIN IN CLOUD

A Dissertation
Submitted to the Council of The
College of Information Technology
University of Babylon in Partial Fulfillment of the
Requirements for the Degree of
Doctor of Philosophy
in Information Technology-Software

By

Hayder AbdulSattar Nahi Abdown

Supervised by

Asst. Prof. Dr. Alharith Abdulkareem Abdullah

2022A.D. **1443 A.H.**

بسم الله الرحمن الرحيم

رَبُّ الْمَشْرِقِ وَالْمَغْرِبِ لا إِلَهَ إِلاَّ هُوَ فَاتَّخِذْهُ وَكِيلا (9)

صدق الله العلي العظيم

سورة المزمل- اية 9

Declaration

I hereby declare that this dissertation, submitted to the University of Babylon as fulfillment of requirements for the degree of doctor of Philosophy in Information Technology\ Software has not been submitted as an exercise for a similar degree at any other university. I also certify that the work described here is entirely my own.

Signature:

Name: Hayder AbdulSattar Nahi Jawdhari

Date: \ \ 2022

Supervisor Certification

I certify that the dissertation entitled **(Network Function Virtualization to Develop a Blockchain in Cloud)** was prepared under my supervision at the department of Software/ College of Information Technology/ University of Babylon as partial fulfillment of the requirements of the degree of Doctor of Philosophy in Information Technology-Software.

Signature:
Supervisor Name: Asst. Prof. Dr. Alharith A. Abdullah
Date: / / 2022

Head of the Department Certification

In view of the available recommendations, I forward the dissertation entitled **"Network Function Virtualization to Develop a Blockchain in Cloud"** for debate by the examination committee.

Signature:
Asst. Prof. Dr. Ahmed Saleam
Head of Software Department
Date: / / 2022

Certification of the Examination Committee

We, the undersigned, certify that (Hayder AbdulSattar Nahi Jawdhari) candidate for the degree of Doctor of Philosophy in Information Technology-Software, has presented his dissertation of the following title (**Network Function Virtualization to Develop a Blockchain in Cloud**) as it appears on the title page and front cover of the dissertation that the said dissertation is acceptable in form and content and displays a satisfactory knowledge of the field of study as demonstrated by the candidate through an oral examination held on: (/ /2022).

Signature:
Name: Dr. Saad Talib
Title: Prof
Date: / / 2022
(**Chairman**)

Signature:
Name: Dr.Ziyad Tariq Mustafa
Title: Prof
Date: / / 2022
(**Member**)

Signature:
Name: Dr.Wesam S Bhaya
Title: **Prof**
Date: / / 2022
(**Member**)

Signature:
Name: Dr. Hameed A. Younis
Title: Prof
Date: / / 2022
(**Member**)

Signature:
Name: Dr. Mahdi Nsaif Jasim
Title: Asst. Prof
Date: / / 2022
(**Member**)

Signature:
Name: Dr. Alharith A. Abdullah
Title: Asst. Prof
Date: / / 2022
(**Member and Supervisor**)

Approved by the Dean of the College of Information Technology, University of Babylon.

Signature:
Name: Dr. Hussein Atiya Lafta
Title: Professor
Date: / / 2022
(Dean of Collage of Information Technology)

Dedication

For the sake of Allah, To my imam (Ali Ibn Abi Talib), my supporter,

To my angel in life, to the meaning of love and the meaning of compassion and dedication to the Smile life mystery of existence, all the world's words are not enough to describe thanks to your character lived his life for us, you gave me the right way, and I hope that you accept this little thing. ***(My Father)***

To the lady who lit lamps for me, lit my ways with affection: These are the words, dear mother; You were the woman who always pushed me, towards better and more beautiful ways, I hope that you accept this little thing. ***(My mother)***

To my beautiful wife: I dedicate this research as an expression of my sincere thanks and appreciation. For her efforts during my studies, she was the most supportive wife.

To the little hands that knock at the door of my days; So that affability and life may enter my days, I dedicate this research to you, my beautiful children: ***Noor, Abdul Sattar, Abu Al-Hasan, Al-Rabbab, and Nahi.***

*My brothers especially my sister (**Mariam**)*

Acknowledgement

I want to thank my supervisor **Asst. Prof. Dr Alharith A. Abdullah** for his support and valuable guidance.

Abstract

A blockchain is a shared distributed database or ledger between computer network nodes. A blockchain serves as an electronic database for storing data in digital form. Therefore, it is important to keep an eye out for blockchain applications that are used in a variety of industries, such as healthcare services and their capacity to respond to dangerous situations, the Internet of Things (IoT), a network of interconnected smart devices, and voting as technology influences democratic institutions.

Network Function Virtualization (NFV) is considered to be a hopeful technology for supporting blockchain with many features like flexible networks and intelligent equipment. NFV decreases the expenses incurred on the maintenance and operation of assets that are generated through expenses, in addition to capital expenditures based on the isolate the physical devices from the main tasks executed by that equipment. The prominent challenges in NFV are the processes of transition, vendor compatibility, network management, rapid growth, and security.

Blockchain-virtualization is a critical problem. The larger a blockchain gets more significant and grows, the more vulnerable it gets. Then turning it into a virtual approach to reduce this vulnerability.The unsolved issue of slow transaction speed is emerging as a main problem in the blockchain network.

A new approach for virtualizing blockchain work based on NFV with automated execution of smart contracts among virtual nodes cloud-based is proposed. That began with building a private blockchain and then applying The NFV to its functions. Many issues have been addressed by combining NFV with blockchain such as (cost, scalability, and speed of execution), which has resulted in the creation of virtual nodes, along with smooth engagement among them and the administration of transactions among nodes and clients, suggesting optimal network administration. The proposed system has been applied to Amazon Web Service (AWS).

The suggested work shows indicate that a throughput of up to 20% has been obtained by applying NFV, accompanied with a speed of implementation of up to 50%. Furthermore, hardware expenditures are minimized, and a secure environment is finally often used to protect the system against virtual threats. Through a confidential file-sharing infrastructure, a private blockchain is established to overcome the security issue. Various institutions could use this private blockchain. To effectively encrypt the files, a significant technique that considers a significant portion of the field of cryptography is used. The other assures that the files are only accessible by the recipient.

In addition, compared to Ethereum with FTP (File Transfer Protocol), a reasonable velocity was attained during transmitting the data. After that, smart contracts were created to facilitate file transfers among nodes.

Finally, presented an approch having a licensed blockchain-NFV to handle and reserve the Electronic Health Files (EHF) the report of the patients. This technique ensures transparency and specifically immutability, which are necessary for protected administration and storage, guaranteeing a technique that is well organized jointly concerning doctors and patients additionally, optimistically, bringing regarding revived confidence in the general health scenario. Also, the requesting purpose is that our profession may present to achieve a velocity of the blockchain system to EHF and encourage different discussions with health organizations to completely utilize the possibility of the mentioned technology.

.

Declaration Associated with this Dissertation

Some of the works presented in this dissertation have been published as listed below.

1. Jawdhari, H. A., & Abdullah, A. A. (2021). The Application of Network Functions Virtualization on Different Networks, and its New Applications in Blockchain: A Survey. Webology (special issue).
2. Jawdhari, H. A., & Abdullah, A. A. (2021). A novel blockchain architecture based on network functions virtualization (NFV) with auto smart contracts. *Periodicals of Engineering and Natural Sciences*, *9*(4), 834-844.
3. Jawdhari, H. A., & Abdullah, A. A. (2021). A New Environment of Blockchain based Multi Encryption Data Transferring. Webology, 18(2).

List of Contents

CHAPTER THREE……… VIRTUAL FUNCTIONS BLOCKCHAIN BASED ON NETWORK FUNCTION VIRTUALIZATION

List of Tables

List of Figures

Table of Algorithms

List of Abbreviations

Abbreviation	Description
API	Application Programming Interface
Amazon S3	Amazon Simple Storage Service
AWS	Amazon Web Services
BC	Blockchain
BSS	Business Support System
CPU	Central Processing Unit
DLT	Distributed Ledger Technology
DoS	Denial-of-Service
DPDK	Data Plane Development Kit
DPI	Deep Packet Inspection
DSA	Digital Signature Algorithm
DSAv	Digital Signature Algorithm-Virtual
EC2	Elastic Compute Cloud
EC2	Elastic Compute Cloud
ECC	Elliptic-curve cryptography
EHF	Electronic Health Files
EM	Element Management System
ETSI	European Tele-communications Standards Institute
FHIR	Fast Healthcare Interoperability Resources
FTP	File Transfer Protocol
GWA	Grey Wolf Algorithm
HL7	Health Level 7 (HL7)

IoT	Internet of Things
IPv4	Internet Protocol version 4
ISP	Internet Service Provider
IT	Information Technology
MANO	Management and Orchestration
MVNO	Mobile Virtual Network Operator
NFCs	Network Function Centers
NFV	Network Functions Virtualization
NFVI	Network Functions Virtualization Infrastructure
NFVO	Network Functions Virtualization Orchestrator
ONC	the Office of the National Coordinator for Health Information Technology
OSS	Operations Support System
P2P	Peer-to-Peer
PoA	Proof-of-Authority
PoS	Proof-of-Stake
PoW	Proof-of-Work
REST	Representational state transfer
RSA	Rivest–Shamir–Adleman
RSAv	Rivest–Shamir–Adleman-Virtual
SBC	session border controllers
SDN	Software-defined networking
SFC	Service Function Chain
SHA	Secure Hashing Algorithm
SHC	Student Health Center

SHVS	Standard High Volume Servers
SM	Smart Contract
TOSCA	Topology and Orchestration Specification for Cloud
TPH	Transactions per Hours
TPM	Transactions per Minutes
TPS	Transactions per Second
UI	User Interface
VBC	Virtual Blockchain
VIM	Virtualized Infrastructure Manager
VMM	Virtual Machine Monitor
VMs	Virtual Machines
VNF	virtualized network function
VNFD	Virtual Network Function Descriptor
VNFM	VNF Managers
YAML	Yet Another Markup Language

CHAPTER ONE

GENERAL INTRODUCTION

1.1 Introduction

NFV refers to a technology created with the important purpose of accelerating the distribution of modern network servicing in the telecommunication field. NFV's major goal is to expand its future evolution aims. A closer examination of the communication environments these days shows that it is rather crowded with many different proprietary hardware devices. The launching of a new network service demands the insertion of different hardware entities on account of the available space, causing much more hardness as its complication increases[1].

NFV is a new approach to many operations in the network like scheming and deploying, in addition to supervisory control network services through disconnecting the hardware of network from the services or all other functions which work inside them. The NFV has a clear duty which is replacing the hardware-centric devices by software implemented CPUs which are executed on typical servers [2] [3].

The major aim of NFV is to convert the functions of the network into a virtualized manner such as proxies, load balancers, firewalls, routers, or any other network functions that are implemented into stable hardware [4]. Such virtual network functions may be implemented in servers and hardware resources like computation, storage, and networking hardware, which are seen as a joint resource collection. They may migrate or be instantiated in several positions within the networks depending on the job imposed on the network. It covers the running of functions in software which may present its service on industry-standard servers with no need for the inauguration of modern entities [5].

Blockchain is regarded as an adaptable choice for building a secure platform due to its characteristics, such as the data traceability and resistance of tamper. It has been broadly supposed that besides its utilization in economic services (e.g. Bitcoin), blockchain may also be executed in application-oriented situations [6], [7]. A blockchain is considered to be a distributed ledger, like a database, but instead of being managed through a central authority (i.e. a company like Google or Small organization), the record is divided over various computers, which can be placed all across the world and run by anybody who has an Internet connection.

For decades, blockchain network gained a great reputation through ledgers that non-changeable in a distribution format along with platforms for independent data-driven planned. Introduced through the popular venture cryptocurrency project ‘‘Bitcoin’’ [8], the blockchain network was basically utilized as the essential spine of a public, distributed ledger system to prepare asset transactions based framework of digital symbols within Peer-to-Peer (P2P) servants. Blockchain networks, particularly the ones utilizing open-access systems or policies, are characterized by their essential features of disintermediation, public approachability of network functionalities, and tamper-resilience [9].

A smart contract is a significant managed factor in blockchain-enabled applications as it offers the capability of automatic control [10]. The secure medium led through blockchain is tightly bound to processes through executing the smart contract. Implementing blockchain-enabled resolutions is an anticipated technical route for supporting cloud computing.

In general, cloud computing can be described as the services that include devices and programs linked to a network of servers [11]. In essence, cloud computing is a philosophy and design concept for computer architecture. It is far more complex but yet lot simpler than traditional computing architecture. The fundamental idea is to keep the Hardware, Operating System, and Applications independent from one another. By utilizing virtualization technology, the program can simply be moved automatically to another server in the event of any malfunction or virus attack, such as one on the operating system, as opposed to shutting down the entire system.

The main aim of the dissertation, a new method is offered to virtualize the work of the blockchain based on the NFV with auto work of the smart contract between virtual nodes based on cloud computing. By blending NFV with Blockchain, all of the above-mentioned challenges have been overcome by moving to software environments through creating virtual nodes, as well as smooth interaction among them and managing the transactions between nodes and clients, indicating ideal network management. According to the suggested work, using NFV has resulted in throughput gains of up to 20% and implementation speeds of up to 50%. Additionally, by using NFV, a high throughput has been achieved with the time difference. In addition, the costs of the hardware are eliminated and eventually a secure environment is used which distances the system from virtual attacks. Also, provide a one-of-a-kind example that uses a licensed blockchain-NFV to manage and store patient Electronic Health Files (EHF). This method ensures transparency and, more precisely, immutability, which are required for secure administration and storage, ensuring a well-organized system that involves both doctors and patients, and, hopefully, restoring confidence in the overall health situation. Our profession may also present to obtain a speed of the blockchain system to EHR and promote different dialogues with health organizations to fully employ the potential of the stated technology, according to the requested purpose

1.2 Literature review

The literature review consists of the many work of blockchain and its applications and NFV with its applications. An aggregate of many scopes of application were determined. A comprehensive discussion of the related outcomes is discussed in the subsections.

1.2.1 Blockchain with Applications

The benefit of utilizing blockchain the find solution to many of the financial, community, and governmental challenges faced by the world, in addition to mentioning in detail the major applications and services of blockchain in developing countries. It illustrates how blockchain has the ability support boost transparency, construct confidence and improve transaction capacity [12].

The blockchain contains different implementations outlying beyond the environment of alternative currencies and far exceeding finance. This investigation attempts to answer how the implementations of Blockchain technology are managed [13].

The Blockchain system as a technology that has the perfect ability supply a powerful cyber security difficult situation solution and a elevated class of privacy security. blockchain supporters claim that consider technology is secure due to its design. In a blockchain systems , third parties are no necessity to keep data [14].

The problems of the existing supply chain such as transmission connection problems among vendors are handled. Also, they suggested a new ideal of the supply chain through blockchain where whole the partners of the supply chain keep each of their transactions inside the blockchain to guarantee more elevated security [15].

A smart agribusiness network security system that depends on the private blockchain. Issues of a surveillance communication frequency of packages via utilizing a darknet to avert DDOS (A distributed denial of service) attacks and IoT(Internet of Things) sensors to observe farms and agriculture [16].

Blockchain technology promises to overcome concerns with trust and enable a trustless, secure, and authenticated system of information exchange for supply networks' operations and supply chains. The new supply chain implementations are moving away from blockchain and toward a broader concept of distributed ledger technologies. The logic behind existing and potential applications of blockchain in supply chains and logistics offered [17].

Some of the disruptive developments that are predicted to affect financial services as a result of quick technological advancements have been studied. Also covered are virtual currencies, the origins of Bitcoin, and a description of blockchain technology, including its definition and significance. The regulatory obstacles to the implementation of this innovative technology are briefly mentioned in the article. Many decision-makers are trying to evaluate how likely it is that the adoption of bitcoin (or other cryptocurrencies) will spread throughout their individual countries. Laws and regulations may be encoded into the blockchain itself, he claimed, making them automatically enforced. In other circumstances, the ledger can serve as legal proof to access [18].

A systems tried to reduce energy exploitation by limiting the interest of whole the hubs through the network based on placing a property of focus on the idea of fair reward diffusion that isn't supposed in general cryptocurrencies [19].

A distributed system of Antimalware database management using a proper blockchain that works on enhances the security of the system via creating transmitted malware evasion of program. blockchain may ensure more satisfactory information administration in the absence of a third party [20].

1.2.2 NFV and Virtualization

Both a transaction model and a blockchain customized for NFV are provided. A flexible and straightforward modular architecture is offered by BSec-NFVO to secure orchestration. created a working prototype of BSec-NFVO for the Open Platform for Network Function Virtualization (OPNFV) using a modified version of a consensus protocol that is collusion-resistant in the typical situation. The findings demonstrate that BSec-NFVO exhibits stable performance as the number of consensus participants rises and incurs little overhead for the cloud orchestrator [21].

An opinions on applications that issues comprehensive survey on NFV introduced, which begins from the introduction of NFV motivations. They clarify the principal theories of NFV in terms of terminology, calibration, and history, and how NFV deviates from the common middlebox depend on the network. Then, the official NFV structure is presented utilizing a bottom-up strategy, depending on which the identical utilized problems and answers are also demonstrated. Lastly, to quicken the NFV deployment and dodge traps so far as potential, they view the difficulties met by NFV and the stream for future trends [22].

A wide survey on NFV platform configuration, investigation only goals existing NFV platform applications. He starts with an architectural design of the regular source NFV platform and offers his taxonomy of current NFV platforms based on the primary object of design. Next, completely examines the design space and develops the implementation options every structure opts for [23].

There are contribution goes in two directions. First, they present a general survey of the hierarchical communications system managed through a primary computer NFV ecosystem, including a wide range of techniques, from low-level hardware speedup and bump-in-the-wire offloading ways to high-level software speedup clarifications, which includes the virtualization mechanism itself. Second, they conclude principles concerning the design, improvement, and process of NFV-based deployments which reach the elasticity and scalability demands of current communication networks [24].

An architecture subsequent a top-down way, It is split into many interactive layers, application layer (e.g. services like OSS (Operation Support System)), control layer (i.e. SDN (Software Defined Network)) controller with distributed operating system), and infrastructure layer (i.e. switches and gateways IoT) [25].

A pattern for strong security and network execution administration suggested. Also, exhibit a use-case to develop a special MVNO (Mobile virtual network operator) virtualized, that can facilely be extended and scaled for large capacity traffic and a number of users. Additionally, consider the diverse ingredients and put many enabling factors of MVNO networks and supply a benefit-cost analysis of utilizing MVNO [26].

A survey of the two types, highlighting their important highlights and their association was performed; to give a comprehension of the two perfect types and how they resolve different subsets of the many problems of system versatility [27].

A method for deploying a virtual firewall function in addition to a virtual routing function to reduce network costs offered . The evaluation's findings have shown what follows: (1) Installing a packet filtering feature, which is a component of the firewall feature, in the sending-side region can also cut down on unnecessary routing processing and transit bandwidth usage, which lowers the cost of the network. (2) The amount of network cost reduction is enhanced in proportion to the volume of packets filtered by the sending-side area's packet filtering function. (3) The effectiveness of statistical multiplexing in lowering network costs increases with the bandwidth cost relative to the cost of the routing function. (4) The proposed method would be capable of deploying the ideal solution in roughly 95% of the cases [28].

The virtual distributed ledger technology (vDLT) is a service-oriented blockchain system with decoupled management/control and execution. According to their QoS needs, including confirmation latency, throughput, cost, security, and privacy, vDLT services and applications are divided into many groups. The current "blockchain-oriented" DLT systems have given way to the newest "service-oriented" DLT systems in this paradigm shift. Different QoS requirements are met through sophisticated schemes, such as categorization, queuing, virtualization, resource allocation and orchestration, and hierarchical architecture, which were influenced by the evolution of the old Internet. Additionally, smart contract management/control and execution are separated to provide QoS provisioning, enhance decentralization, and speed up vDLT evolution. Virtualization enables the dynamic creation and operation of many virtual DLT systems with greatly differing properties to support various services and applications [29].

1.2.3 Blockchain Applications in Healthcare

The technological and social obstacles depending on SHS via investigating state-of-the-art specialist opinions presented. Additionally offering a blockchain depends on the SHC (Student Health Center) structure to supply inherent security and solidity of the system. Finally, they addressed the problem of honest access to medical data [30].

A numeral of ingredients measures essential parameters regarding the human body such as blood pressure, etc. automatically with all mentioned the information is kept at locations protected based on suggested security algorithms. Finally, handheld important issues by addressing the smart model to discover illnesses, measure essential health parameters, and immutable repository [31].

An explanation of the future direction for healthcare data in the blockchain presented. Also provides an overview of the framework and interior functioning and protocols for addressing heterogeneous medical data. Finally, addressed the problem of the electronic medical record storage administration system [32].

Many contributions regarding using blockchain systems in clinical data sharing are suggested. First, they investigated the conditions of the Office of the National Coordinator for Health Information Technology (ONC) and their influences on systems that rely on blockchain technology. Second, they propose FHIRChain, which blockchain-based decentralized architecture that emulates FHIR data interoperability standards and is prepared to satisfy ONC demands through encapsulating the Health Level 7 (HL7) Fast Healthcare Interoperability Resources (FHIR) standard for shared clinical data. Third, they present a decentralized application that depends on FHIRChain utilizing digital health identities to certify parties in decision making. Finally, they loved the problem of permissioned clinical data sharing [33].

A “vaccine blockchain” system that relies on blockchain in addition to machine learning technologies is improved. The system is developed to backing vaccine traceability and may utilize to handle the troubles that regard to the vaccine production. Further, the benefit of machine learning in this system will be practical and useful advice or suggestion to fortification practitioners and beneficiaries, permitting them to select more acceptable immunization approaches and vaccines. Finally, addressed the problem of vaccine surveillance and traceability system [34].

A paradigm of telemedicine system utilizing blockchain systems for the healthcare of the village population and patient data security suggested. Using this model will enable people to control many issues like medical data security, economically, socially, and technologically. Finally, addressed the problem of a telemedicine system for protected data storage and trustworthy medical care [35].

1.3 Problem Statement

1. Blockchain virtualization is to reduce (cost ,scalability) and remove the miner term .
2. The larger a blockchain gets more significant and grows, the more vulnerable it gets. Then turning it into a virtual approach to reduce this vulnerability.
3. The unsolved issue of slow transaction speed is emerging as a main problem in the blockchain network.
4. Another significant issue network carriers are faced with is how to easily migrate from the actual network infrastructure to NFV-based solutions.
5. Proof of work demands effort on the part of the users this problem is due to a hash being integrated with another hash into every transaction.
6. Virtual Blockchain could ease interoperability of electronic health Files.

1.4 Dissertation Objectives

The purpose of this work is to develop the private Blockchain architecture and employ the NFV in the Blockchain environment. The subsequent aims are suggested to perform the research purpose:

1. Constructing a private network that involves all procedures and structures of blockchain to be able to guarantee the security of transmitting various data and consequently shield these data against attacks.
2. Constructing NFV from scratch and applying it in the blockchain environment.
3. Get the virtual functions such as key distribution, distributed ledger, and hash function of blockchain depending on cloud services.
4. Get virtual nodes based on Constructed NFV.
5. Apply the virtual functions to healthcare systems.

1.5 Contribution

The contributions of this dissertation are observed in the following:

1. Construct a virtual private blockchain that is used for various data transmissions, such as images and text files.
2. Apply double encryption in private blockchain network.
3. Improving the structure of the blockchain systems via the utilization of double encryption algorithms, such as RSA and hash function algorithms.
4. Apply NFV to the private blockchain system (on three functions of blockchain key distribution, hash function , and ledger).
5. Building auto smart contract that aims to automatically carry out, manage, or record legally significant occurrences.

1.6 Limitation

- **Blockchain attack**

We wouldn't employ the 51% of attacks that occur when the majority of a network colludes against a small number of participants on the proposed system.

- **AWS cost**

The important problem in AWS is the cost, which we cannot work continuously with this incubator, as it requires large amounts of money if the reservation is annual. In addition, we cannot deal with files of large sizes, because the larger their size, the greater the demand for storage, and thus we need an increase in the cost.

- **Ledger**

The suggested technique applies the dissemination of data (images, pdf files), but makes an effort to disseminate additional data such as audio and video.

- **NFV Security**

NFV offers a number of new network functionalities, but it also creates a window for additional security threats. By its inherent nature, software is less secure than hardware. From a security perspective, routers and firewalls on specialized hardware are more difficult to breach. Attacks known as Distributed Denial of Service (DDOS) are significantly more likely to target software. The platform needs to be protected from ongoing dangers that could overwhelm the network. A hypervisor can offer virtual machines (VMs) a high level of isolation, so if one VM contracts a computer virus, it may not propagate to other VMs.

1.7 Dissertation Layout

The remains of the Dissertation chapters are described in the following:

Chapter Two: Contain background and summary of the blockchain technology, NFV, AWS, and Consuses algorithm.

Chapter Three: Explain the construction of private blockchain, suggested the unique architecture of blockchain, and a new architecture for the healthcare system.

Chapter Four: This chapter explains the results and investigations that have been acquired based on the proposed technique.

Chapter Five: Shows the work's conclusions. Also, it offers different future work suggestions.

CHAPTER TWO

THEORETICAL BACKGROUND

2.1 Introduction

Blockchain is a technology that allows an individual or any party to transfer assets of value to another person safely and without the interference of any intermediary. A blockchain is a series of records or static blocks of data, and it is managed by a group of computers not owned by any single entity [36]. Blocks of data are secured and linked together using coding principles [37].

The blockchain network is independent, and not subject to any central authority. Because it is basically a shared and immutable record, and the information in it is open and available for anyone to view. Hence, anything built on the blockchain is inherently transparent. Also, blockchain transactions are free and have no direct cost [38].

NFV is a method that presents a characterized that is targeting network services to virtualize, such firewalls [28], in another term "the separation of network functions from exclusive hardware devices" and utilizing those functions as VMs NFV utilizes Information Technology (IT) virtualization approach to virtualize networks toward building blocks that rump connects or joining to provide exchanging of information services [40].

Furthermore, NFV increases and enhances the network function in addition to the supervisory control of networks, which have traditionally been run on proprietary hardware. These services are packaged as virtual machines (VMs) on commodity hardware, which allows service providers to run their network on standard servers instead of proprietary ones [41].

Cloud computing is one of the technologies that involve the transfer of all processing in addition to the storage space of computers to the cloud for a server device accessible through the Internet [42]. IT programs are transferred from products into services. Therefore, this technology help to remove the issues related to the development and maintenance of IT issues faced on behalf of the company that makes use of it.

Thus, the aspects that are given most attention are the use of such exclusive services, and the cloud computing infrastructure that relies on advanced data centers to make big storage area available for users [43].

2.2 An Overview of Blockchain Technology

Blockchain is an actual revolution in the world of financial trading. It even extends beyond that field to be a thorough technology which can be used as the base for generating a complete technological system such as the Internet system that is dealt with nowadays. The blockchain technology is dependent on a peer-to-peer system [44]. The transactions occur among users of this technology without a third party. Being a decentralized technology, nobody has the ability to control the operations that occur via it: no government agency or company could take part in the management or regulation of the course of work. Every transaction is secured with a digital signature, sent to the recipient's "public key," and signed utilizing sender's "private key." The owner of a cryptocurrency must demonstrate ownership of the "private key" in order to spend money [45]. To exemplify, if Bob sends some data to Alice, no one will be able to know Bob nor Alice, because the people in the blockchain system are simply represented by codes, as shown in Figure (2.1).

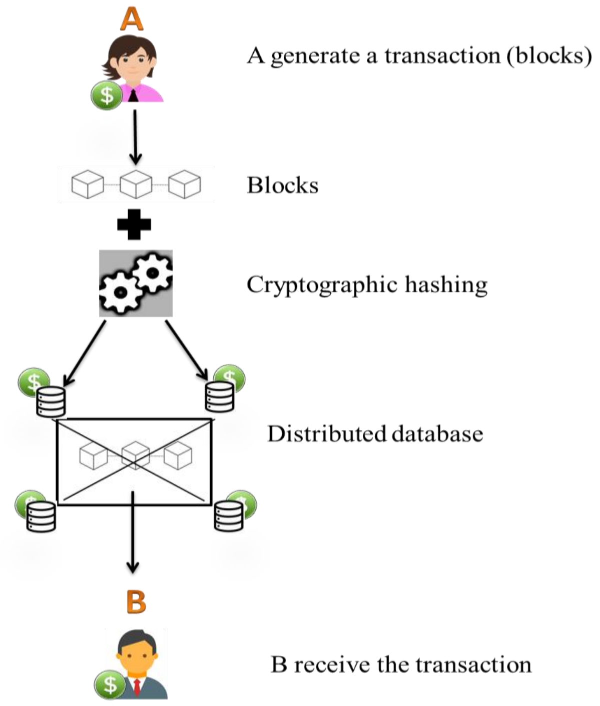


Figure 2.1: General Process of Blockchain

Blockchain is a straightforward and innovative method to push through data between two persons or entities in a completely automated and secure way [46]. One of the parties generating the transaction via generating a block which is confirmed via thousands, possibly millions, of computers, and distributed throughout the network. Then, the verified block is added to a stored chain within the network, which creates a unique record linked to other records. For a single record to be falsified, the entire series has to be falsified on millions of computers. This is practically impossible [47].

In a technical perspective, a blockchain is just a chain of data blocks, hence the term "blockchains". The terms "block" and "chain" in this context refer to digital information (a block) stored in a public database (a chain).

The blocks that make up a blockchain consist of a set of digital data. It can be viewed as a ledger that contains a collection of information related to specific financial transactions. Once a block is completed, a new block is started to be opened, connected to the former block, and then attached to the chain. A block is permanent; once formed, it can in no way be altered or changed. Block can generally be divided into two parts [48].

Block header: The header is made up of several components, such as the software version number, the previous block hash code, the block registration date, transaction amounts and other information, as shown in Figure (2.2).

Block body: The block body contains all the transactions installed in the block, in addition to information about the people involved in the transactions. Instead of using real names, transactions and purchases are recorded using a digital signature, which is more like a user name, and requires no personal information.

Each block contains its own hash code that distinguishes it from the rest of the blocks; this code is composed of a long string of letters and numbers for example (0000000ddjyd6d6d87q2bnc024bs023g29ls73). Single block storage capacity can be up to 1MB of data. This means that a single block can hold many thousands of transactions. A blockchain may also consist of millions of blocks.

It is possible to compare regular banking transactions with blockchain transactions. A blockchain is similar to a bank transaction record, as a block can be represented by a single transaction that an automated teller machine confirms, for example, after a user withdraws an amount of money from it. When a block stores new data, it is added to the blockchain that consists of a series of interconnected blocks. There are several reasons why blockchain is admired by many people [49]:

- Decentralization: it is not a property of one entity.
- Unchangeable: no one can alter the data inside it.
- Transparency: anyone can track the data within it.

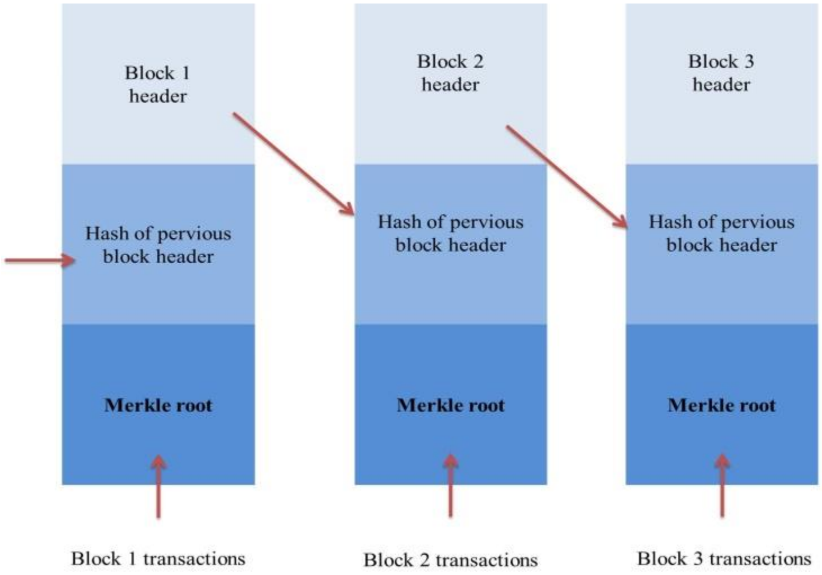


Figure 2.2: Blockchain Structure

In light of the reasons mentioned above, a number of characteristics and advantages of blockchain technology can be pointed out. Being a technology which is nobody has control over is considered one of the most appealing features of the blockchain technology. As it has a decentralized system, it is denoted that this technology is not the property to anybody but rather the ownership of the actual users of this technology. Supporters of blockchain, and digital currencies in particular, argue that governmental (or government-related entities such as banks) have no right to control people's money. They state that the people themselves should have the authority and the right to conduct monetary transactions without the need for an intermediary, thereby supporting a mechanism which helps decrease money transmission fees to the minimum.

Another feature is the scale of security and privacy provided by this technology [50], which is relatively good. Despite the fact that traditional financing systems owned by banks and governmental entities do have a certain level of privacy and security, however, their systems are vulnerable to breakthroughs as they have the risk of being penetrated. Penetrating blockchain systems is somewhat impossible, as this would require the alteration of the information and data of millions of devices that are distributed all over the world.

As for the last feature, since blockchain users are dealing with digital currencies, this technology guarantees a high level of secrecy and privacy. The users are only referred to as encrypted codes within the system, and no one has the ability to uncover any piece of private information concerning other users. Also can be traced back to the fact that this technology is managed through a decentralized system.

However, blockchain technology itself is not contentious, has operated without a hitch for years, and is successfully being used for both financial and non-financial applications in the real world [51]. Yet, no one can deny that blockchain technology in general is a technology that deserves attention as it imposes itself, in one way or another, onto the global stage, and cannot be ignored under any circumstances.

Concerning the future predictions for this technology, the scene is not completely blurry. In fact, there are several signs regarding the blockchain technology that can be used to clarify the scene, as follows:

- Digital currencies are recognized by many countries, especially Bitcoin. There are many large countries in the world that have begun to adopt Bitcoin as a recognized currency, including the US, Australia, and the Netherlands.
- Facebook, in cooperation with many other companies, announces the launch of its digital currency: Libra. (Libra is not a traditional digital currency like other digital ones, but it is a digital currency of a special nature behind which many large companies and institutions stand).

Briefly, the blockchain technology refers to a modern revolution in the world of IT which has the ability to resist different circumstances and eventually evolves and expands its uses. The number of users is increasing noticeably, and this is a significant indicator of its development possibilities in the future such as smart contracts and other uses that may grow to be essential in everyday life. Blockchain can simply be described as a system that carries a new view of old things.

2.2.1 Blockchain Concept

As has been mentioned before, decentralization is one of the basic concepts on which the blockchain technology depends, as the system depends on a group of nodes, each computer or server in this system represents a node that performs several tasks such as storing transaction information, the timing of its occurrence, and the addresses of the blocks connected to it. By keeping several copies of the financial transaction file in different nodes around the world that anyone can access, there is no longer a need for a trusted third party to act as an intermediary to manage transactions between people.

The application of blockchain involves a total of six layers [52]. At the present time, blockchain is of rather high complexity and requires years to develop become more simplified and comprehendible. It is necessary to divide the blockchain into several technical layers, as follows:

- **Application Layer:** The mission of the application layer is to develop blockchain solutions to be used across various applications and industries.
- **Models Layer:** The task of models layer is to facilitate smart contracts, as it is responsible for creating work flows and determining the manner through which the users interacts with the system.
- **Contracts Layer:** While the model layer deals with the workflow, the contract layer deals with the contract itself. Given the financial ramifications to the undefined or well-executed contract layer, much attention should be paid for ensuring the correct issuing of contracts, free from any potential vulnerabilities.
- **System Layer:** The system layer includes of the basic components required for maintaining the blockchain itself, like the consensus protocol and its associated sub-systems.

- **Data Layer:** The data layer is responsible for managing the information that is stored on the blockchain, both inside the transmitted chain and the data base (off-chain).
- **Network Layer:** The network layer in blockchain network topology features P2P networking, client connectivity, connectivity strategies, and user behavior.

The important step that should be taken into consideration to accommodate the direct effects of regulatory and commercial [53]. Blockchain application is the understanding of its architecture. Since the blockchain is a part of the information technology, an information technology architecture can be provided. This consists of three layers as shown in Table (2.1), in a sequential form, each of which complements the other.

Table 2.1: Blockchain information technology architecture.

Upper Layer	It refers to the blockchain application. This layer is the final output to the work as a service presented by the developer that uses this environment.
Middle layer	blockchain ledger distributed ledger technology (DLT). Distributed ledger technologies are very popular. One of the technologies that fall under the protection of DLT is the blockchain based upon which it is constructed.
Down Layer	Hardware of the blockchain. The network of the blockchain is indicated via the many nodes which depend on the computational power to add a strong footprint. It is characterized by applications to participate in the consensus (confirming and saving transactions of that particular blockchain).

2.2.2 Work Blockchain technically side

Blockchain is a network of devices that communicate with each other and communicate using a peer-to-peer network, meaning that the operations between them take place without an intermediary. The blockchain operates in a distributed log system [54].

That is, a record containing all transactions that occurred on the blockchain network from the beginning of its inception is shared, meaning that any data transmissions that occurred on the network are saved in this record, and the record is shared with all devices on the blockchain network. Furthermore, every device on the network It is called (node) which has an updated version of the transaction history that contains all the previous transactions.

Thus, if the first party wants to transfer or send data to a second party, a broadcast of the request is made on the blockchain network (the request is sent to all devices on the network) in order to verify the process to ensure that the first party owns the data that it wants to send [55]. Through the devices on the blockchain network, where each device on the network reviews the record that it has to ensure the availability of data with the first party, where each device reviews the previous transactions of the first party in the record, and if it finds that it has previously received the intended data. In this case, the first party owns the sent data, and therefore the transmission process is agreed to be completed.

All operations that take place simultaneously are encapsulated in a new block and added to the block chain Figure (2.3), the update is sent to all devices on the blockchain network, thus the existing record on all devices becomes updated.

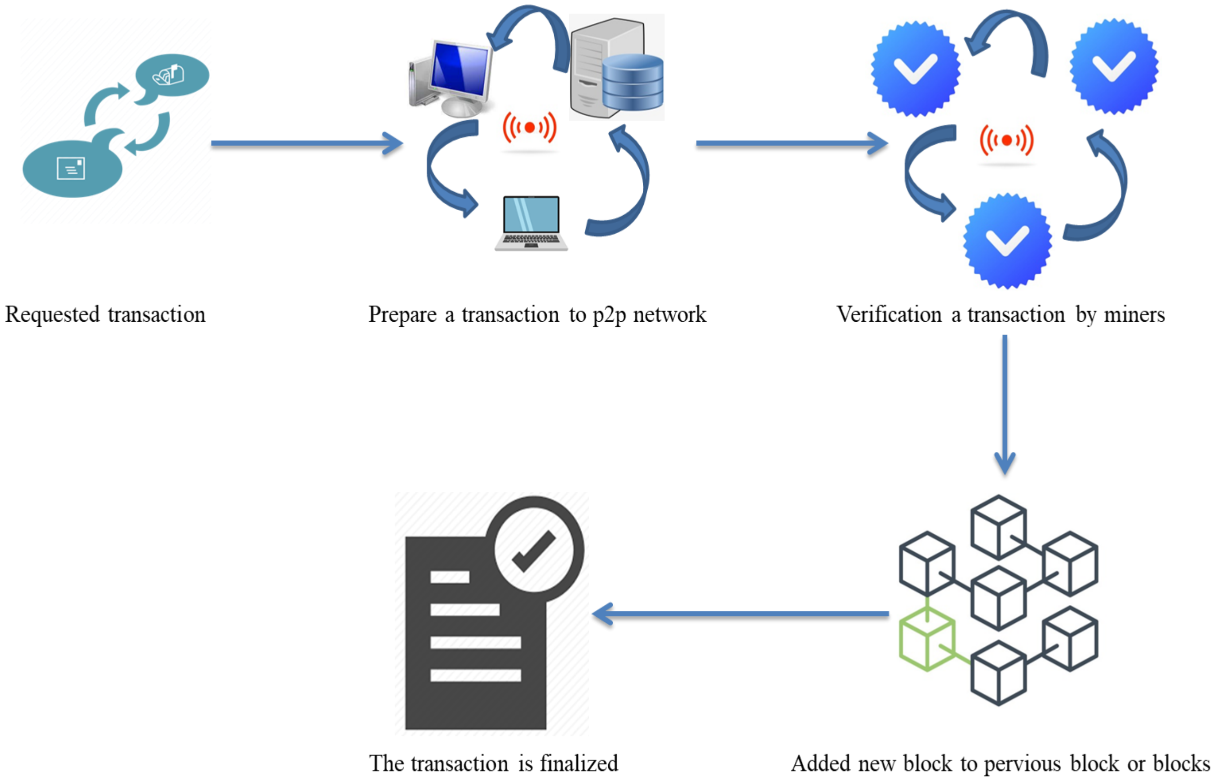

Requested transaction
Prepare a transaction to p2p network
Verification a transaction by miners
The transaction is finalized
Added new block to pervious block or blocks

Figure 2.3: Blockchain Technology work [56].

2.3 Network Functions Virtualization (NFV)

NFV is an idea in network structure that separates hardware and network missions utilizing virtualization mechanisms [2]. Through virtualizing whole classes of network physical device functions toward modular systems, NFV reaches more inclusive scalability in the collection of physical devices that are interconnected via links. These are utilized to switch information among the devices in addition to computing services which are that considered a cross-discipline that includes both the science and technology [5].

NFV uses common server-virtualization techniques such as those distributed in enterprise-class IT, however, it is unparalleled. The use of hardware devices through various network functions is unimportant to virtualized network function (VNF). Alternatively, one or more VMs could deploy distinct manners and software on the switches, Standard High Volume Servers (SHVS), or cloud computing infra-structure that has the ability to include VNFs [57].

Depending on the interpretation of the European Tele-communications Standards Institute (ETSI), the main objective regarding NFV is to convert the direction in which network operators design networks through developing the principle of IT virtualization approach. This will merge numerous network tools into industry-standard like giant-sized servers and switches. In addition to the storage that may positioned on the data center either within the network or in the end-customer building. NFV swap the hardware devises (black boxes) still predominate the built-up foundation of networks [58]. The following sections present the architectural features of NFV, as well as, their reliability and availability.

2.3.1 Architecture of NFV

NFV provides an open architecture with a lot of resilient options for deploying NFVI solutions. The ideal infrastructure or architecture of NFV is made up of three particular layers: NFV infrastructure (NFVi) – with regard to equipment and services of cloud to perform network applications, Virtual Network Functions (VNFs) – application program which is responsible for providing a particular network job (such as routing, authorization of access to data, and mobile core), and Management Automation and Network Orchestration (MANO) which possess the capacity to turn network parts or components in the issue of hours instead of months and permits to move in dexterity [59]. However, it may cause some forms of disorder within the virtualization and NFV process, thereby indicating the necessity for proper management at an early stage as highlighted in Figure (2.4).

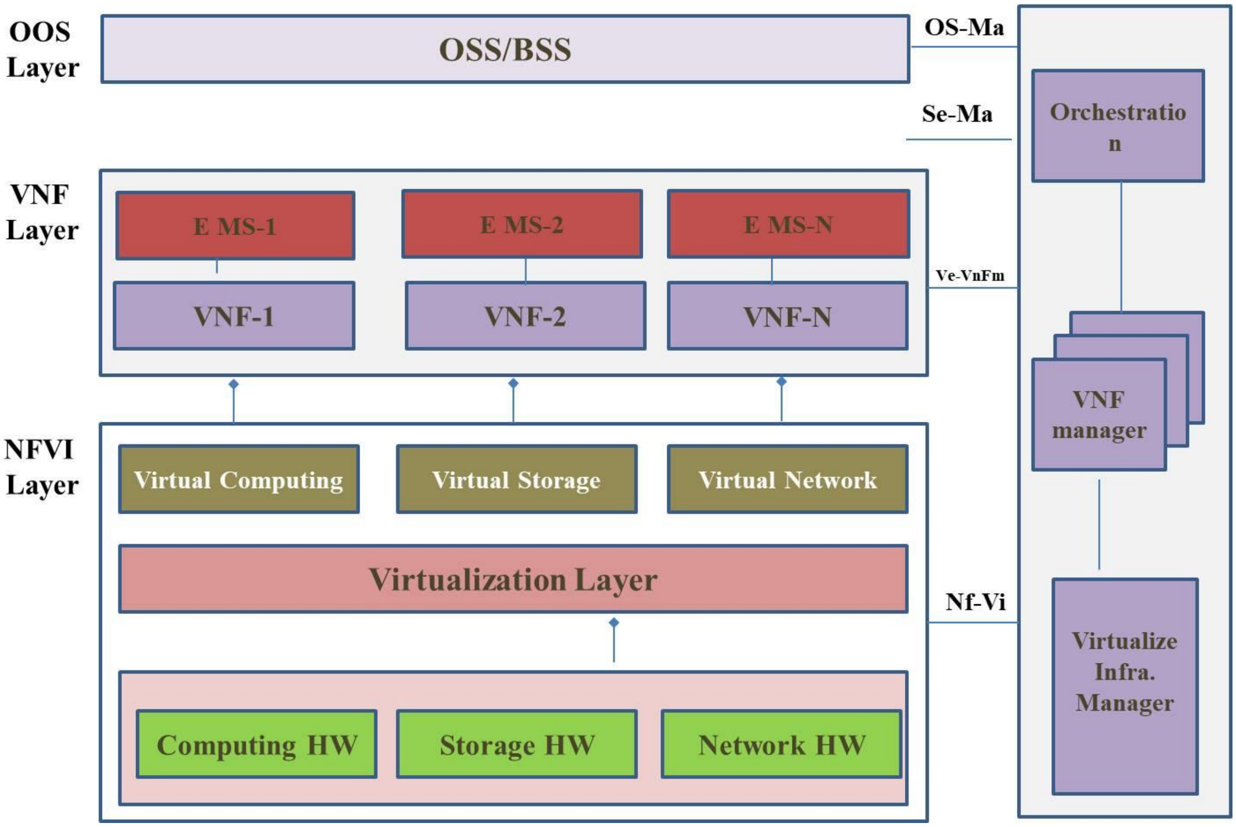


Figure 2.4: NFV Architecture [60].

2.3.1.1 Virtual Network Functions (VNFs)

VNFs can be described as a function that is executed using software based on the infrastructure of NFV. VNF can be implementing onto numerous VMs, each of which ought to be supervised via a module referred to as the Element Management System (EMS). This is considered after the design of the VM-instance and its configuration, control, performance of security, and achievement of implementation. The EMS is assigned fundamental information that is necessary for Operations Support Systems (OSS), and implements the administration functionality for a VNF-instance [61].

2.3.1.2 Management and Orchestration (MANO)

The MANO operating field involves the orchestration and lifecycle administration of physical and software resources. MANO has three items that form the infrastructure virtualization and lifecycle administration of VNFs, whereby the focus is on total virtualization-particular management missions that are needed in the NFV framework [62]. The Virtualized Infrastructure Manager (VIM) is a job bulk of the MANO working field which is in charge of the following things: controlling, managing and monitoring the NFVI count, the storage, and the resources of the network. This functionality reveals that VNF Managers and NFV Orchestrators are given the capacity to deploy and manage VNFs. It also assigns the same job to the hypervisors and controllers in the NFVI [63].

2.3.1.3 NFV Orchestrator (NFVO)

This aspect is based on various Virtualized Infrastructure Managers to implement the orchestration of NFVI resources which generate whole Managers of the VNF, and it is in charge of the management of the lifecycle of VNF instances. NFVO reacts together with the NFV exterior module (OSS/BSS) to provide an initial policy-based layout, in addition to its administration abilities. Furthermore, several models of network management service deployment are run along with VNF packages [64].

2.3.1.4 VNF Managers (VNFM)

The VNF manager is responsible for the administration of VNFs. They react with both EMS and VNF to obtain an appropriate provisioning and initial layout administration. The life process of VNF-instances are managed from VNFM via initializing, scaling, modernizing, and finishing the VNF instances. Each VNF-instance must be solely related to one VNF Manager [65].

2.3.1.5 Virtualized Infrastructure Managers (VIMs)

These entities run the orchestration through managing the NFV infrastructure resources. The VIM is interested in some aspects that belong to the control of NFV infrastructure resources such as computations, storages, and network resources. There is more than one functionality provided by VIMs, such as specifying, improving, and releasing NFV infrastructure resources, as well as managing how the resources are associated [66].

2.3.2 NFV Reliability and Availability

As has been mentioned above, the Network Function Virtualization dissociates network missions from dedicated hardware accessories and executes missions of the network in the virtual approach via software programming. In addition, it provides flexibility in terms of scaling the Service Function Chain (SFC) orchestration [67]. Despite the fact that the dynamics and elasticity of VNF improve the defense against attacks like DoS [68], the software virtualization context of VNF additionally leads to a list of security problems, vulnerabilities, and another malware types like backdoors, causing VNFs to become more weaker to attackers [45]. Corresponding to electromechanical hardware devices like VMs, protection missions like firewalls and load balancers are placed in the central location so as to ensure the security of a set of devices. Therefore, counter attacks toward VNFs is a significant issue in the use of NFV. Reliability remains an important case in the study regarding NFV SFC, with the focus on flexible service scheduling in the event of a dynamic server malfunction.

The service availability demands for NFV are required to be at least identical to those for traditional systems. These requirements can be achieved whenever the components of NFV provide equal or more acceptable performance in one or more of the following aspects: average of failure, time of discovery, time of repair, success average of the discovery and repair, and effect for every failure. In order to meet the service availability demands, it is necessary that a number of factors are taken into consideration in the VNF design, such as commodity-grade hardware and presence of various layers of software (i.e. hypervisor).

As NFV MANO components play a significant part in preserving the availability of service functions like fast service generation, dynamic acclimation to load, and overload banning, however they need to be extremely authoritative [70]. The comprehensive service resiliency is based on the implicit NFVI reliability as well as VNF inner resiliency.

2.3.3 Network function Virtualization Implementations

The Internet Service Provider (ISP) is the service provider that provides communication between companies and their branches. With the provision of connectivity, services such as firewalls, VPN encryption, DNS or Routing and others might be required either for the network itself or for its connection. Previously, real Firewall devices and other devices had to be provided by the ISP or service provider so as to achieve such services. At present, the NFV technology allows the ISP to provide the services mentioned above and more without purchasing real devices from different companies, as it only needs to provide servers, storage and a network [71].

Through these elements, the service provider can provide services quickly and with high flexibility. For example, a company needs 5 firewalls in its branches. The ISP will create five Virtual Machines and add firewall copies to them and distribute them on the network.

That is, all services have become virtual and the ISP does not need to buy specific devices, but rather buy copies or applications that implement these services which are installed on virtual servers. This will provide high flexibility as services will be on demand and the cost of services will be low. This means that no devices need to be updated, purchased or maintained, as all this will turn into programs. The section below explains and reviews some solutions and implementations of NFV in some technologies.

2.3.3.1 Network Function Virtualization for IoT

The Internet of Things (IoT) [72] gives an idea of capability of being connective to everything from everywhere at any time. Thus, this reaction of objects that are physically linked to the network may be carried out freely. IoT is closely linked to the mechanization of sensors, as most instance sensors and actuators are considered to be a part of a greater IoT network. It has been stated that the utilization of IoT equipment like computer, portable, mobiles, household appliance, manufacturing systems, electronic healthcare services devices, monitoring tool, and other extensions linked to the Internet would override 45.5 billion in 2020 [73]. Those IoT sensors in addition to the actuators might present different sizes of facts and statistics. Thus, the necessity to set up modern network access and essence devices ought to be raised. To administer the network accessories sufficiently, the network hardware resources need to be virtualized.

NFV is a free technology. It neither requires nor depends on the SDN technology, however it improves and eases the overall performance. NFV supplies a set of virtual applications that are referred to as (VNFs). These may contain procedures to Deep Packet Inspection (DPI), routing, security, and management of traffic, which may be merged to provide network services that are characterized to the IoT. Together, the SDN/NFV structure for IoT given in Figure (2.5) offers public interactivity of SDN and NFV to supply a secure connection in addition to the easier access to IoT platforms. These structures consist of NFVI, VNFs, and MANO plane, which assist one another so as to realize possible network virtualization and continuous network connectivity, as well as to execute effective packet influx basics via the SDN controller [6].

NFV is the technology which has the main goal of changing network functions before being operating by means of hardware into software, and executing it onto an unspecialized server. The way of refinement in the execution or performance of general-purpose servers and the work steps of server virtualization as seen with the virtual machine monitor (VMM) have made it possible to ensure a secure, scalable, and reliable performance that is serviceable even to carrier networks. By constructing a virtualized IoT-dedicated network using NFV technology and by optimally diffusing resources based on to service demands, it is possible to carry out network infrastructures which are pliable, economical, and effective to be used within the IoT.

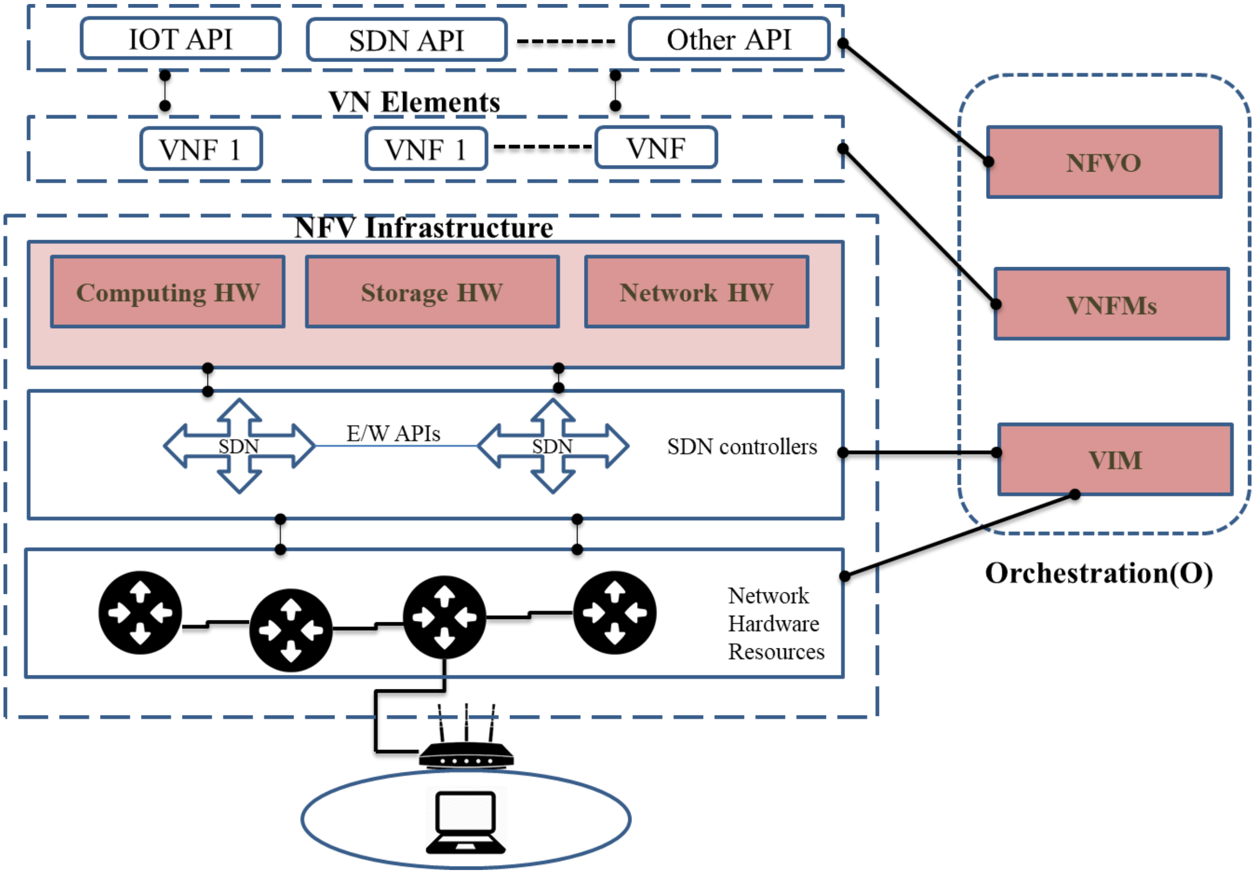


Figure 2.5:A common architecture for NFV merged with SDN-IoT.

2.3.3.1.1 IoT-Enabled Healthcare Network based-NFV

The IoT-enabled end-to-end devices are becoming more prevalent in healthcare [74]. Through a network, these devices are linked to one another. Even while this has a lot of benefits, there are drawbacks as well [75]. A network that can handle the obstacles is required for such an IoTenabled network. Security is an issue since it involves one of the most important patient health data points [76]. Additional networks may also be included in this network. As a result, searching for a patient record from a linked IoT-enabled medical imaging gadget requires agility and flexibility as well as the maximum bandwidth from the network of the associated hospital [77]. Architectures need to be innovative and have the ability to handle the aforementioned difficulties [78].

Administrators may directly program network control and abstract the underlying infrastructure for applications and network services thanks to the evolving NFV architecture, which separates the network control from the forwarding function. Additionally, NFV software tools enable IT firms to swiftly create, monitor, secure, and optimize the network while modifying traffic flow in response to shifting requirements.

NFV also offers a low-cost, standards-based, vendor-neutral method for network architecture that simplifies it while enhancing manageability, coordination, and control. Ethernet switches that are programmable, low latency, and high performing complement SDN well and aid in building a seamless network between a company's data centers and the cloud.

The healthcare sector is becoming more consumerized at such a quick rate that the market as a whole is being readjusted. Companies that have never previously influenced this industry are quickly rising to prominence as its primary power brokers. In order to respond to the expanding influence of data-driven customers, business models are being revised. Agile start-ups and well-known companies are forming novel alliances to benefit from the emerging digital-first environment[79].

The digital revolution has contributed significantly to this transition by enabling individuals to use connected gadgets like tablets, wearables, and handheld devices to live healthier lifestyles. The secret has also been the development of cloud-based technology. For instance, this year's groundbreaking strategic alliance between Philips and Salesforce.com resulted in the development of a platform that enables medical equipment to work with large amounts of data.

The most prevalent Internet of Things (IoT) application, smart healthcare, will optimize healthcare delivery and experience while lowering operational and capital expenditures (OPEX/CAPEX) for healthcare providers by utilizing cloud and fog computing. Collection, compilation, and analysis of unprocessed sensory data are necessary for smart healthcare applications and services.

2.3.3.1.2 Security IoT based- NFV

This part lists a number of different solutions regarding the field that utilizes NFV to ensure the secure performance of IoT. An expanded federation cloud architecture for advanced networking to guarantee the security of connected IoT devices [80]. The security solution uses virtual functions in a lightweight manner in addition to Service Function Chaining (SFC). A universal security policy could be obtained through the IoT gateways in edge computing, which can be done through building a chain of VFs for various aims, like firewall and discovery the intrusion. They observe the IoT network for weaknesses and attacks and separate the involved devices whenever discovered. Furthermore, SFC is mainly accountable for the management of the flow inside the IoT system, as needed for cloud and IoT structures to possess the suitable infrastructure for support. All this can be obtained or accessed through deploying a federation agent at the IoT controller. The transmissions themselves are achieved utilizing REST application software. The IoT network controller receives the configuring information via the federated network that has the ability to manage the network controller transmissions, as these are later on sent to the IoT gateways to be run. Lastly, the network controller has the ability to switch the information with the IoT proxy, which assists in the managing process of the data plane based on a programmable network protocol. A module is performed within the IoT network controller so as to secure the IoT-Cloud network slices.

The security direction by suggesting an approach that includes a unique (IPv4) called address resolution protocol (ARP). This protocol provisions security NFV services so as to guard upon attacks of ARP spoofing as well as the process of gathering information from every devices or endpoint. The work further offers some information about an SDN-based architecture to enforce the control of both fixed and constantly changing network access to the IoT for smart homes. Each of the ARP demands passes over a virtualized confided structure called ARP server, which is characterized by the full capacity to protect the entire operations of ARP, dropping the messages of ARP broadcast, and simply allowing ARP spoofing during ARP proxy through designing or adapting the server of ARP. In addition, resolving important issues in packet processing delay by following a technology called high-speed packet processing [81]. These technologies involve Deep Packet Inspection (DPI), with Carrier-grade Linux, multi-core processors, and virtualizations facilitating the distribution of cores among applications. Only the NFV-IoT associated donation focuses on this aspect. The building architecture contains domestic ingredients such as a data plane in addition to NFV dispatcher, with local security services.

The security agent, which is considered one of the main elements, always picks information based on the control plane user, IoT policy manager, security services, and the Ryu controller to ensure that the opposite network reaches the rules of control, often in a forced manner. The NFV sender receives all copied packages that are sent from the corresponding port. Next, these packages are sent to the identical security service depending on the sender index. A security agent obtains associated input to straighten the security services towards all influx. Depending on a test, a number of security declarations or alarms will be created. The server validation of IPv4 ARP may defend against the ARP spoofing, whereby the identical data plane development kit (DPDK) execution works in a great manner for the smart home IoT network [82]. NFV or SDN fields possess diverse components, applications, and orchestration managers. A harmful component in each of them might own dangerous influences on the entire framework. For instance, a malicious VNF via a normalization software trader, a host OS kernel, or MANO ingredient, may harm the whole network area. The extent to which those components are more secured in terms of integrity, confidentiality, and other regards associated with the principle of security will determine whether it will be referred to as well-protected. Therefore, we introduce the trend analysis of Internet of Things based on NFV with other techniques, as shown in Figure (2.6), that shows that the trends of IoT with NFV initially starts by providing the scalability and dynamic mobility for the IoT gateways. Then, the work develops and deals with the 5G network. However, in the middle of the period, there is a trend towards dealing with big data that comes from the IoT devices based on virtual networks.

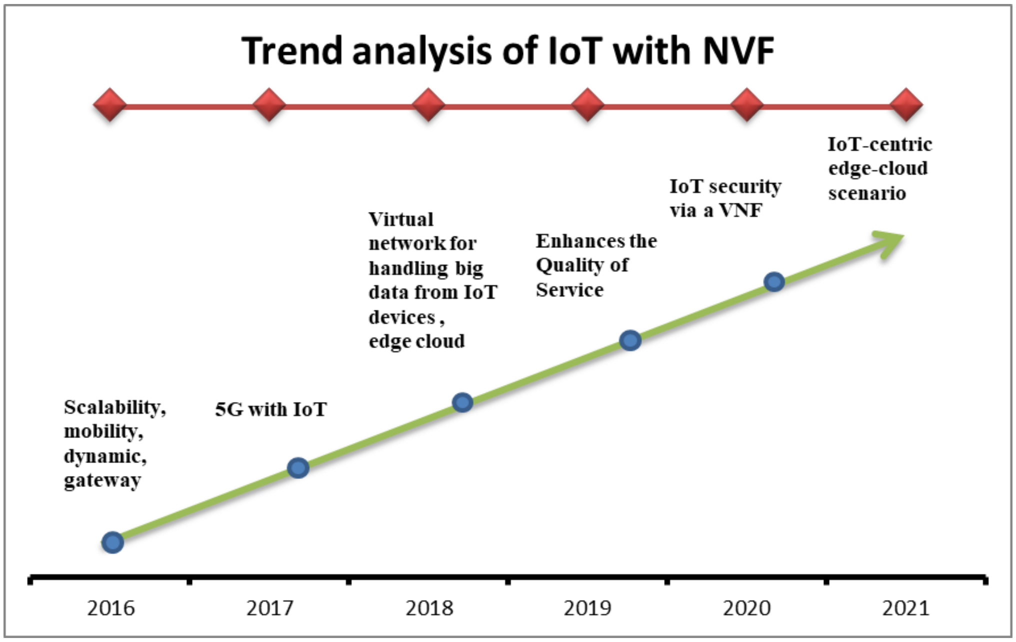


Figure 2.6: Trend analysis of IoT with NVF

2.3.3.2 Network function Virtualization for Cloud Computing

NFV has the potential ability to migrate enterprise data centers into the cloud [83]. Cloud computing enables several organizations to obtain the administration of their IT hardware infrastructure from an outside supplier to, as it is necessary for cloud services suppliers. However, as indicated in [84], the process of migration applications from particular data centers to cloud centers is found to be a rather complex procedure, as some applications tend to be network-based when providing their services like firewalls, and load balancers.

Considering the tasks that are executed during the resource exploitation within cloud services, the main focus has been on the placement of VM placement within bare-metal servers [85], [86], with little attention paid to the physical network hardware. Despite, a number of complicated services have been pointed out and eliminated from the services presented by data centers, such as 3G/4G IP Multimedia Services.

In this section, there are a number of challenges identified which need to be fixed so as to create actual Network Function Centers (NFCs), as well as to increase the network resource exploitation and to promote a simple network management [87]. As is customary and in a traditional way previously, network services were implemented as hardware based network appliance. An architecture that performs these network appliances as a software-based system with virtualized entities [88]. The studies in [89], [90] offer platforms to run middle-boxes for software-based. The suggested NFC follows the NFV idea and performs services of network as software-based system entities. Given the expansion of NFV, [50] considers the probability of getting help from an outsourcing enterprise to perform a series of operations on the middle-box to the cloud. It offers these outsourcing works to solve numerous difficulties that administrators of networks face and outsource more than 90% of middle-box hardware in networking infrastructure.

A Customer SDN Controller manages each customer's (i.e., tenant's) network [91]. A pioneer work which shows a structure for outer network function suppliers. They suppose a survive cloud service whereby every middle-box correlates with a virtual switch for providing the network functions, as well as for managing traffic streams and re-forwarding them. These switches determine the destination of the transmit traffic and its movement between more than one physical server, utilizing the common routing given by the cloud-based networking.

The placement of the NFVs in the physical boxes (such as personal computer) and usage of network bandwidth are important for the performance of cloud computing technology. A strategy which makes use of integer linear programming and uses in the arrange of minutes to select the placement of 1024 VMs in the data center of 16 servers. Their strategy takes into consideration the order of seconds to decide upon the VM placement [86]. The online type of the VM placement, whereby a demand is received each time the VM location is determined, based on a Markov approximation technique [85].

There are a number of advanced techniques proposed throughout the past two years which ultimately target the shift of computing and networking from the current manual order to fully automated process. Several solutions have been introduced which harmonize with the remnant infrastructure. Among these technologies are cloud computing and NFV. Generally, the mentioned solutions are prepared to ensure that computing and networking processes are extra automated and flexible to assist cloud and virtualized structures.

2.3.3.3 Network Functions Virtualization and Blockchain Security

NFV separates the network into parts that can work on ready systems. Ensuring the security of those parts requires embedded protection [92]. As the network parts are virtualized, NFV networks include a standard idea that does not resemble common networks. There is some complication about the virtual machine monitor (VMM), associated controls, and procedures for transmitting data, in addition to the boundaries between the virtual and hardware parts in networks.

Although using NFV as a tool with some environments may enhance the NFV security through using encoding information (encryption), immutability, Tamper-evident of these environments like (blockchain), yet the security in NFV remains one of the main difficulties and challenges in executing such an effective and powerful technology [93].

With the growing number of choices for NFV tools in many applications, there is an increasing direction towards solving some challenges in terms of security. It is rather challenging for a number of reasons, including hypervisor dependencies, flexible network boundaries, and the scalability of available resources. Other significant challenges include unauthorized access and leakage of data, for which it is recommended that virtual machines are used for controls of authentication as a solution [94].

So far, blockchain has received much attention in many fields, but, it additionally is remarkable difficulties and challenges need to be overcome, such as the majority attack. This takes place whenever the available resources are attacked to achieve a specific purpose with the correlative evaluation of the capabilities. Such majority attack could be best faced by obtaining the highest rating or feasibility whenever most transactions exceeded the block reward. In addition, the network hash rate was lower with marked variation and prone to reorganization with a new approach of mining [95]. Other issues involve fork problems (related to decentralized node version troubles), and scale of blockchain.

When the blockchain increases in growth, the data grows larger, and the operations (loading of store and computing) additionally become harder. Therefore, lots of time is required for data synchronization, which forms a huge problem to the user when running the system [96].

2.3.3.4 Network Functions Virtualization and blockchain Scalability

Users are creating exploding amounts of transactions on different networks. Network Functions Virtualization (NFV) presents a strategy to uphold these transactions with the economy, in addition to scaling it through converting network functions on custom-made hardware into software executed VNFs running on commercially available off-the-shelf (COTS) devices [97].

The difficulty of deploying VNFs for many users is the fact that it needs a high-efficiency distribution of any package flow that comes behind the distribution of the flow to the required VNFs applicable to the service [98].

The common data based on blockchain (e.g. Bitcoin) has a fixed size. This small size of data has become a source of anxiety for delays obtained via transactions. To build things more critical, the universality of options of third-party validations has been directed to the more rapid extension of the blockchain [99, 47].

The problems of blockchain scalability may be classified into three divisions: storage space, cost-of scalability [100], and reaching distinct output-with-scalability. Now, the fixed block volume of the blockchain blocks turns out the greatest impasse. Blockchains are obverse to an increase in pausing time demanded by transactions because of the small block volume. Furthermore, for blocks with a short block creation time, several forks are noticed to be built through the waiting time duration of the former block. This indicates that the block creation time duration should never be decreased arbitrarily. Consequently, the blockchain output seems not to increase properly. Blockchain users have to spend money on the transaction cost that occurs. It becomes onerous to micropayments and eventually affects the blockchain. Lastly, besides the development in size application and the extension of blocks, the chain expands and needs storage, therefore, the memory becomes a problem.

2.3.3.5 Network Functions Virtualization and blockchain Storage

Virtualization has performed a primary part in labeling different difficulties in the fields of IT [101]. Typically, virtualization indicates mechanizations created to present an abstraction of essential resources (i.e, storage). Through producing a logical design of resources, instead of a hardware design, virtualization remarkably develops the performance, promotes system development, clarifies system administration and configuration, and decreases the price of work and operations.

In fact, virtualization is considered to be one of the significant enabling technologies at the back of modern progress of IT, comprehensive some techniques cloud services [102], edge computing [103], and NFV [104].

Recently, the great growth of crypto-currencies DLTs such as blockchain has raised significant attention. A virtualized distributed ledger technology is an operative block inside the network base which includes clear external interfaces and a clear functional role. Consequently, a virtualize DLT as a function implies the execution of NFVs which are used in VM.

Significant network issues are faced considering the shift from the actual infrastructure to NFV-based solutions. The departure of functionality from the location additionally generates the issue of efficiently putting the virtual appliances, so as to dynamically create an instance on request. Another aspect to point out is the time needed to discover and overcome failures in the database of blockchain. As part of the future works, it is suggested that the process will involve the execution of multiple DLTs in the main ledger and in the cloud.

2.4 Metrics for Evaluation

In this section, the performance of the proposed system will be evaluated using a range of evaluation measurements**.**

2.4.1 Transactions Per Second

The amount of transactions that a system can process in one second is measured in transactions per second. This term is used to measure the performance of every system that serves data transactions on a regular basis. TPS is a measurement used by payment processors and networks, such as decentralized applications**.**

Though distributed ledger have several applications, it is most commonly associated with peer-to-peer transactions. An effective payment processor must be quick and effective. As a result, when it comes to payment processors, the statistic of "transactions per second" is important.

The formula for calculating TPS is [105]:

$$TPS = T \div S \qquad (2.1)$$

Where T = Transactions , S = time in seconds

Or

$$Th=t * count\ (Rs) \qquad (2.2)$$

Where t= time in seconds, *Rs*=number of transaction

2.4.2 Consensus mechanisms

Consensus mechanisms, often known as consensus algorithms, enable dispersed systems to collaborate while remaining secure.

Many people confuse consensus protocols and consensus algorithms. Protocols and algorithms, on the other hand, are distinct. A protocol is a set of specific instances in a regulation that controls the operation and interaction of a system and its various components. Algorithms are like process instructions for solving a problem or calculating a result.

These approaches have been used to achieve consensus among database nodes, application servers, and other enterprise infrastructure components for decades. New consensus techniques have been developed in recent years to allow cryptoeconomic systems like Ethereum to agree on the cases of the network. There are some types of Consensus protocol:

1- **Proof-of-Work (PoW):** which we used in our work, nodes vie versus together to validate the following transaction block and acquire a reward. Also is the mechanism that permits the decentralized Block chain technology to reach agreement on issues like as account and transaction order Figure (2.7). This prohibits users from "double spending" their currencies and makes the Block chain technology extremely hard to attack or corrupt.

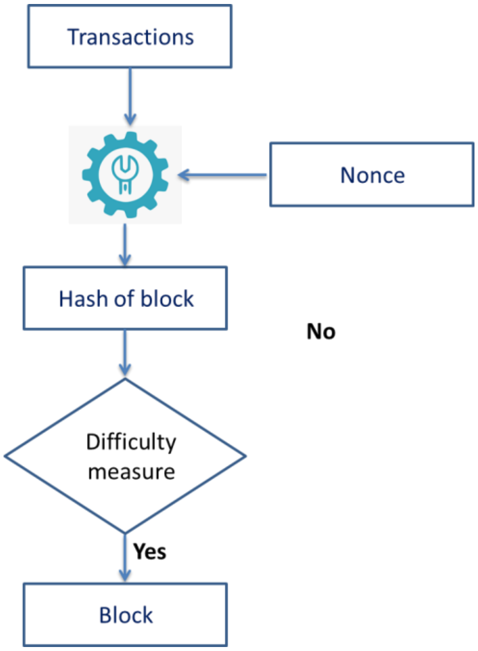


Figure 2.7: Proof-of-work flowchart

2- **Proof-of-Stake (PoS):** is a consensus process in which new blocks are validated by those who hold the most of the blockchain networks Figure(2.8). This allows for speedier and less expensive transactions. For continuing engagement, it compensates those with the most invested in the network [106].

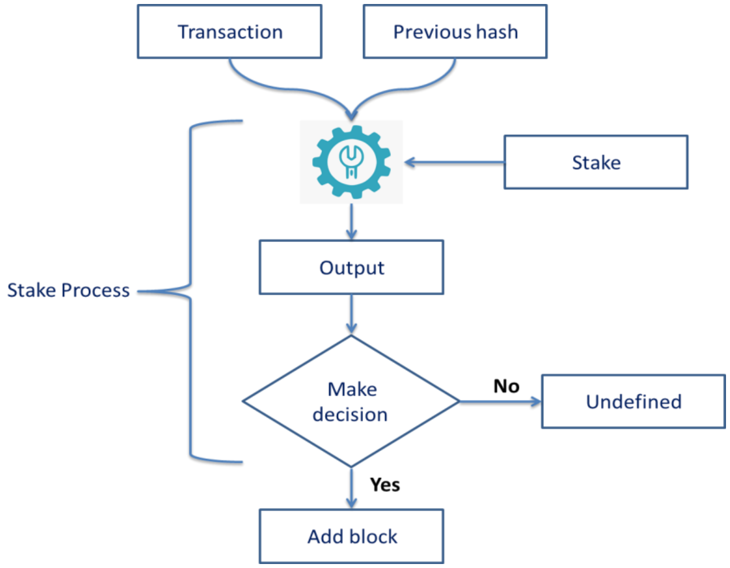


Figure 2.8: Proof-of-Stake flowchart

3- **Proof-of-Authority (PoA):** Although proof-of-authority is not widely utilized, it does have a distinct form. It is mostly utilized by private enterprises or institutions that use blocks generated via verified sources with unique network access credentials Figure (2.9). In contrast to other procedures, assurances are based on reputation and authority rather than public consensus.

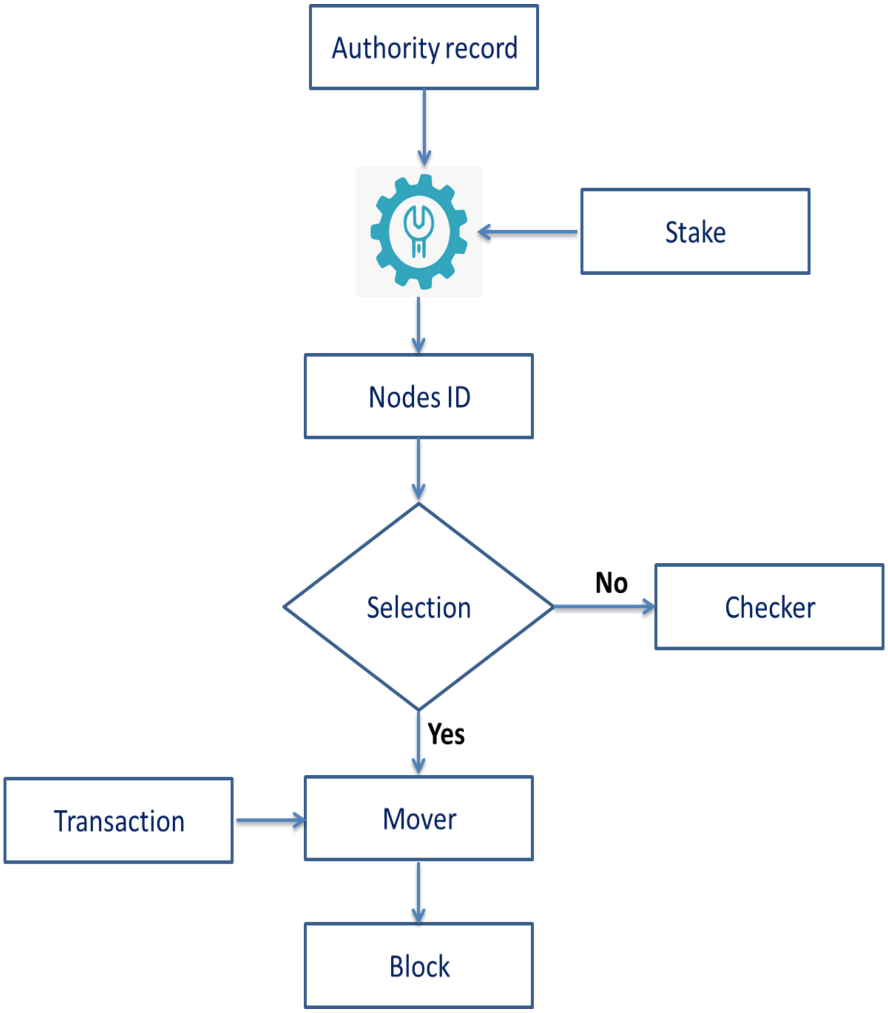


Figure 2.9: Proof-of-Authority flowchart

2.4.3 Transaction size

A transaction's size is equivalent to the quantity of data it retains. A transaction, as any other container, could only store much more information. The transaction size limit refers to the volume of data that a blockchain transaction can compute based on [107], when both input and output grow, the overall size grows as well.

Besides contemporary centralized data standards, blockchain size restrictions are minimal, however crypto transactions are extremely light in terms of data storage. The block size restriction for Bitcoin is 1 MB, although this modest volume of data can hold approximately 2000 transactions.

2.4.4 Throughput

The number of initiatives executed in a particular amount of time is referred to as throughput. Transaction throughput is a term used in the blockchain world to describe how quickly a blockchain processes transactions. It is generally stated in transactions per second (TPS), and it can be defined in minutes (TPM) as well as hours (TPH).

2.4.5 Latency

The time duration between an input and the delivered output is referred to as latency in computing. It's present at every phase of computation, from user-to-computer IO delay to network latency when data and sent content flow out of a computer to servers across the internet. Latency also distinguishes two temporal delays in cryptocurrency. One of those is delay in a blockchain network, while the other is latency around an exchange.

The period between sending a transaction to a blockchain network and the network's initial verification of approval is known as network latency. The transaction gets further definitive after the first verification as more blocks are added beyond the original verification.

2.4.6 Scalability

The capacity of blockchain technologies to sustain increased transaction loads and the number of nodes in the network is known as scalability. Scalability refers to a computer system's capacity to manage an expanding amount of work (e.g., a database or search engine). A blockchain network which has a huge volumes of information somehow doesn't scale well or has limited scalability. Blockchain doesn't quite take substantial steps to adapt the system to meet growing needs for data, resources, and data.

CHAPTER THREE

VIRTUAL FUNCTIONS BLOCKCHAIN BASED ON NETWORK FUNCTION VIRTUALIZATION

3.1 Overview

In this chapter, a modern technique is structured for virtualizing the functions of the blockchain that are merged with NFV in addition to the automatic manner of execution of smart contracts among virtual nodes, and this work is executed within cloud Amazon web service (AWS) in two approaches, the first based on the cloud services to use it as NFV architecture, the second we use the cloud as a container for our system. Through integrating the two techniques NFV and blockchain, all blockchain challenges are the procedures of transition, agent compatibility, network management, fast expansion, and security, have been overwhelmed via designed software environments via constructing virtual function blockchain, in addition to that, easy interaction within the blockchain system and handling the transactions among nodes with the clients, indicating ideal network management.

3.2 Virtual Blockchain Environment

With this, we show that the proposed environment that was built consists of a complete network of Blockchain with its components (nodes, smart contract, peer network, ledger). Also, the NFV was built that a general concept that includes a set of functions and services and there is no strict specific standard to describe it. And adapting it to work within the blockchain environment, after building the network, we introduced this tool to the node functions hash, ledger ,and key distribution to get a virtual blockchain environment.

The framework of our proposed system is briefed in many steps and two phases: The first phase include the below steps Figure (3.1).

Step 1: The private blockchain is built according to the specified environment starting from identifying a suitable use-case to a final decision.

Step 2: The blockchain is linked to the cloud for applying the NFV services.

Step 3: The new contribution made in this work, namely the virtualization of the hashing blocks and leger (data base of blockchain) via NFV based on cloud services.

Step 4: Used the private blockchain to transfer Files as case study.

Step 5: The last step includes applying the proposed system to healthcare.

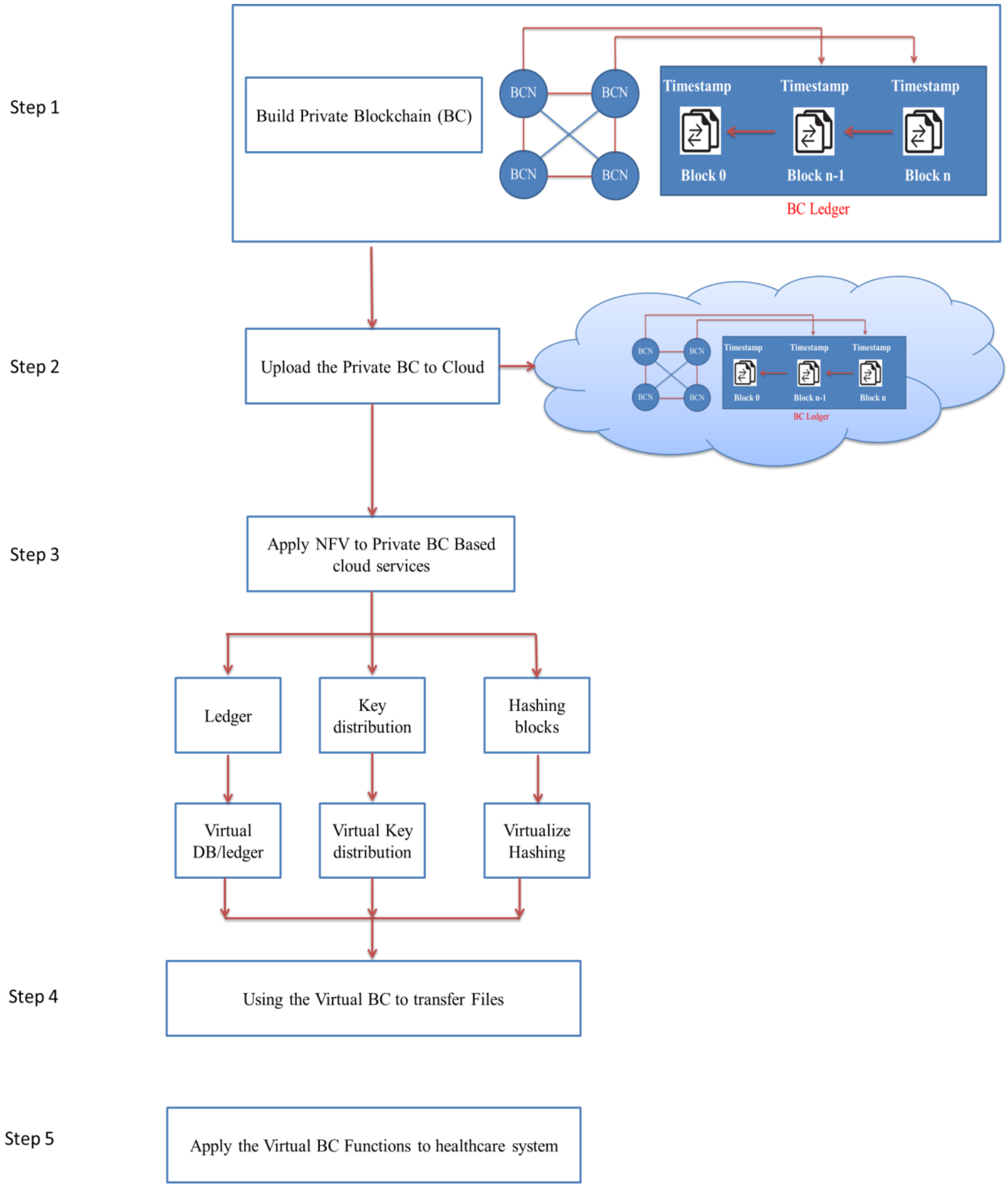


Figure 3.1: First phase of proposed system.

The second phase will explain in the section (3.7)

3.2.1 Build Private blockchain

Initially we created the public framework as User Interface (UI) to instantiate the blockchain and to instantiate the nodes. In this part, we are proceeding to describe how can construct a private blockchain utilizing the python programming language.

Following is the state of creating a private blockchain for a particular party. The main provision in transferring data to happen in the environment for transmitters and receptors who shall obtain multi-chain platforms placed inside it. Considering that private blockchains are created at first via three nodes. Figures (3.2) shows the ingredients of the blockchain architecture, as posted in the following points.

a) Nodes: Any devices used blockchain

b) Transactions: Creating the blocks of a blockchain.

c) Block: The data construction appropriated for preserving a group of transactions spread to all nodes within the created networks

d) File Chain: A series of blocks in a particular arrangement.

e) Consensus: A collection of principles for performing the blockchain operation.

f) Smart contract: Unique smartly established contract to communicate with data.

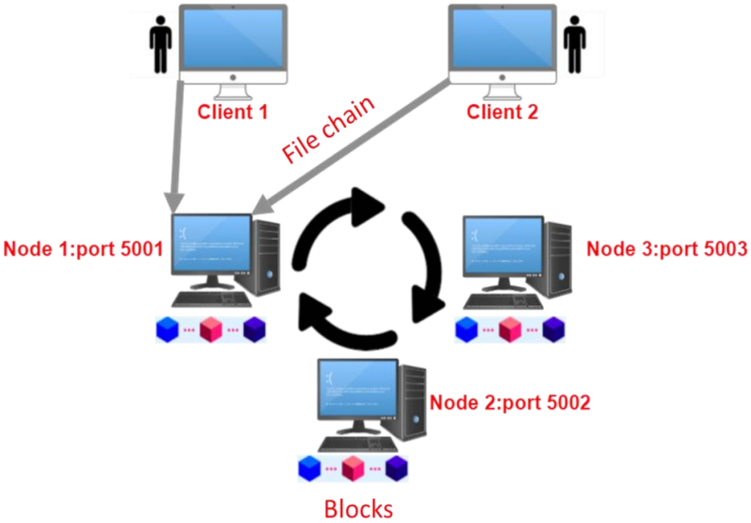


Figure 3.2: Part of our private blockchain system for three nodes.

Below Algorithm (3.1) indicated is the essential initial schema of the Python class generously employed for constructing the blockchain:

Algorithm 3.1: Class Blockchain:

```
Input: set of transaction
Output: genesis block
Step 1: define instances in a class
Step 2: define array of transactions
Step 3: define array of blocks
Step 4: add empty set for nodes
Step 5: add random and unique id for each node
Step 6: create genesis block
Step 7:end
```

Also, the worked on creating the chain by adding a block of transactions to the blockchain containing (timestamp, transaction, nonce, and previous hash) as shown in Algorithm (3.2).

Algorithm 3.2: The Creation of the Chain of Blockchain:

```
Input: transaction (images, number or pdf file)
Output:(block, block number, timestamp)
Step 1: define method for create block
Step 2: add a block of transactions to the blockchain
Step 3: create dictionary of blocks
Step 4: add block number
Step 5: add timestamp of each transaction
```

Step 6: *add nonce of the transactions*

Step 7: *call pervious hash*

Step 8:*end*

Also, created a very important and reliable part in the process of sending transactions, which is the wallet (address) algorithm (3.3), which contains the private and public master keys that represent the address of the sender and recipient. RSA creates a comprehensive service of arithmetic functions utilizing modulo-n arithmetic.

Algorithm 3.3: The Keys (address) Generation

Input*: set of transaction*

Output*:(sender public key, recipient public key, block ,block number, timestamp)*

Step 1: *define new method of wallet*

Step 2: *import pychrptodome*

Step 3: *import RSA or ECC*

Step 4: *chose size of key based on RSA or ECC*

Step 5: *specification random generator*

Step 6: *generate private key*

Step 7: *based on private key, generate public key*

Step 8: *response (private key ,public key)*

Step 9:*end*

The Assumptions that used for calculate the key generation with timing:

Block Size (KB): The following block sizes are considered to be the actual block sizes to be utilized for RSA. Both ECC and RSA use the identical block sizes, which are determined by the key size.

The characteristics: Below feature used for simulation to compare the performance characteristics of the RSA and ECC encryption algorithms is **time for key generation (ms)**, **time to encrypt (ms)** and **time to decrypt (ms).**

Key size (bits).

Table 3.1: Shows the ECC and RSA comparative key sizes with identical levels of security[108].

Key size (RSA) (bit)	Key size (ECC) (bit)
160	1024
224	2048
256	3072
384	7680
521	15360

Because of the timing disparity in each of above three parameters, simulation ran repeated tests for each parameter for roughly 20 times to obtain the parameters' average timings.

Clients can exchange data in a transaction then sign of this transaction based on their private key in addition to share the public key. The validated of that signature may with the public key via anybody on the network in order to confirm the tight of this transaction.

The building of transactions addresses based on created a data address based on the public key (K) via utilizing the hash function. Also, used the Secure Hash Algorithm (SHA), particularly SHA256. Would execute in the following steps:

Step 1: Initiating with the public key K.

Step 2: Calculate the SHA256 hash

Step 3: Repeat the SHA256 hash of the output of step 2.

Step 4: encoding the result with Base58Check.

Step 5: Constructing a 160-bit number as address.

Also, in proposed system utilized the SHA-256 algorithm as below algorithm (3.4) in the private blockchain to hashes of the data. The moment that the data is positioned within the hashing system, the algorithm gets back a 256-bit string indicating the content of transactions. Therefore, immutability will give to the blockchain through that.

Ever after every block will be expressed via a hash, which choice be calculated based on the hash of the prior block, deteriorating each block in the chain will cause the further blocks to have invalid hashes, consequently causing damage to the complete blockchain network.

To compare the time it takes for hash algorithms to execute, two alternative loops are used. Three key scenarios are considered for the two loops: a short series of data to be hashed, Middle and a large series of data to be hashed, with comparisons made among SHA-1, SHA-256, and SHA-512.

Algorithm 3.4: The SHA-256 Signature

```
Input: set of transaction
Output: hashed data (number ,letters, image or pdf file)
Step 1: add new methods with parameters (like signature and sender public key)
Step 2: import binascii( for extract sender public key)
Step 3: verifier signature
Step 4: Import SHA (SHA-1, SHA-256, or SHA-512)
Step 5: hashing the transaction with SHA
Step 6: verify (hash, signature)
Step 7: signature (valid or not valid)
Step 8: end
```

The operation of the hashing is based on the private key to constructing the signature, whereas not needed to confirm it. Anybody can confirm the validation of the signature depending on the public key, signature, and data. Figure (3.3) refers to the private blockchain digital signature procedure, which is performed in many steps:

The First client procedure;

Step 1: The first client signs his /her transaction via creating a hash value emanated based on the transaction.

Step 2: In the next step encrypts mentioned hash value via utilizing his / her private key then transmits to the second client the encrypted hash in addition to data.

The second client procedure;

Step 1: The second client confirms the received transaction.

Step 2: The confirmation is done by comparison (decrypted hash with hash value) that emanated from the receiving operation.

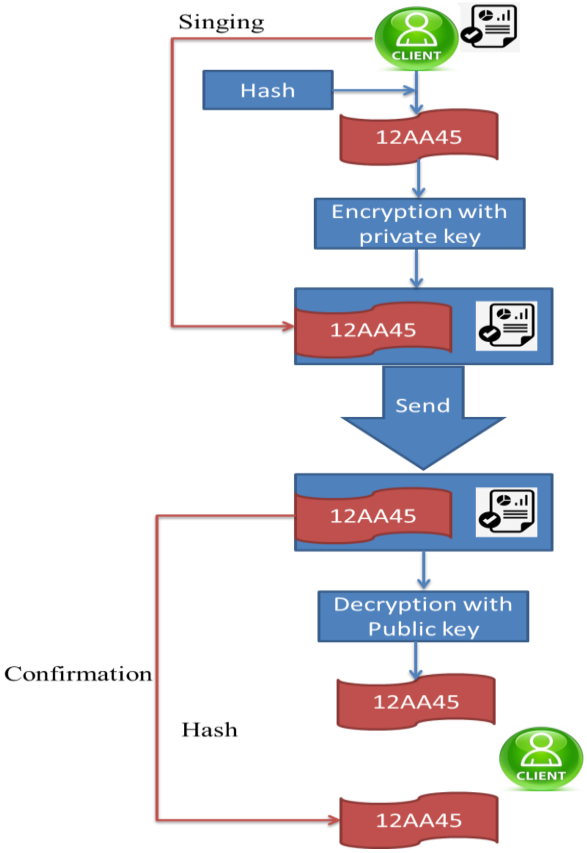


Figure 3.3: Private blockchain signature procedure.

In a blockchain system, Proof of Work (PoW) indicates the complicatedness concerned with confirm or forging novel blocks on the blockchain.

The PoW can be executed via specifying a number that fixes trouble when a user achieves several computing works. Users of the blockchain environment should discover the number complex to recognize while effortless to confirm, below the major idea of PoW. The goal is to obtain a hash containing a set of zeros through which the complexity of the network currently required is determined, It also aims to find *nonce* that meet a certain criteria. The validity of the hash is determined based on (DIFFICULTY nonce) this means the number of zeros at the beginning of the string, the DIFFICULTY contains a fixed value determined by us and it is changeable (for example “0000”), if the number of zeros in the difficulty is the same as the specified number, this means the validity of the proof see Algorithm (3.5).

Algorithm 3.5: **The Proof of Work**

```
Input: transaction , keys addresses

Output: valid transactions

Step 1: build new method for validation proof

Step 2: Call (transactions, hash of the last block, nonce, difficulty)

Step 3: g=merge (transactions, hash of the last block, nonce) in one string

Step 4: hashing (g) for proving the validity proof

Step 5: call DIFFICULTY

Step 6: if hashing (g) = DIFFICULTY=0000, it valid proof

Step 7: build new method for proof of work

Step 8: hash the last block in the chain

Step 9: set nonce to zero

Step 10: while (g) is false: increment the nonce by 1until meet to criteria

Step 11: Return nonce
Step 12: end
```

The most important case in the work of the blockchain is the validity of the chain Algorithm (3.6). Originally, we need to know why we check to test the validity of the chain because the process of simulating and addressing between nodes, which each node contains its local block chain, for example, the difference in the length of blocks between the nodes, this needs to update the blockchain at the node which contains the least blocks, the chain that arrives from one of the nodes must be really valid, and if it is longer than the chain inside it, it must update its local blockchain.

Algorithm 3.6: The Validation of Chain

```
Input: transaction , keys addresses
Output: valid transactions
Step 1: build new method for validation chain
Step 2: Declaring variables (last block, current index=1)
Step 3: while current index <length (chain)
Step 4: select the second block
Step 5: check the validation hash of the current block based on previous hash
Step 6: if previous hash =hash (last block), then valid hash
Step 7: prepare transaction
Step 8: test the validation of nonce
Step 10: Return logical result
Step 11: end
```

As mentioned above, every node has a local blockchain, and it is possible for a conflict to occur between one node and another algorithm (3.7), so we must work out a consensus mechanism. Each node must have a list of nodes that are around it and take the blockchain that is in them, meaning that each node communicates with the neighboring node to tell it that it has a blockchain.

Algorithm 3.7: **The Resolve Conflicts**

```
Input: file chain
Output: success response
Step 1: build new method for resolve conflicts
Step 2: add list of nodes
Step 3: declaring for new chain variable, new chain =none
Step 4: compute length of chain
Step 5: for nodes in neighbors
Step 6: if length > max_length and valid chain
Step 7: max_length=length
Step 8: new chain=chain
Step 10: Return logical result
Step 11: end
```

3.2.2 Auto Smart Contracts

Smart contracts can be defined as a technological means of building blockchain, whereby you can create automated legal contracts held in the blockchain. Below steps illustrates the smart contract works:

- **Established contract**: in this step, nodes come to a consensus. Depending on the specified conditions.
- **Conditions:** A step that initiates the smart contract.
- **Confirm:** In this step, the scenarios of the contract judge if the condition meets the events established in the smart contract.
- **Running:** In this step, the scenarios of the contract perform their procedures that consider as functions.
- **Finishes:** A smart contract is completed

Technological changes and digital characteristics in the lawful domain have thrown a shadow over different dealings, particularly current contracting approaches like a Smart Contract. The mentioned is an information program which aims to execute the agreement in a computerized form no wanting the interference or intercession of others. This form of implementations strategies functions as computerized machines all mean adopting additionally developed technological means, see Figure (3.4).

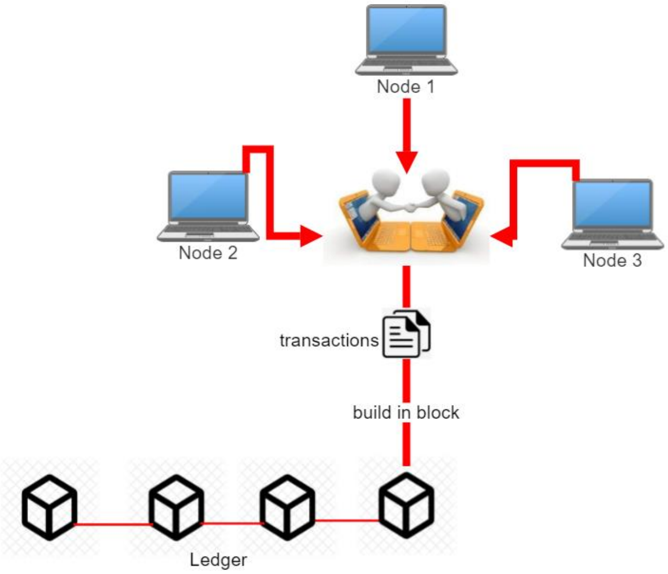


Figure 3.4: Exhibits the function of smart contracts in blockchain system.

Smart contracts could be defined as a technological means used in creating blockchains, and it is considered the main player in the work of this environment, via which a computerized lawful agreement could be constructed as it is kept on the blockchain. Via the current profession, whereby smart contracts represent the principal aspects, found synchronically with nodes with autonomous smart contracts acquired in virtual. This indicates that they exist in the existence of the virtual blockchain. The automated smart contracts in Algorithm (3.8) include the smart contract components like nodes and clients, moreover to the issue of the agreement, and considerable significantly the agreement terns which are programmed and positioned based on the criteria which are determined by both parties.

Algorithm 3.8: Smart contract algorithm for file transferring

```
Function contract
  Input: sender public key,
         Sender private key,
         Recipient public key,
         File
  Output: file, Recipient Address, Sender Address, File, Timestamp, Block
if (details of block exists and Nodes is exists) then
    if (Nodes is registered in the nodes list) then
        return Transaction is done
    else
        return Transaction Not Found
end
End function
```

3.3 Upload Private blockchain to AWS

The built system uploaded to the system to S3 after creating a Bucket storage wallet. We store different types of files in the storage wallet such as text files, images. Whenever a file id uploaded to amazon S3, the option is provided to include meta data along with the files and assign permission for controlling the access to these files. That is done through preparing an Amazon S3 bucket, constructing inside Amazon S3 a storage container or can creating a bucket -or utilizing an existing bucket. Also, we can upload the modification to the bucket, and Amazon EC2 instances utilized in deployments may have the ability to download the modification from the bucket. We utilize the Amazon S3 console to construct a bucket of an Amazon S3.

Initially and before the Blockchain is uploaded to AWS. Several axioms are created. To begin with, an account is created and logged into. Many services which match the offered works are uploaded too; the most important of them is Elastic Compute Cloud (EC2). It can be described as a web service that presents protected, computing able to be changed scale amplitude in rang cloud. A novel virtual machine is initiated, and then the block chain system is modernized relying on the load balancers that could establish many processes and many ports to execute the program.

We upload the content of private blockchain to an Amazon S3 bucket in the following steps as shown in Figure (3.5).

Step 1: Create a private account in AWS.

Step 2: Sign in to the AWS Management Console.

Step 3: Create domain and subdomain in the cloud.

Step 4: Create a bucket in AWS S3.

Step 5: Select a Region.

Step 6: create a bucket folder.

Step 7: Upload index.

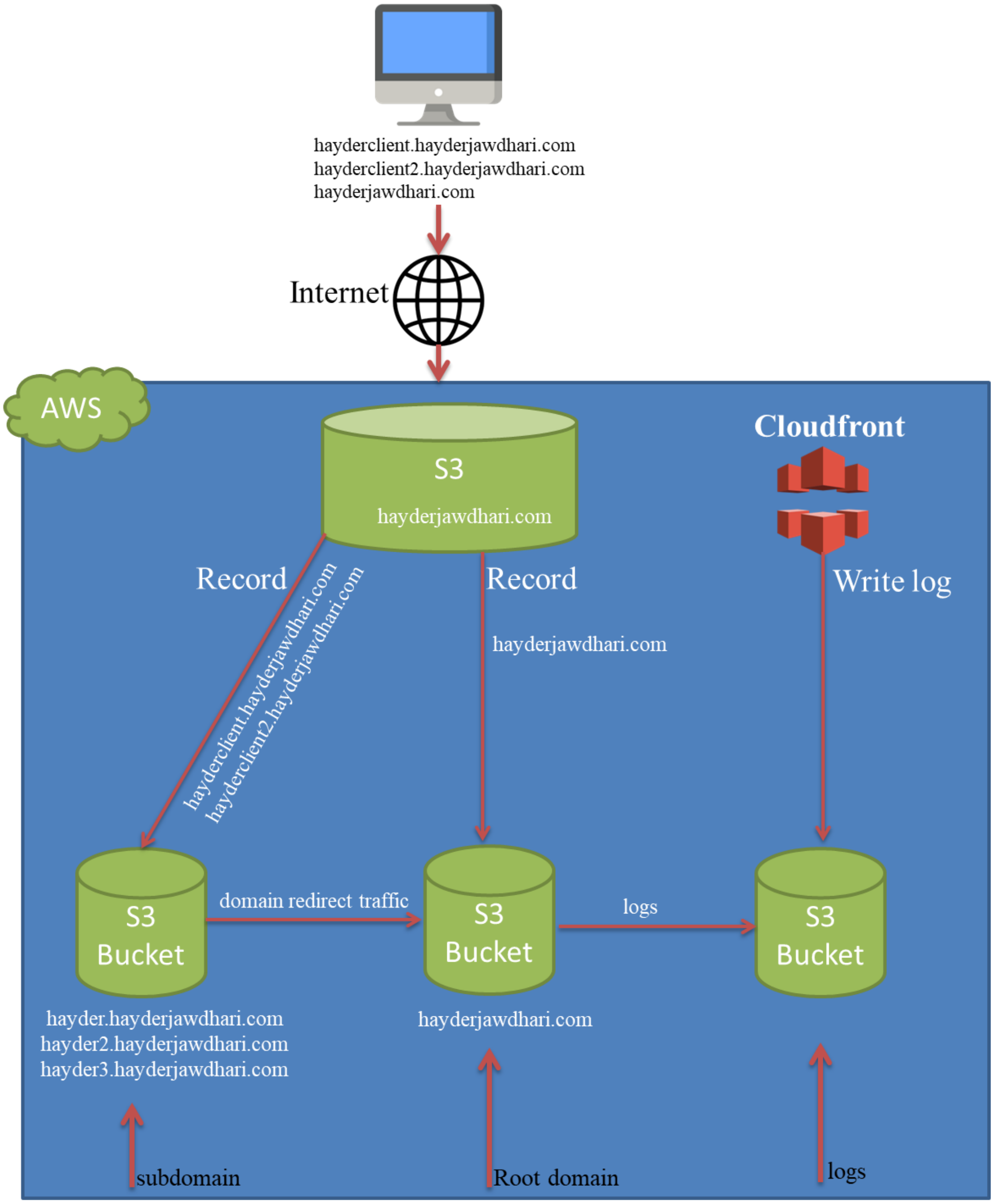

hayderclient.hayderjawdhari.com
hayderclient2.hayderjawdhari.com
hayderjawdhari.com
Internet
AWS
S3
hayderjawdhari.com
Cloudfront
Record
hayderclient.hayderjawdhari.com
hayderclient2.hayderjawdhari.com
Record
hayderjawdhari.com
Write log
S3 Bucket
domain redirect traffic
S3 Bucket
logs
S3 Bucket
hayder.hayderjawdhari.com
hayder2.hayderjawdhari.com
hayder3.hayderjawdhari.com
hayderjawdhari.com
subdomain
Root domain
logs

Figure 3.5: Steps of upload private blockchain to an Amazon S3.

3.4 Apply NFV to Private Blockchain

Relying on the EC2 and S3 that are included in Amazon, the NFVI layer is constructed, after which the virtualizing strategy will operate as VMs and container for storing or computing infrastructure. According to some procedures the NFV is installed on AWS.

After uploading the private blockchain, we used the cloud services available in AWS and used it as NFV inside the nodes in the blockchain, thus got a virtual encryption as well as a virtual ledger, in addition to the key distribution , and this tool is applied to the functions. Then used NFV to get virtual nodes and thus this gives a clear address to get the virtual blockchain.

Finally, the outcome was acquired via using the NFV. A whole of virtual nodes and all functions in these nodes has been acquired including each of the transactions, address (keys), and hash functions. Ultimately, this leads to a virtual blockchain that has got commonality nodes containing a duplicate of private blockchain.

3.4.1 Virtual Hashing

The virtualizing software and program which enables the operation of different systems altogether on a particular computer — enables you to do exactly that. Utilizing virtualization software, you may have ability of operating different systems onto certain physical machines. That mean allow us of virtualizing hash functions in blockchains. It is shown that our work includes two sides of virtualization (hardware and software virtualizations). We will reduce the processes of the hashing in blocks of the blockchain, as we mentioned previously, each transaction input process needs to be processed and this requires time, effort and cost, by using NFV we will reduce what was mentioned. Considering the below structure Figure (3.6) is determined by consensus and validation methods, all transactions never process until the majority of nodes enable the suggested transactions. Insomuch as the transactions fail, they will be sent continuously unless consensus arrive which permit the transaction procedure to be finished. In case one is never reached, the transactions are truly defeated.

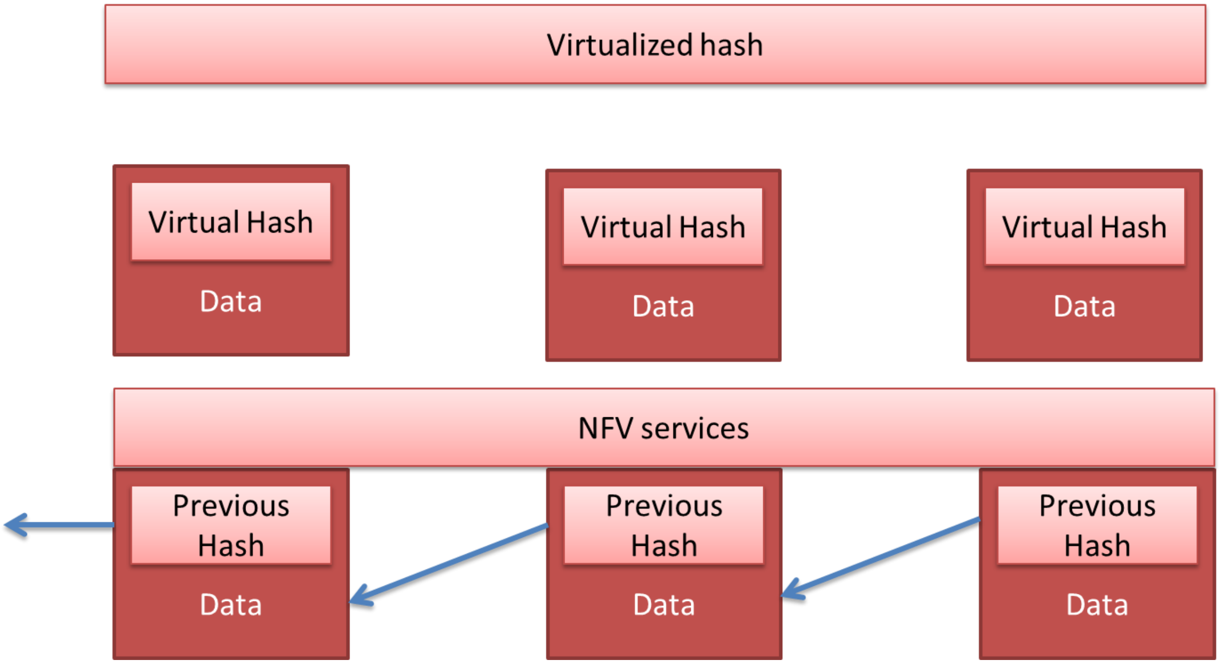


Figure 3.6: The proposed architecture virtual hashing.

3.4.2 Virtual Ledger

A similar procedure is adopted for the ledger. For creating virtual databases and disposing equipment we need in the storage process. Figure (3.7) illustrates the proposed architecture of the virtual ledger. As we showed there are many resources that were originally used as sources for the work of ledger storage, cryptography, consensus, and network resources. The abstraction of physical resources is accomplished by obtaining virtual resources. The virtual resources are attained utilizing a hypervisor. The storage will be depicted as a virtual ledger; however, virtual networks are consisting of virtual nodes. As will the virtual node is a software ingredient with hosting instruction.

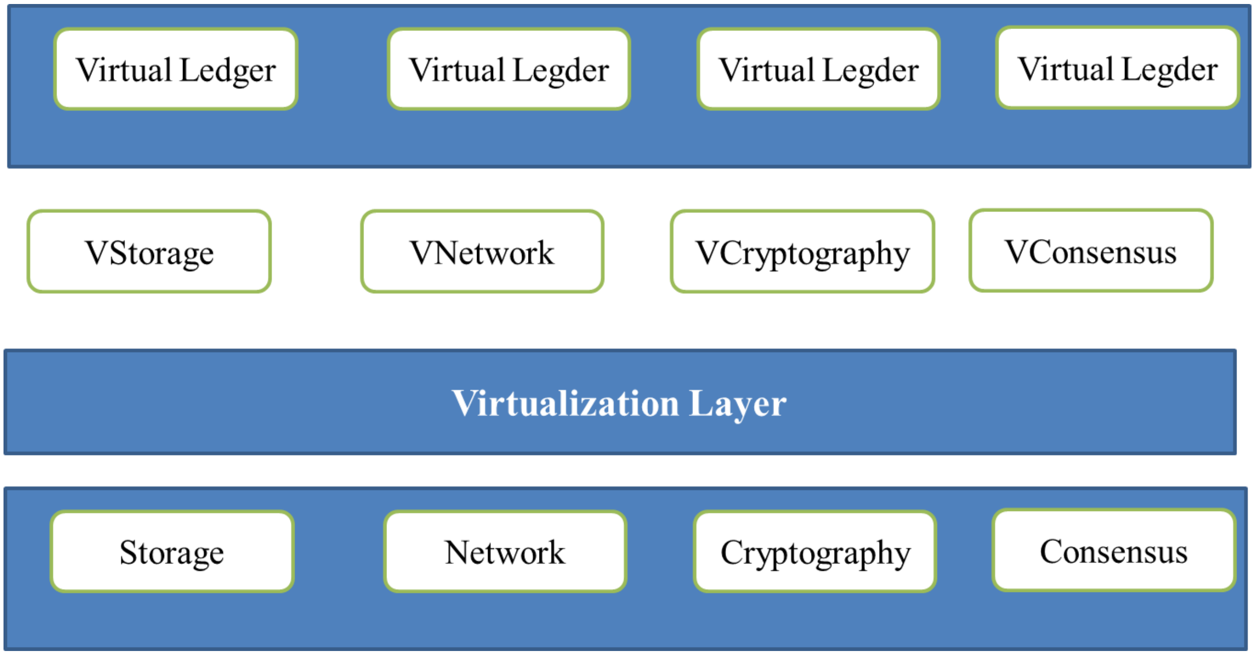


Figure 3.7: The proposed architecture virtual ledger.

3.4.3 Virtual Key Distribution

The private key provides the blockchain user property of the data on a presented address. Wallet of the blockchain automatically creates and keeps private keys for users. When transmitting from a wallet, the transaction will sign with the private key, which implies to the whole environment that the user has the control to transfer the data on the address the user transmitting from. We use the NFV in the key generator that is, we applied this tool to the first steps of the functions of the blockchain, which is the wallet that contains the addresses of the sender and receiver, i.e. the private and public key, which resulted in the process of creating keys by default that reduces the effort in generation if the environment is used to transfer many transactions as shown in Figure (3.8).

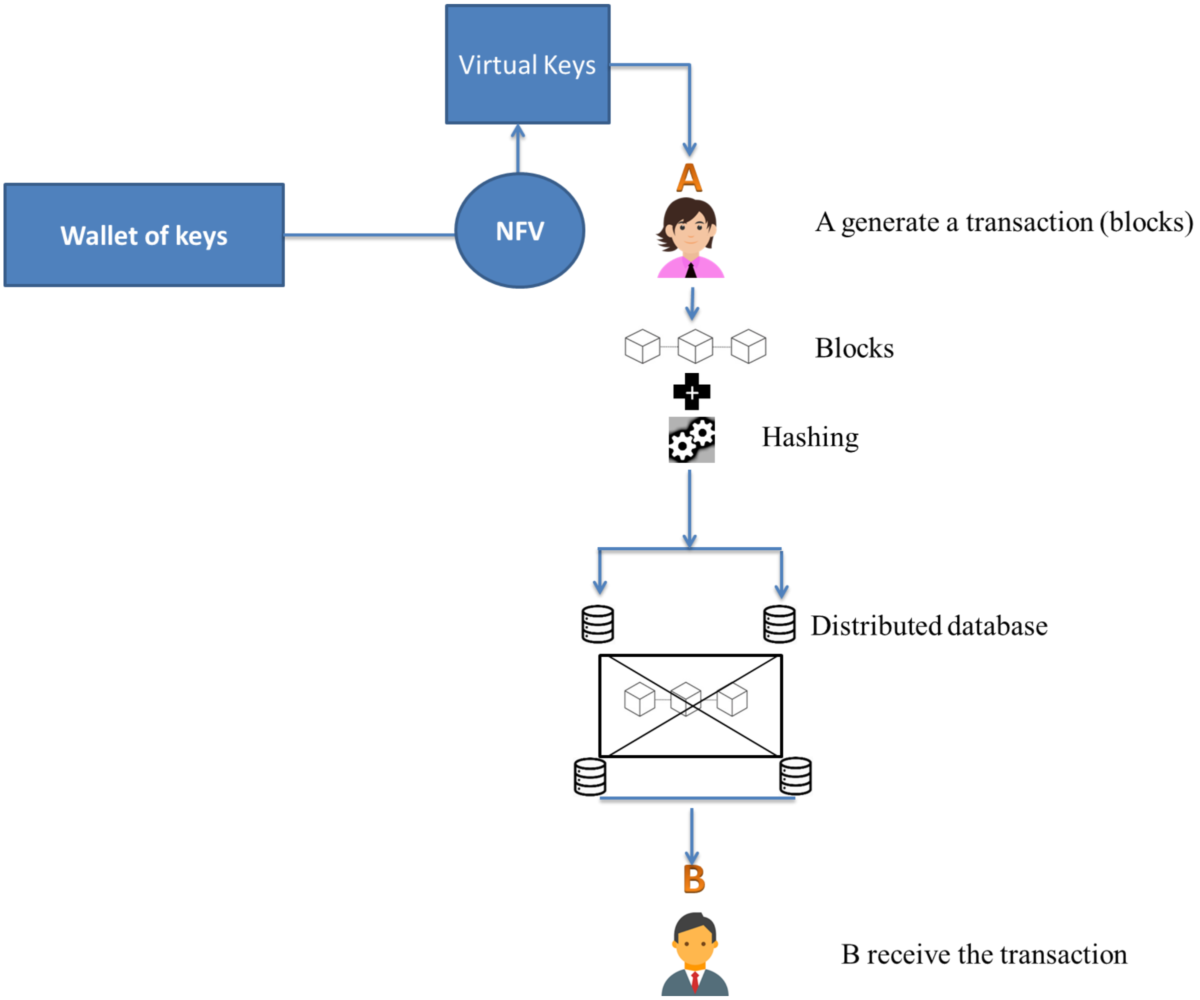


Figure 3.8: The proposed architecture virtual keys.

3.5 Virtual blockchain Environment for file transfer

Private blockchains are built for overcoming issues in security via the creation of secure file-sharing networks. Such a form of private blockchains is useful in a varying range of applications. The high level of security is reached via the use of a significant algorithm which considers cryptography to be crucial within the process, so as to ensure the robust encryption of files. This process makes sure that nobody besides the receiver can reach the files. In addition, the file transfer was performed at a high speed in comparison with Ethereum with FTP. A last smart contracts are created for fitting the file transferring process among nodes.

Also, proposed a new approach for file transferring. The dispatch operation in our blockchain is executed on duo kinds of data, the foremost applied to many types of symbols such as numbers and letters, and the second executed with the many types of files such as doc, PDF, and jpeg, that indicated in Figure (3.9). Sending procedure of the data that relies on the private and public key.

Before the process of digital signature known in the blockchain, which this system performs for every transaction sent through it, we encrypt the file twice for the first time, depending on the keys that the blockchain indicates for the purpose of encryption in an asymmetric way, Elliptic Curve Cryptography (ECC) is a type of public cryptographically secure that employs the statistical features of elliptic curves. ECC, as with all cryptographic keys, is based on mathematical functions that are simple to compute one way and yet hard to reverse. The futility of calculating the discrete logarithm of an element of a random elliptical curve is a source of problems in ECC.

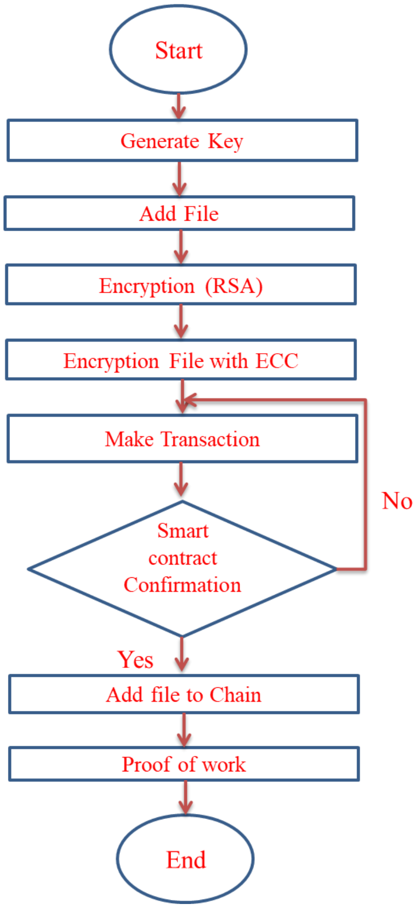


Figure 3.9: The Proposed blockchain for various data transfer.

3.6 Apply Virtual Blockchain in Healthcare

The health care system consists of various organizations, Individuals and procedures whose major responsibility is to manage, enhance, and maintain people's health, who should provide specific services, such like medical centres, pharmacy, hospitals, and insurance companies. Properly complete systems provide a high-quality service level and safety of the e-community while also improving illness treatment and budgeting, and this is achieved by taking into account several aspects:

Figure (3.10) illustrates the structure of the suggested healthcare system. We clarify the structure of the sub-system that performs as stated in the next steps.

Step 1: In suggested system, we give permission to the user to enter into the system via an interface of our private blockchain, then ask for the wished health record.

Step 2: The condition of the smart contract is initiated for privacy in addition to transparency. It will examine security and entrance control. When the user tries to access has permitted user records, at that point they are supplied with access to an exact health record.

Step 3: The smart contract verifies that the nodes have suitable privacy.

Step 4: The permission status is based on the access control policy for every user.

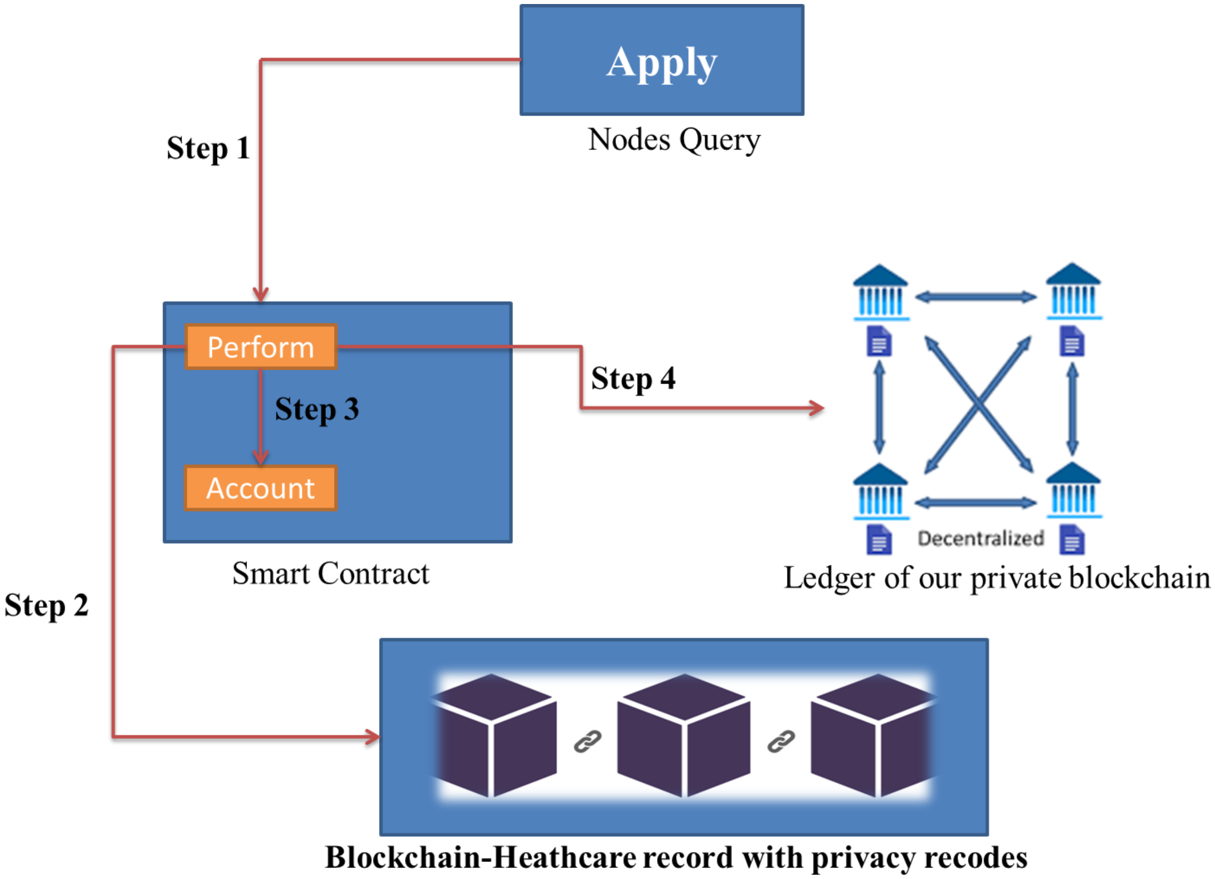


Figure 3.10: Healthcare subsystem.

The complete process is performs based on the following steps.

Step 1: The user should log into the private blockchain- healthcare then looks for their wished health record.

Step 2: For examinations privacy, the smart contract is started..

Step 3: The privacy is guaranteed by the suggested smart contract. Next, monitoring the access control permission, users are reported that they have the ability to see the report with the result.

Figure (3.11) illustrates the architecture of the virtual blockchain-healthcare; the main component of that system is a user interface, blockchain in two approaches (local and global). The topology of this system consists of many components (nodes, local blockchain, and root blockchain).

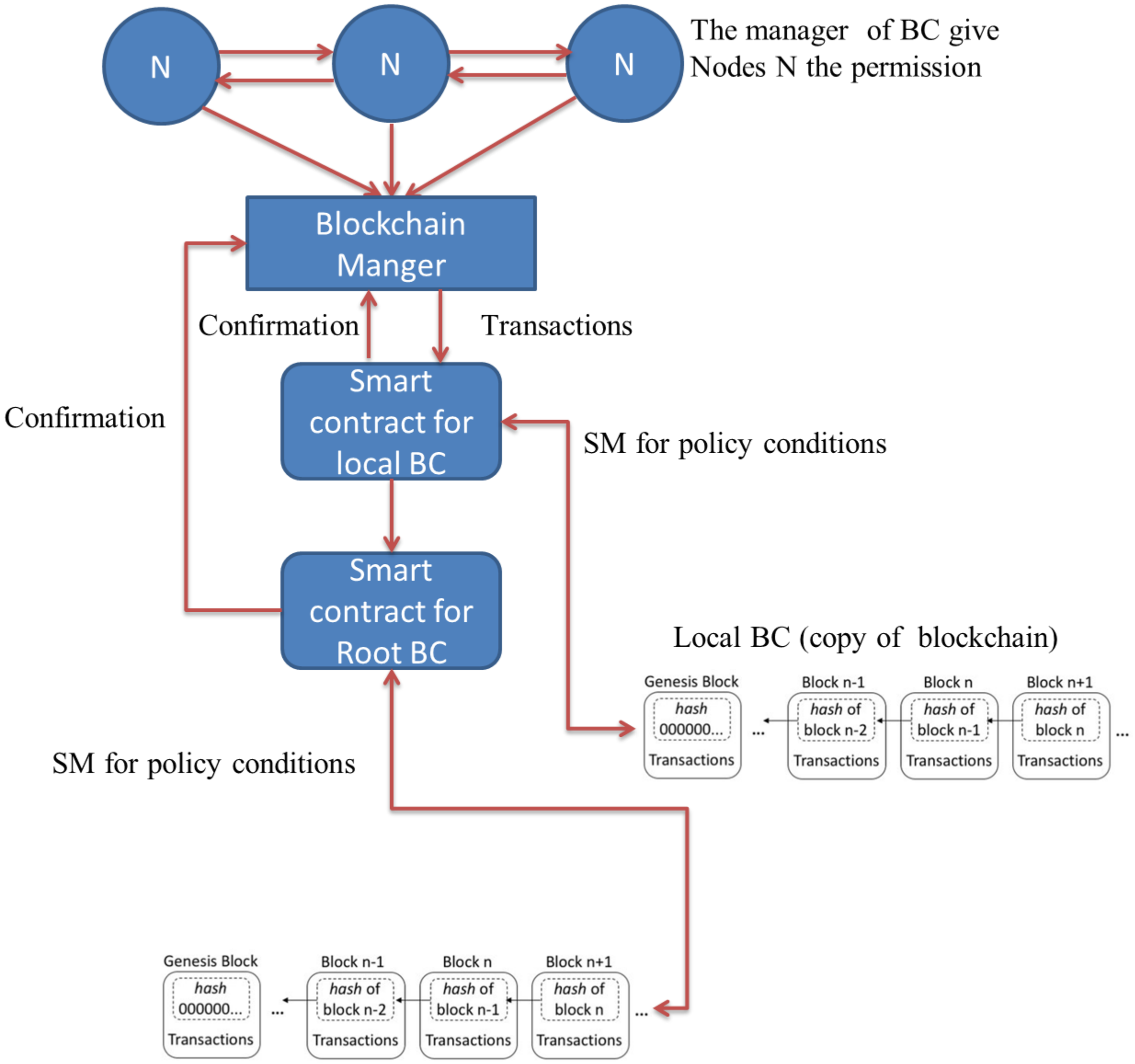


Figure 3.11: Architecture of virtual blockchain- healthcare system.

3.6.1 Confidentiality

Health care agencies will need to distribute necessary data to get a first response plan to diseases, enhance statistical data on a large scale, and optimize the healthcare quality in which electronic health systems use actual access to health patient records to give prompt assistance to individuals at the closest point of service. Like a result, health data distribution, editing, and evaluation are crucial for identifying and developing new treatments for emerging diseases. But, exchanging health data over several institutions poses a number of confidentiality problems, particularly in the absence of encryption. Individuals could be unwilling to share personal data with anyone else, which might stymie the implementation that connects every health practitioners. As a result, it is vital to ensure safe permissions and avoid monitoring of users' identities along with original data recognition. We took advantage of the strong privacy imposed by the blockchain in saving patient reports and preventing others from intruding on them, and we considered each node as one of the sections authorized to view the report, with the addition of another field showing the content of the report without opening it through the use of the two terms (negative and positive) Figure (3.12).

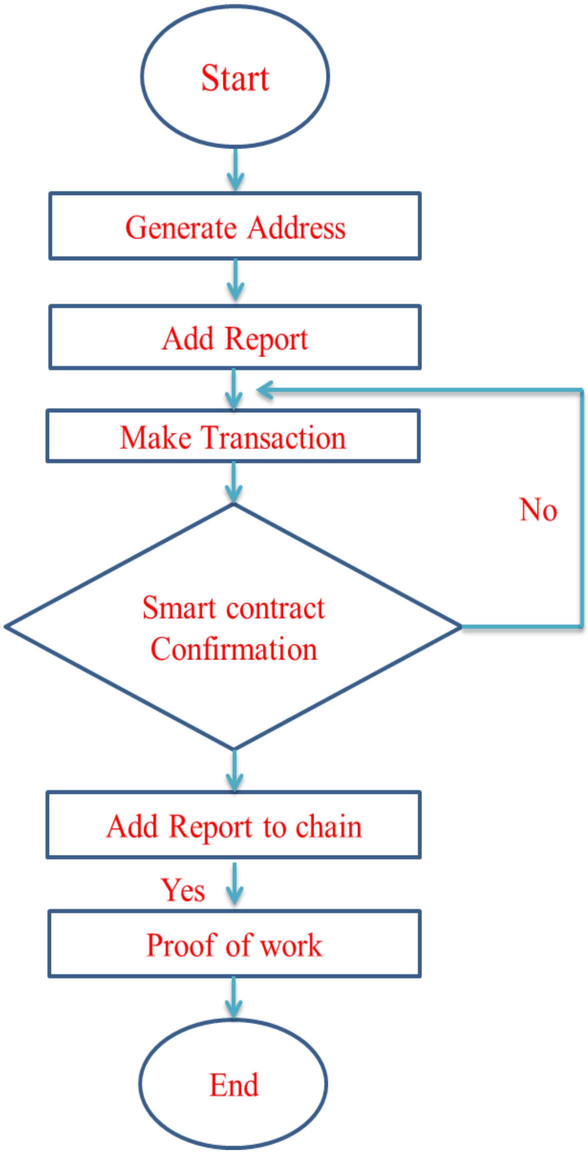


Figure 3.12: General health files transactions.

3.7 Virtual Blockchain Based on Programmed NFV

In proposed system, a new system is proposed to virtualize the blockchain functioning depending on the NFV. In conjunction with auto smart contracts among nodes that worked in a virtual manner within cloud computing. Over combining NFV with blockchain, all of the following issues in NFV are the manners of transformation, vendor adaptability, control of the network, speedy extension, furthermore security, has been succeeded through shifting to software environments by building virtual functions that work within the blockchain, as well as a high level of interaction smoothly way amongst them and handling the transaction among the node and client, showing perfect network administration.

The suggested architecture shows in Figure (3.13) that refers to virtual bl ock chain. The ingredients involve networking, computing, and storage. All resources contain an interior content, as they indicate the encrypting and consensus. The virtual resource decreases or pass out using physical devices. This idea is achieved through applying NFV as an abstraction layer above the hardware to be the virtual layer. Eventually separating virtual devices from central physical ones. The virtual machines in this approach are utilized as another choice to compute and store hardware and software. The description of blockchain is about nodes or functions that are performed within these nodes in order to get a virtual environment. An obvious service of virtual environment is to host or route, it gives sufficient evidence that its ingredients are software. Furthermore, the environment additionally is denoted via a virtual links, indicated to reasonable and relational links connecting the nodes. It is presented as an unambiguous hardware links followed by features that can undergo a dynamic change.

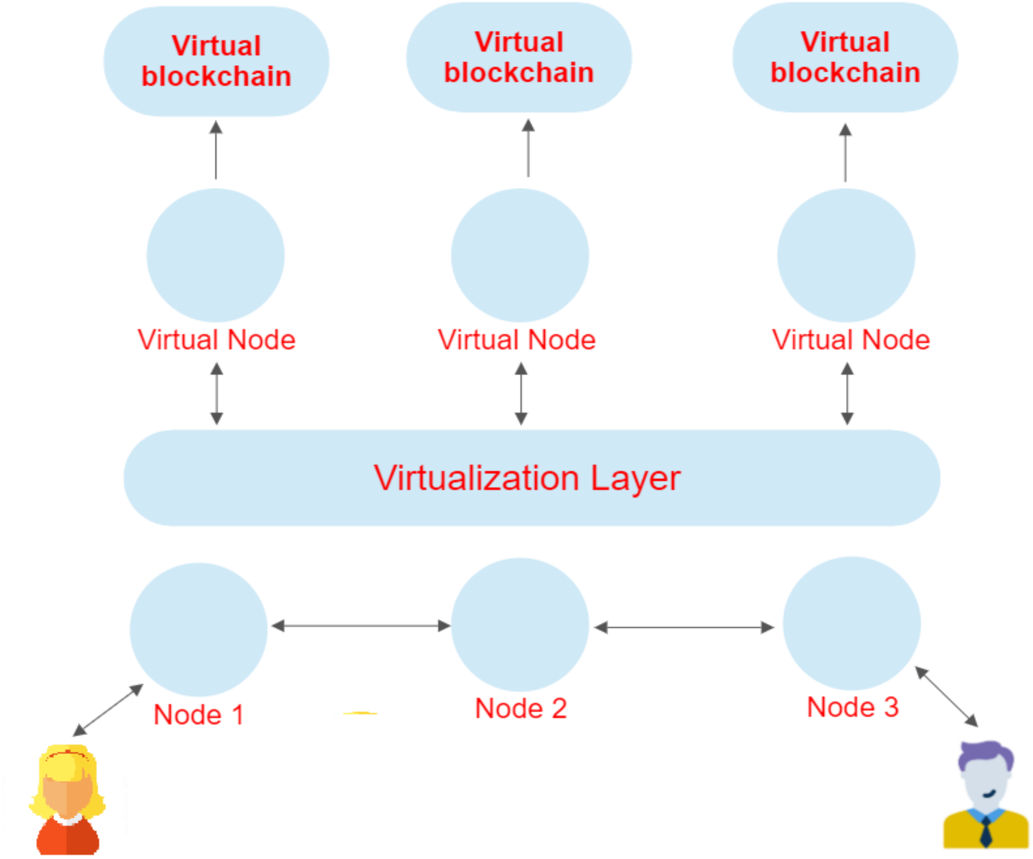


Figure 3.13: Proposed a new architecture of the blockchain.

This section is consider the **second phase** of proposed system which include the below steps as shown in the Figure (3.14):

Step 1: Use our private BC that built in the first phase. (Subsection 3.1)

Step 2: Build Network functions virtualization (**NFV**).

Step 3: Apply NFV to the private BC functions.

Step 4: Upload private BC to the cloud as a secure environment.

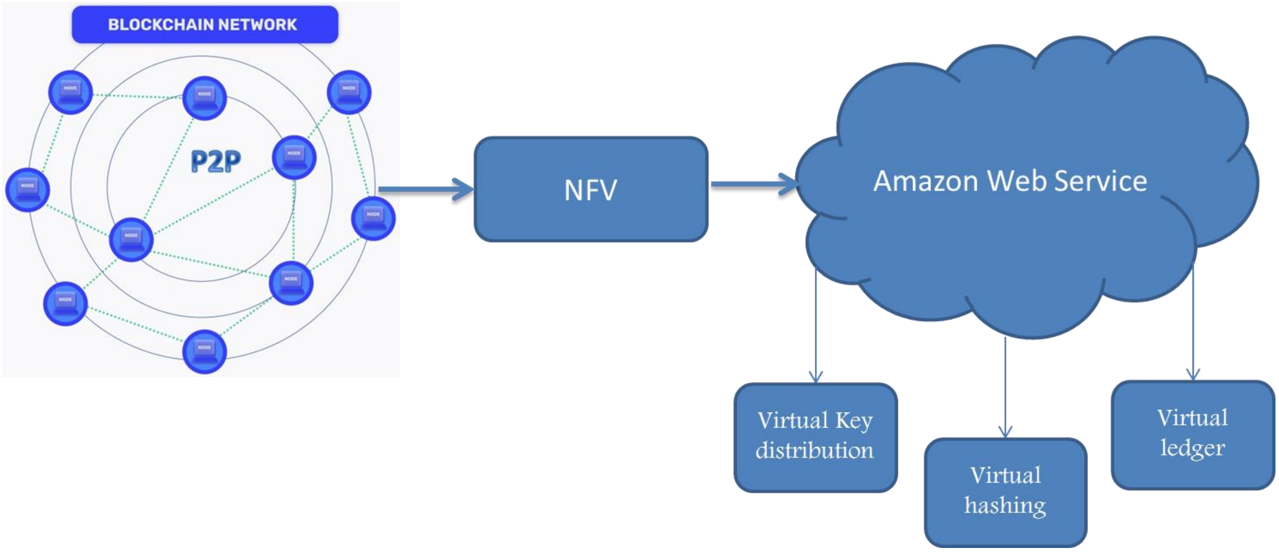


Figure 3.14: The second phase of proposed system.

3.7.1 Build private Blockchain

Here used same our private blockchain that explained in sub-section (3.1).

3.7.2 Built Network Function Virtualization

NFV was implemented in two phases; the first was using a ready-made tool based on AWS, that is, by adding this tool directly to the targeted functions by the node, which is encryption and the ledger. The second stage was to apply NFV programmatically and dive inside it and know its internal parts that work on these functions, which we started with the OpenStack TOSCA (Topology and Orchestration Specification for Cloud) Parser. It is constructed within YAML (Yet Another Markup Language) a profile of parse TOSCA. It is used to read the templates of the TOSCA in addition to constructing a graph included in-memory nodes of the TOSCA algorithm see algorithm (3.9).

***Algorithm 3.9:The* TOSCA Parser**

Input: *Functions address*

Output: *success operation*

```
Step 1: define method for TOSCA Parser
Step 2: Parses the yaml file identical to the TOSCA vnfd
Step 3: return parsed_file
Step 4: end
```

Then the configuration of the network is worked and call the functions to be virtualized by relying on the IP of each node see below Algorithm (3.10)

***Algorithm 3.10:* The Network Configuration**

```
Input: url network
Output: Virtual Functions
Step 1: define method for configure_network(net, vnfd)
Step 2: call the legder and hash functions
Step 3: return VNF
Step 5:end
```

So that can get the VNF Algorithm (3.11) we built a method that makes it easier for us to build the virtual network.

***Algorithm 3.11:* The VNF Building**

```
Input: url Nodes
Output: url virtual functions
Step 1: define method for vnfd_creation
Step 2: Creates vnfd from network."
Step3:if the path found, return output(vnfd_creation - hayder2.hayderjawdhari.com<hayder.hayderjawdhari.com><http://haydernfv1.hayderjawdhari.com)
Step 4: end
```

The following algorithm represents NFV in general Algorithm (3.12).

Algorithm 3.12: The Algorithm of NFV Nodes Recall

```
Input :nodes locations
Output: virtual nodes functions
Step 1 : Parse the yaml file
Step 2 : Create the mininet nodes
Step 3 : Configure the Blockchain
Step 4 : Configure the nodes
Step 5: Return the node of the blockchain if the blockchain exists (from Step 3).
Step 6 : Create vnfd
Step 7 : Orchestration of NFV function
Step 8 : Return NFV-blockchain, Virtual Nodes
Step 9: end
```

3.7.3 Apply NFV to the Private BC Functions

Here followed the same previous approach in sub-section (2.3) in the process of applying NFV to the functions of the blockchain by placing a layer of virtualization on the functions of the blockchain mentioned at the beginning of the chapter and we got the same results.

3.7.4 Upload Private BC to The AWS

After applying NFV to the system, we made a domain and a sub-domain of the blockchain and it was uploaded to the cloud (see subsection 3.3) to take advantage of its services to protect this environment as well as to obtain access control of the system completely to be used within the World Wide Web.

CHAPTER FOUR

EXPERIMENTAL RESULTS

4.1 Introduction

The results of implementations of the proposed system are shown in this chapter, which describes the outcomes of the proposed development for the blockchain system based on the NFV. The results of design of the Private blockchain is illustrated in Section (4.3) The proposed private blockchain implementation and evaluation and comparison are described in Sections (4.5, and 4.6), whereas the suggested blockchain-NFV in (4,8). The virtual implementation for secure healthcare files is presented in Section (4.10).

4.2 Simulation

A laptop computer is used to run the suggested system, which is written in Python. Computers and mobile phones were also used as nodes (smart contract). We used AWS as the incubator and virtual layer provider for our system as shown below:

1.Elastic Compute Cloud.

2.Elastic Load Balancing.

3.Route 53.

4.Simple Storage Service.

4.3 Results of Construction the Private Blockchain

Building a blockchain network depends on several things, starting with the keys, which are the transaction (data), the sending and receiving addresses, the number of nodes, smart nodes, and time stamp. This data has been transferred to a special system and user interface that can be handled smoothly. Figure (4.1) represents the main interface of the system.

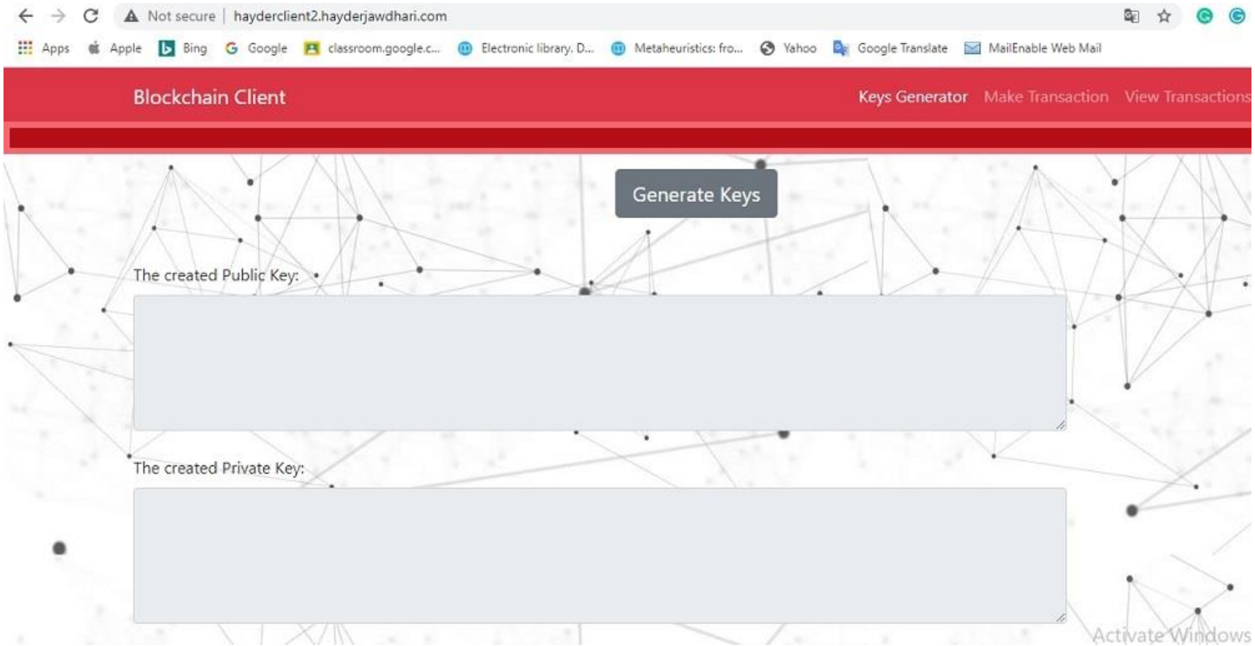


Figure 4.1: Main interface of the system.

4.3.1 Key Generation

A public key is used to encrypt all blockchain transactions. As well as the transactions decrypting through the private key, and the process generation of key with time of encryption and decryption that based the manner of [108] but in different results Tables (4.1, and 4.2).

Table 4.1: Key generation and time (ms) of encryption and decryption for RSA algorithm

Size of file (KB)	Size of key	Time of generation key	Time of encrypted	Time of decrypted	Encrypted file size
711	160	90	310	911	905
711	224	108	372	1105	810
711	256	205	512	1812	780

From the above table, we can see that the time increases with the length of the key, also the encryption time increases with decryption time. However, the file size is decreased when the length of the key is increased when using RSA

Table 4.2: Key generation and time of encryption and decryption for ECC algorithm

Size of file (KB)	Size of key (bit)	Time of generation key (ms)	Time of encrypted (ms)	Time of decrypted (ms)	Encrypted file size (KB)
711	512	25	101	45	711
711	1024	30	80	95	711
711	2048	41	98	112	711

From the above table, we can see that the time increases with the length of the key, but the encryption time varies with its increase and decrease. However, decryption depends on the length of the key, meaning that the decryption time grows with the get bigger in the length of the key with the stability of the file encrypted using ECC. Even though the key length is the same in both systems, key creation times vary, and it can sometimes take a very long time to generate the keys. Figure (4.2) illustrates that the key creation time is about identical in both situations for smaller key sizes, though as the key size increases, RSA consumes more time to produce the keys, but this time rises linearly with the key size.

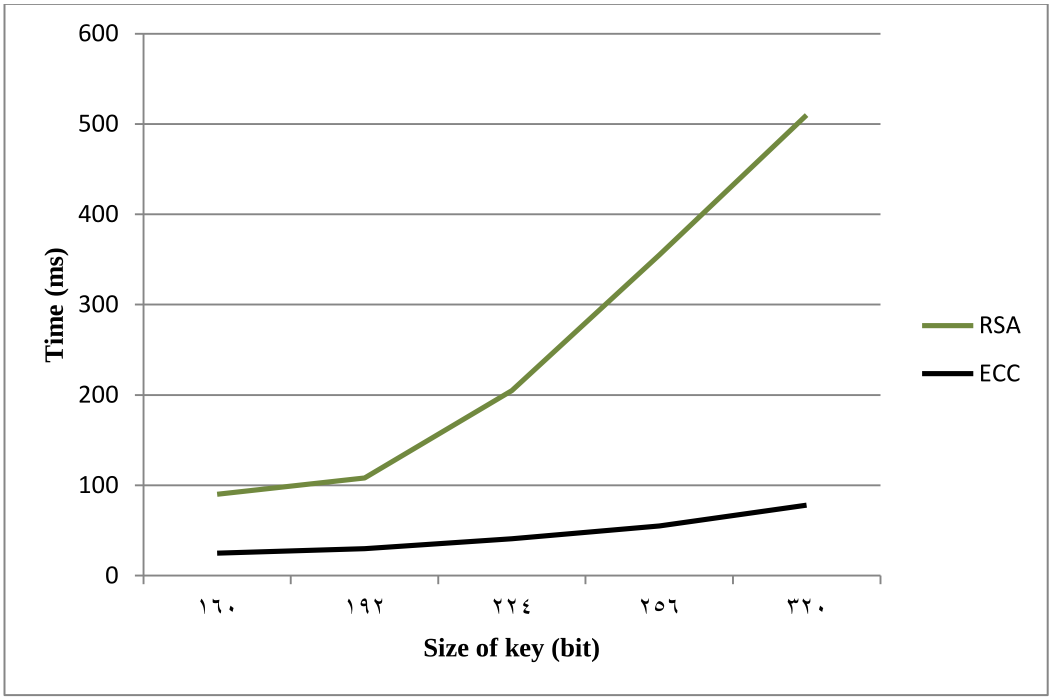


Figure 4.2: Key Generation Time Comparison RSA & ECC.

Encryption timings for the ECC and RSA methods are shown in Figure (4.3).

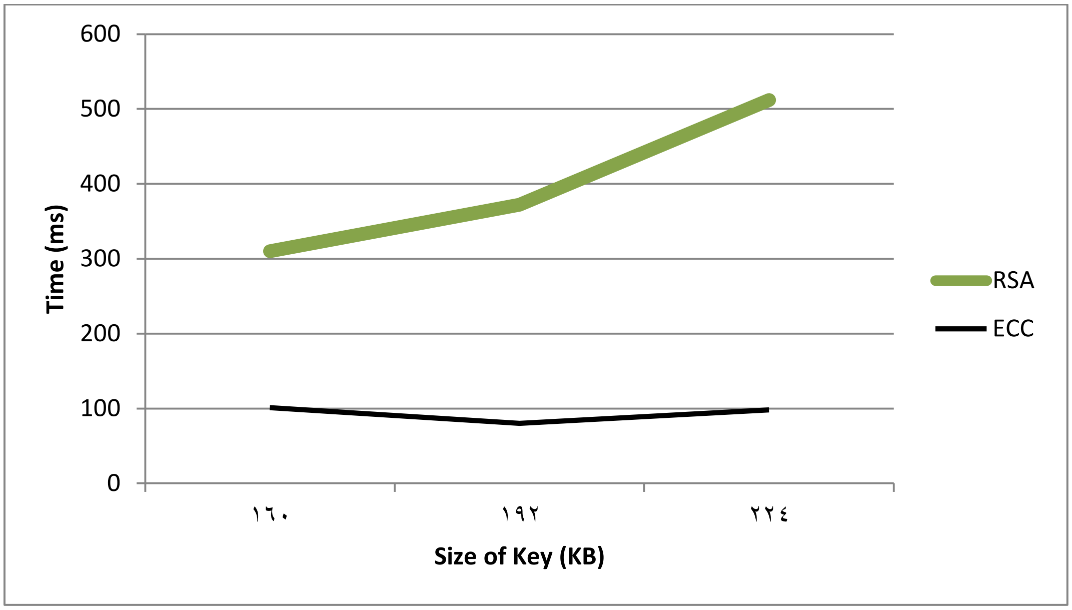
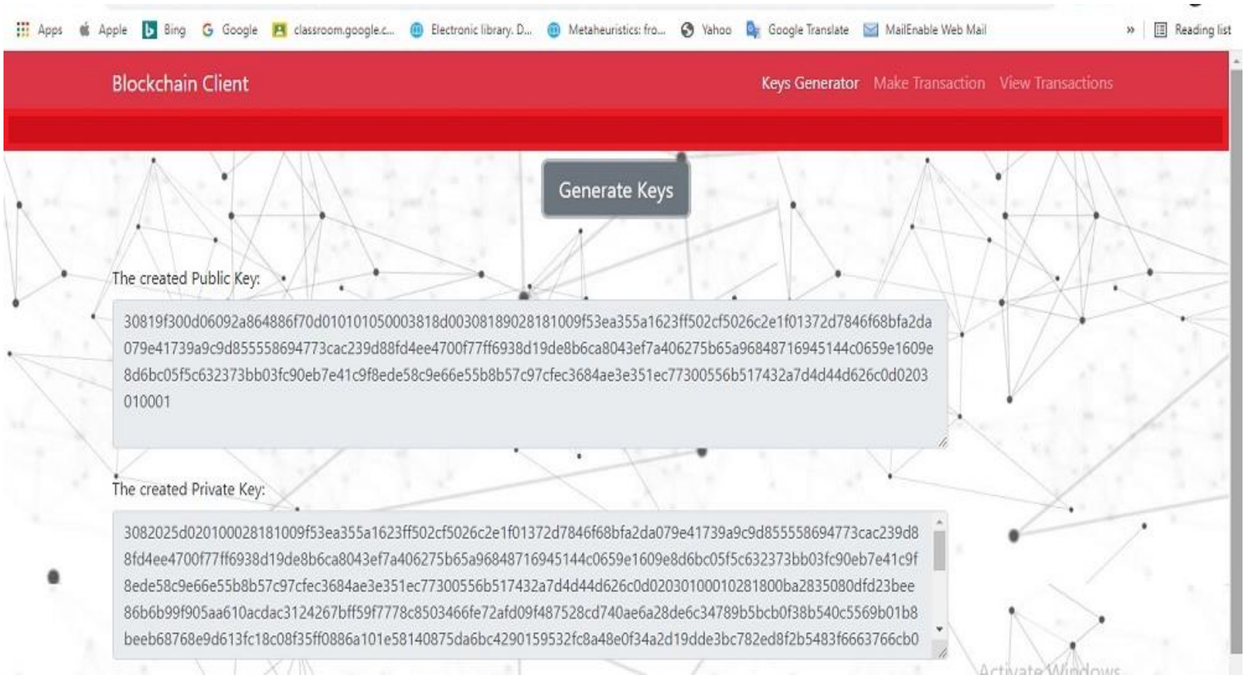


Figure 4.3: Encryption Time RSA & ECC.

The below Figure (4.4) show the interface of our private blockchain system key generation.



The created Public Key:

```
30819f300d06092a864886f70d010101050003818d0030818902818100 9f53ea355a1623ff502cf5026c2e1f01372d7846f68bfa2da
079e41739a9c9d855558694773cac239d88fd4ee4700f77ff6938d19de8b6ca8043ef7a406275b65a96848716945144c0659e1609e
8d6bc05f5c632373bb03fc90eb7e41c9f8ede58c9e66e55b8b57c97cfec3684ae3e351ec77300556b517432a7d4d44d626c0d0203
010001
```

The created Private Key:

```
3082025d020100028181009f53ea355a1623ff502cf5026c2e1f01372d7846f68bfa2da079e41739a9c9d855558694773cac239d8
8fd4ee4700f77ff6938d19de8b6ca8043ef7a406275b65a96848716945144c0659e1609e8d6bc05f5c632373bb03fc90eb7e41c9f
8ede58c9e66e55b8b57c97cfec3684ae3e351ec77300556b517432a7d4d44d626c0d02030100010281800ba2835080dfd23bee
86b6b99f905aa610acdac3124267bff59f7778c8503466fe72afd09f487528cd740ae6a28de6c34789b5bcb0f38b540c5569b01b8
beeb68768e9d613fc18c08f35ff0886a101e58140875da6bc4290159532fc8a48e0f34a2d19dde3bc782ed8f2b5483f6663766cb0
```

Figure 4.4: Interface of key generator

4.3.2 Hashing Algorithm

Figure (4.5) shows that the bigger the number of hash bits, the much more secure the system is. As a result, the output bits of SHA-1, SHA-512, and SHA-256 are equivalent.

While choosing a secure hash algorithm, the file type for execution is a significant consideration. The time it takes to execute a file of type character and number, image file, or text file is shown in Figure (4.6). As a result, SHA-1 takes much less time to process huge files than SHA-256 and SHA-512. For example, if there are 4000 text lines of normal data, it is encrypted into 64 characters and you decode the 64 characters, which are converted into 4000 lines, which are stored inside the blockchain. Only 64 characters are encrypted, and the encryption process for the block takes place at the end of the day or within the chosen time frame.

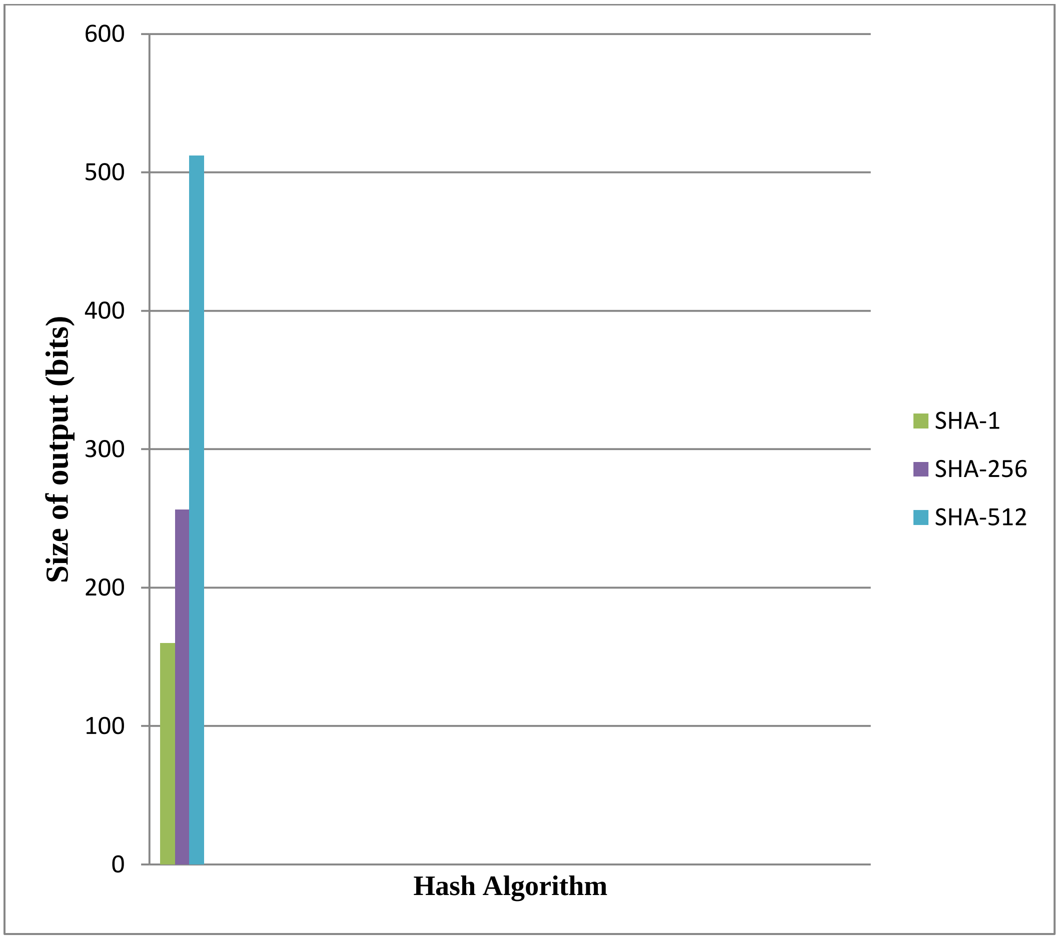


Figure 4.5: Comparing Hash Algorithm Evaluation.

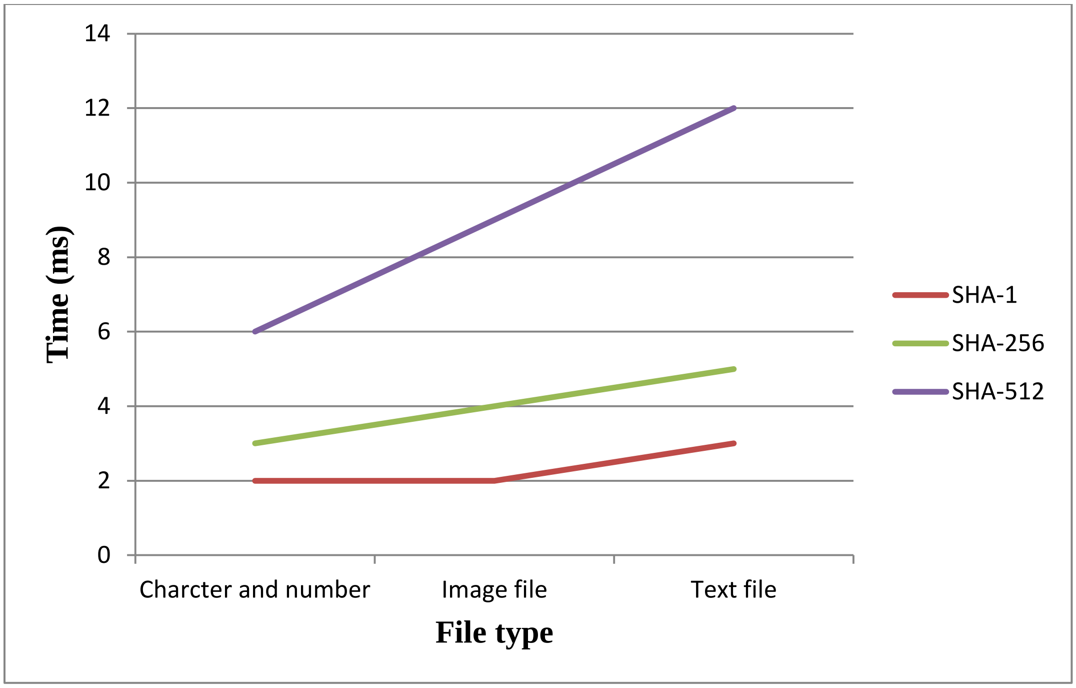


Figure 4.6: Comparing Hash Algorithms based on file type.

With these two loops, the configuration is executed on localhost, and the results of many samples are compiled and analyzed. There are three main samples, which are listed in Tables (4.3,4, 4, and 4.5).

Table 4.3: two loops (ms) Implementation time to small series

Hash Type	First loop	Second loop
SHA-1	355	372
SHA-256	415	390
SHA-512	366	455

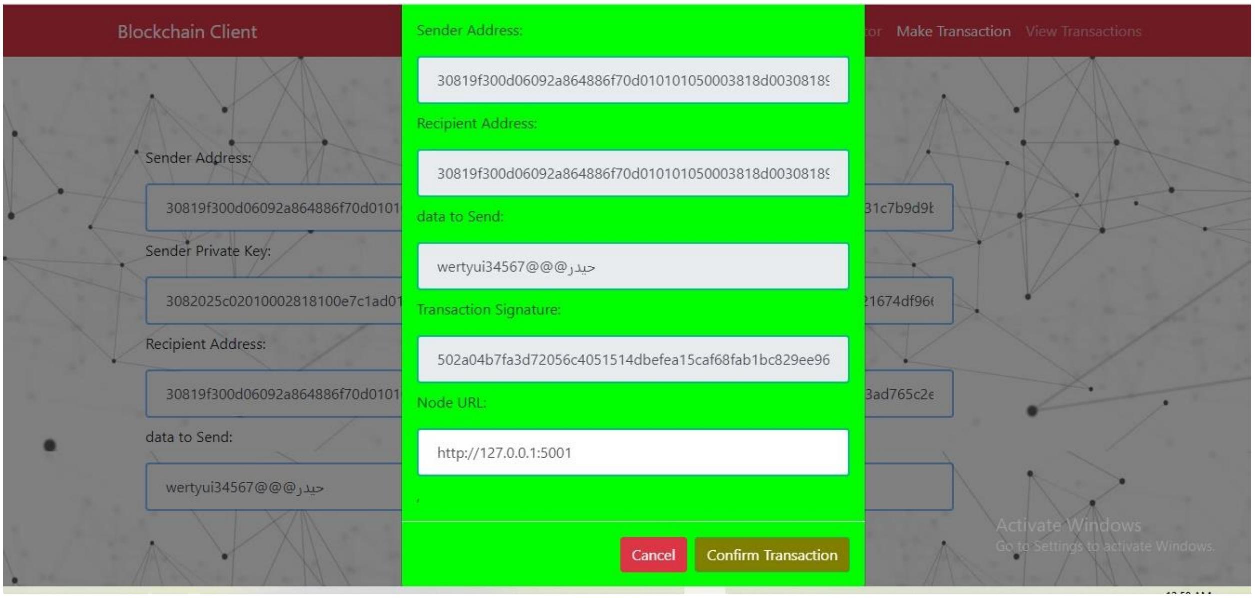
Table 4.4: two loops (ms) Implementation time to middle series

Hash Type	First loop	Second loop
SHA-1	417	510
SHA-256	433	605
SHA-512	399	602

Table 4.5, two loops (ms) Implementation time to large series.

Hash Type	First loop	Second loop
SHA-1	715	810
SHA-256	680	805
SHA-512	680	802

The Figure (4.7) below indicates the main window of the hashing and signature process.



Sender Address: 30819f300d06092a864886f70d010101050003818d0030818

Recipient Address: 30819f300d06092a864886f70d010101050003818d0030818

data to Send: wertyui34567@@@حيدر

Transaction Signature: 502a04b7fa3d72056c4051514dbefea15caf68fab1bc829ee96

Node URL: http://127.0.0.1:5001

Figure 4.7: Step of hashing technique.

4.3.3 Smart Contracts

The smart contract that implemented was very fast and also has sufficient protection for all the nodes and this speed decreases very slowly with the increase of the nodes as shown in the Table (4.6) below.

Table 4.6: speed of smart contract in our system

Number of Nodes	Time (ms)
2	1
5	1.2
10	1.5
20	1.8

40	2
60	2.2

Noticed in Figure (4.8) the small difference in time when the number of nodes increases.

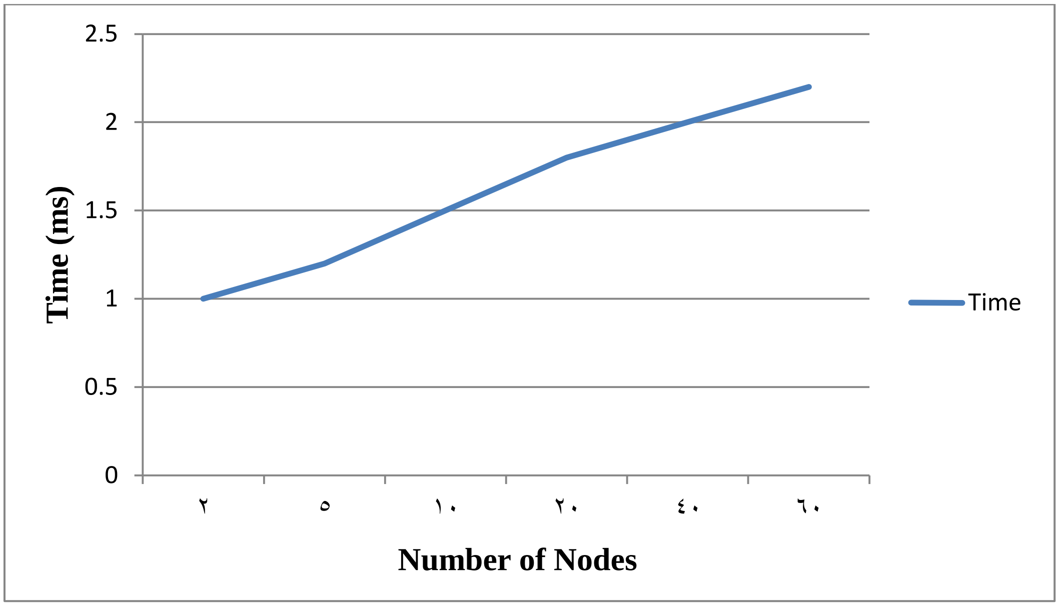
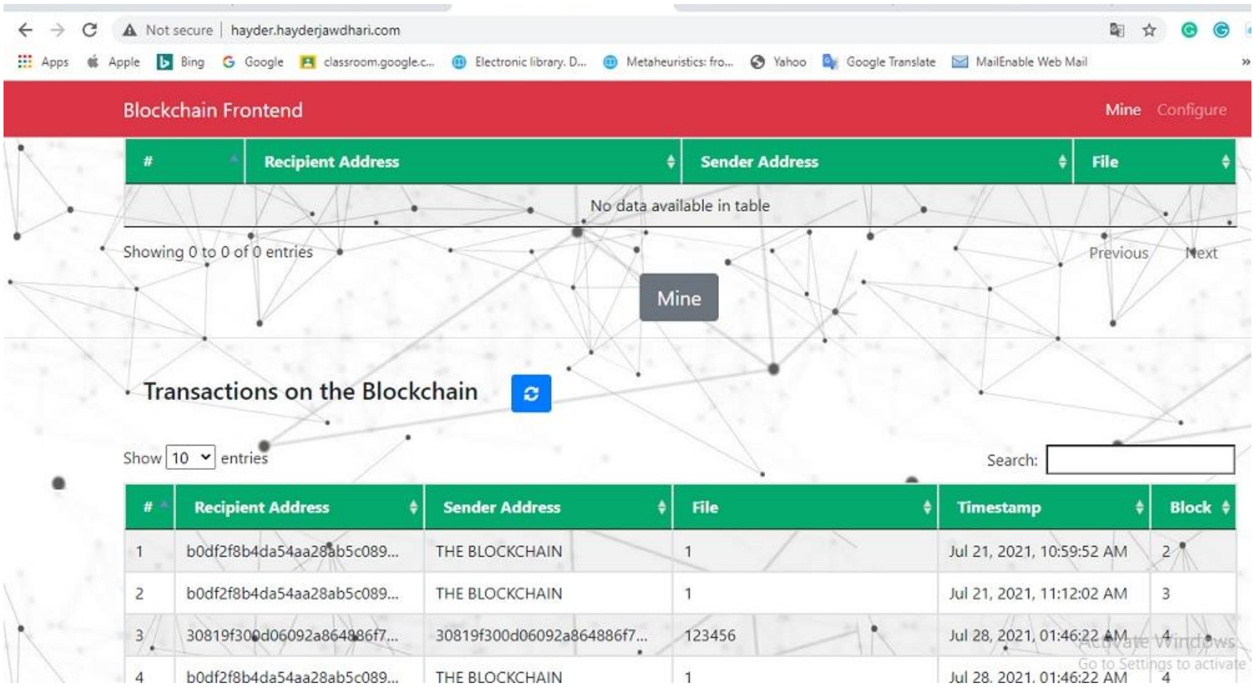


Figure 4.8: Difference time of Smart contract execution.

Figures (4.9, 4.10 and 4.11) refer to the direct application of the smart contract between the different types of data in the proposed system. The recipient address, sender address, files type, timestamp and block number are also shared. Through the three figures, we note that all transactions arrived at the same time and from the same sender's address.



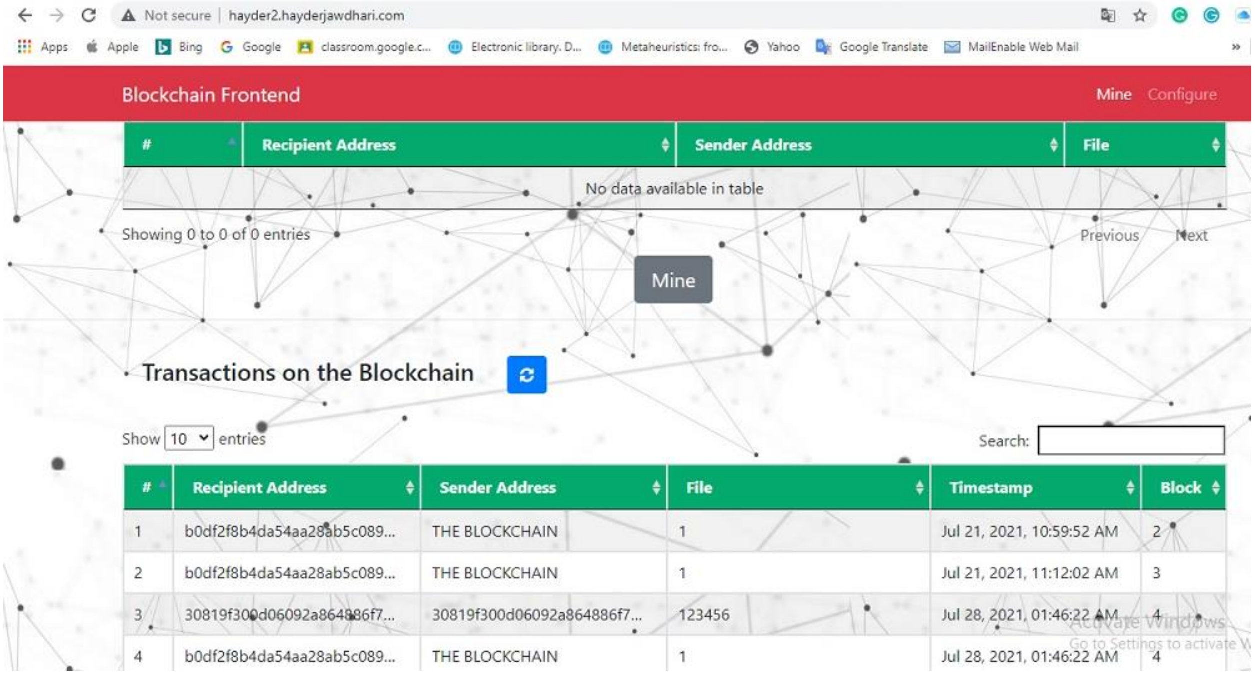
#	Recipient Address	Sender Address	File
No data available in table			

Showing 0 to 0 of 0 entries

Transactions on the Blockchain

#	Recipient Address	Sender Address	File	Timestamp	Block
1	b0df2f8b4da54aa28ab5c089...	THE BLOCKCHAIN	1	Jul 21, 2021, 10:59:52 AM	2
2	b0df2f8b4da54aa28ab5c089...	THE BLOCKCHAIN	1	Jul 21, 2021, 11:12:02 AM	3
3	30819f300d06092a864886f7...	30819f300d06092a864886f7...	123456	Jul 28, 2021, 01:46:22 AM	4
4	b0df2f8b4da54aa28ab5c089...	THE BLOCKCHAIN	1	Jul 28, 2021, 01:46:22 AM	4

Figure 4.9: The smart contract process in first node.



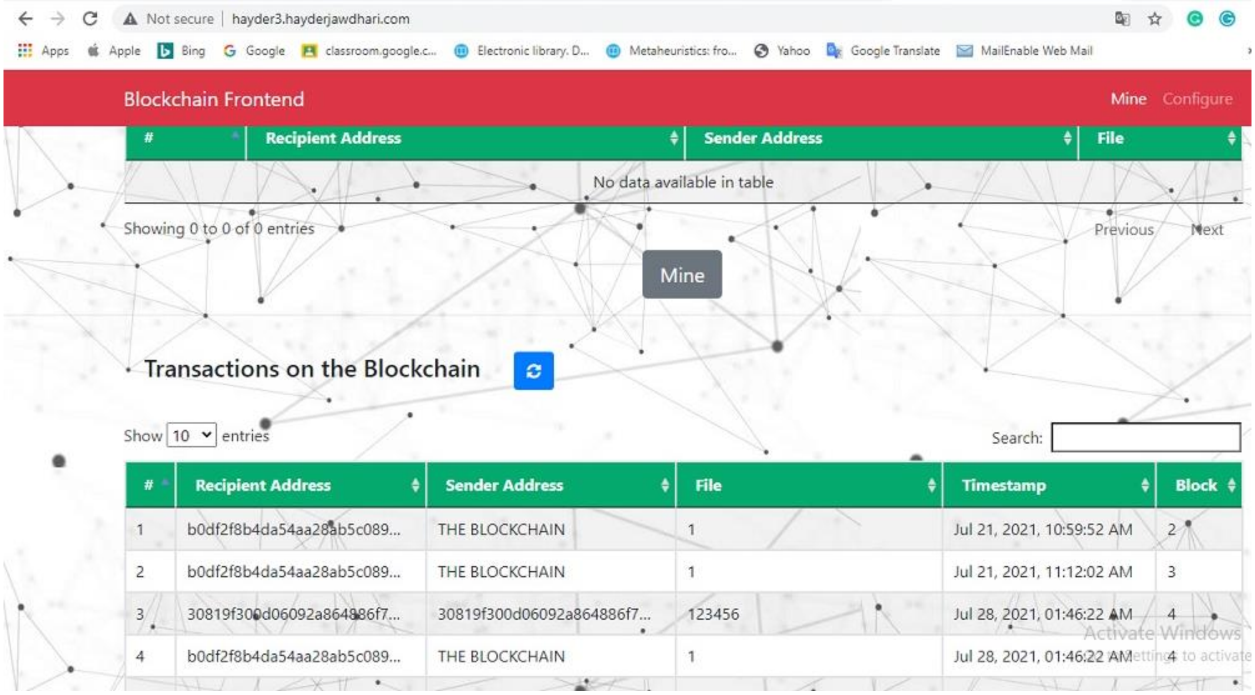
#	Recipient Address	Sender Address	File
No data available in table			

Showing 0 to 0 of 0 entries

Transactions on the Blockchain

#	Recipient Address	Sender Address	File	Timestamp	Block
1	b0df2f8b4da54aa28ab5c089...	THE BLOCKCHAIN	1	Jul 21, 2021, 10:59:52 AM	2
2	b0df2f8b4da54aa28ab5c089...	THE BLOCKCHAIN	1	Jul 21, 2021, 11:12:02 AM	3
3	30819f300d06092a864886f7...	30819f300d06092a864886f7...	123456	Jul 28, 2021, 01:46:22 AM	4
4	b0df2f8b4da54aa28ab5c089...	THE BLOCKCHAIN	1	Jul 28, 2021, 01:46:22 AM	4

Figure 4.10: The smart contract process in second node.



#	Recipient Address	Sender Address	File
No data available in table			

Showing 0 to 0 of 0 entries

Previous Next

Transactions on the Blockchain

Show 10 entries

Search:

#	Recipient Address	Sender Address	File	Timestamp	Block
1	b0df2f8b4da54aa28ab5c089...	THE BLOCKCHAIN	1	Jul 21, 2021, 10:59:52 AM	2
2	b0df2f8b4da54aa28ab5c089...	THE BLOCKCHAIN	1	Jul 21, 2021, 11:12:02 AM	3
3	30819f300d06092a864886f7...	30819f300d06092a864886f7...	123456	Jul 28, 2021, 01:46:22 AM	4
4	b0df2f8b4da54aa28ab5c089...	THE BLOCKCHAIN	1	Jul 28, 2021, 01:46:22 AM	4

Figure 4.11: The smart contract process in third node.

4.4 Cost of Construction the Private Blockchain

In the table below we will show in detail the cost required to build a private blockchain network, which starts from the number of computers representing each computer per node.

The cost of private blockchain construction is used upon numerous activities of the environment Table (4.7) includes:

- **Computers (Nodes):** the number of computers used in this environment is three and the rest (57) are used as the port numbers to refer to the nodes that have a local blockchain.
- **Deployment:** Deployment on AWS
- **Upgrade:** a new condition in Smart Contracts.

Table 4.7: activities of the blockchain environment.

activities	Approximate cost
Computer	3*300$= 900$
Deployment	register a domain=12$ hosted zone is =$0.50 per month Amazon CloudWatch =$1.00 Data Transfer =0.07$ Bandwidth =0.07$ Elastic Compute Cloud= 97.84$ Elastic Load Balancing=150.53 $ Route 53 = 3.00$ Total =265.01$ per month

4.5 Evaluation the Proposed System of Blockchain

The main metrics that were utilized included: throughput, Consensus, transaction size Table (4.8). The first metric indicates the number of transactions in the system per second (transaction per second). Entire transaction time indicates the entire period that started from the client procedure which his/her role creates the transaction then finishes by arriving in the blockchain. The second metric consensus algorithm should choose suitable due to it might cause a massive passive influence on the nodes and all operations in the system. The third metric transaction size also should choose suitable may have risen deployment of blockchain fees.

Table 4.8: Major blockchain execution evaluation metrics

Metric	Challenge	Solution
Tps	The parameters of system should choose in appropriate way is required when want to attain the required transaction per second.	create an parallel verification instead of single verification, that speed up the operation of Proof of Work
Consensus	Validation of transactions.	Add utility functions for Power of work consensus protocols.

Transaction size	The size of transaction that to be added in the following block.	Smart contracts get better the implementation time of transactions and decrease transaction size.

4.6 Comparison the Proposed System with Standard System.

In this part, will present a comparison between the system designed by us and the rest of the common blockchain systems in terms of the tokens used, security, cost, smart contracts are shown in Table (4.9).

Table 4.9, comparison between our private blockchain and others blockchain systems

Blockchain	Tokens used	Security	Cost **($)**	Smart Contract
Our Blockchain	Text, number, letters, Arabic letters, Pdf files.	Asymmetric - key, hash functions, Proof of Work.	(1,165) for 3 computers.	Consensus algorithm, Auto smart contract, programmed smart contract
Ethereum blockchain	Ether	Permissionless, immutability	15,000 up to 50,000	Solidity , Vyper [109]
Bitcoin	digital currency	cryptography	7,000-11,000	Pay-to-Public-Key-Hash (P2PKH) [110]

Noted from the above table that there is convergence and divergence at the same time. Through the token field, we were able to send all formats, including files of medium sizes, compared to the rest of the systems that send only one format. As for the security field, we applied what the systems use in addition to techniques that are able to verify the transmitted files. As for the cost field, it indicates a significant reduction in cost compared to the rest of the systems because it depends on nodes and AWS only, which are computers or any other device. The last field was built as an automatic smart contract based on the transmitted formulas that simulate them according to their type and content.

4.7 Upload proposed system to AWS

Among your client and Amazon S3, Amazon S3 transfer acceleration can deliver quick and secure transfers across lengthy ranges. Amazon CloudFront's globally distributed edge locations are used for transfer acceleration. There are many results we got based on many metrics:

4.7.1 Architecture

The important result that we got from uploading the proposed system to the cloud is the architecture through which we obtained virtualization and created architecture similar to NFV.

4.7.2 Scalability

AWS Web Service monitors all real - world applications time and increases capability as necessary to keep consistent, predictable outcomes at the cheapest cost.

4.7.3 Flexibility

When RIs are purchased for use in a specified Availability Zone (AZ), AWS clients gain a large discount on their EC2 consumption (up to 75% when compared to On-Demand pricing), as well as capacity reservation. It can also swiftly adapt to varied workloads, data formats, and configuration options, allowing for a faster reaction to new business needs and circumstances.

4.7.4 Parameters for Comparing Cloud Cost

For better understanding of the cost difference, we’re considering the same region (Bahrain) to compare CPUs (vCPUs/Cores: 2) and operating systems (Windows) for AWS instances and Azure Virtual machines. That calculates for many types of instances such as **general-purpose**, **compute-optimized**, **Storage optimized** and **accelerated computing**, the hourly on-demand price structure of each service is listed in Table (4.10) below for each of the four instance-type instances.

Table 4.10: Comparison of On-Demand Pricing

Instance	AWS	Cost (per hour) ($)	Azure virtual machines	Cost (per hour) ($)
general-purpose	t3.nano	0.0109	B1s	0.0146
compute-optimized	c5.large	0.198	F2s v2	0.108
Storage optimized	i3.large	0.281	L8s v2	0.748
accelerated computing	g4dn.xlarge	0.829	H8	0.924

4.8 Blockchain-NFV

A clear and common NFV-blockchain architecture is proposed to dive into the issues such as the ability to increase or decrease in scale, the quality or state of being secure and funding networks in blockchain systems. Via virtualizing blockchain environment, it turns into the possibility to be efficacious, scalable, and elastic at blockchain domains. Further, an industry viewpoint is supplied through the execution of NFV to the existing architecture. The consequences demonstrate that throughput above 20% has been acquired via using NFV, attended with a speed of execution above 50%. Eventually, a significant throughput has been got with the time excellence through the utilizing of NFV.

4.8.1 Virtual Distributed Ledger Technology

In comparison to DLT, vDLT boosts transaction speeds to roughly 120 transactions per second as shown in Figure (4.12). We build a network with sixty nodes. We create a variety of block levels ranging from 0 to 10. The block size has been fixed at 65 transactions per block. The pace of arrival of transactions is 77 transactions per second.

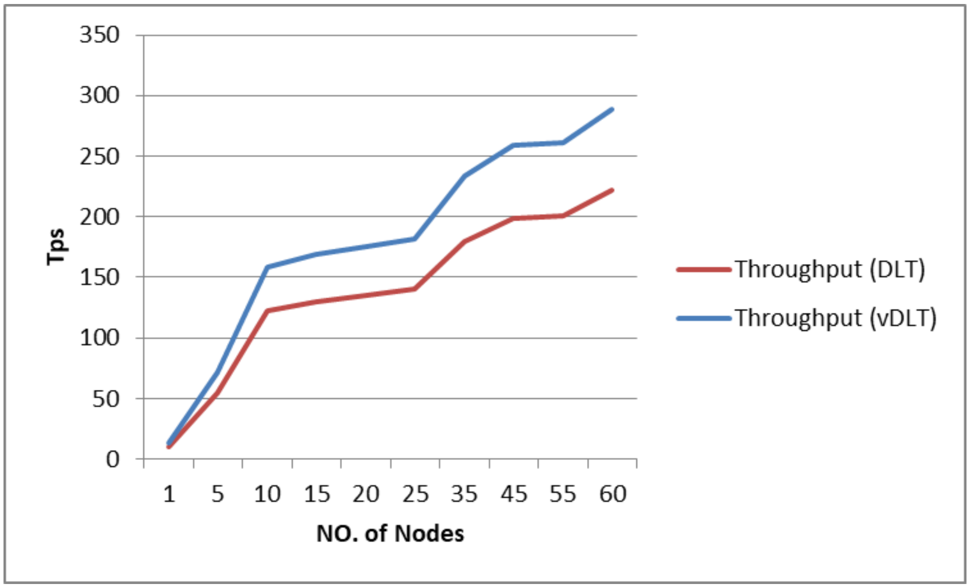


Figure 4.12: Comparison to DLT, vDLT throughput.

4.8.2 Virtual Hash algorithms

In this part, we did several experiments on five types of files of different sizes, how the hash affects these files and how much CPU is used, thus we made a comparison between SHA-1 ,SHA-256,SHA-512 before and after applied NFV to hash function Table (4.11).

Table 4.11: Comparison between SHA-1, SHA-256, and SHA-512 CPU usage without NFV.

Experiment No.	File size (KB)	SHA-1 CPU %	Time (ms)	SHA-256 CPU %	Time (ms)	SHA-512 CPU %	Time (ms)
1	20	1.880	50	1.722	43	1.922	51
2	80	2.875	14	2.522	13	2.570	23
3	400	1.255	8	1.255	9	1.300	16
4	5	0.544	18	.551	15	.677	18
5	8	1.144	33	1.222	27	1.248	36

From Table (4.11) and Figure (4.13), it is obvious the percentage of CPU time used to grow as the file size grew larger as well as the implementation time increased as the size of the file grew. The total time for the 5 experiments was 123 (ms) for SHA-1, 107 (ms) for SHA-256 and 144 (ms) for SHA-512 and the CPU for the five experiments was 7.69% for SHA-1, 7.27% for SHA-256, and 7.78%

for SHA-512, we observed the using of SHA-256 is better from two sides the first is the usage of CPU and the time.

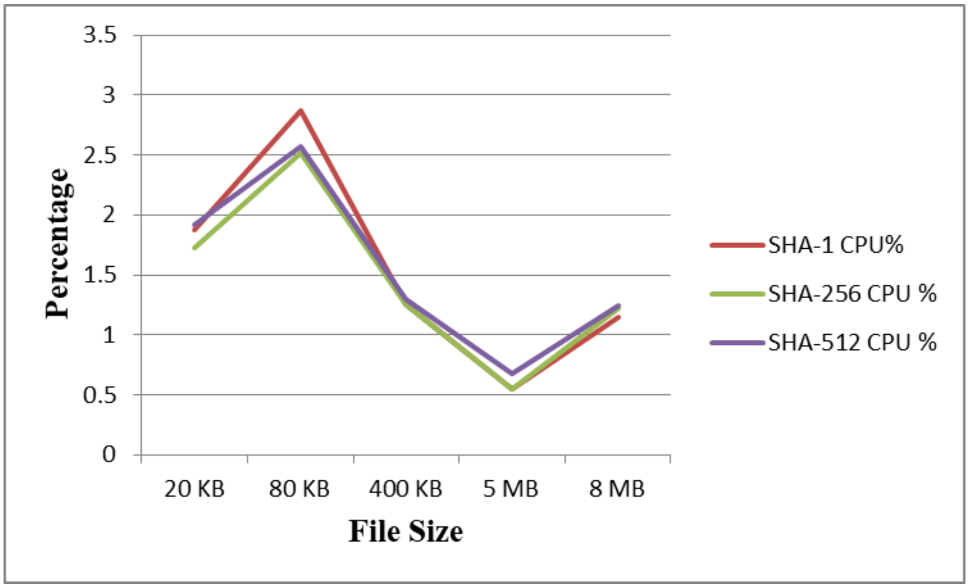


Figure 4.13: CPU percentage without NFV.

But in Table (4.12) and Figure (4.14) we notice a noticeable difference in the decrease in CPU usage, after creating a default hash to encrypt the files in the virtual ledger

Table 4.12: Comparison between SHA-1, SHA-256, and SHA-512 CPU usage NFV.

Experiment No.	File size (KB)	SHA-1 CPU %	Time (ms)	SHA-256 CPU %	Time (ms)	SHA-512 CPU %	Time (ms)
1	20	1.512	41	1.088	33	1.654	37
2	80	2.114	9	2.147	5	2.325	15
3	400	1.110	3	1.055	6	1.101	11
4	5	0.240	7	.411	11	.514	13
5	8	1.044	21	1.111	18	1.018	29

Where the SHA-1 CPU decrease to 6.02% in 71 (ms), SHA256 decrease to 5.81% in 73 (ms) and SHA-512 decrease to 6.61% in 105 (ms)

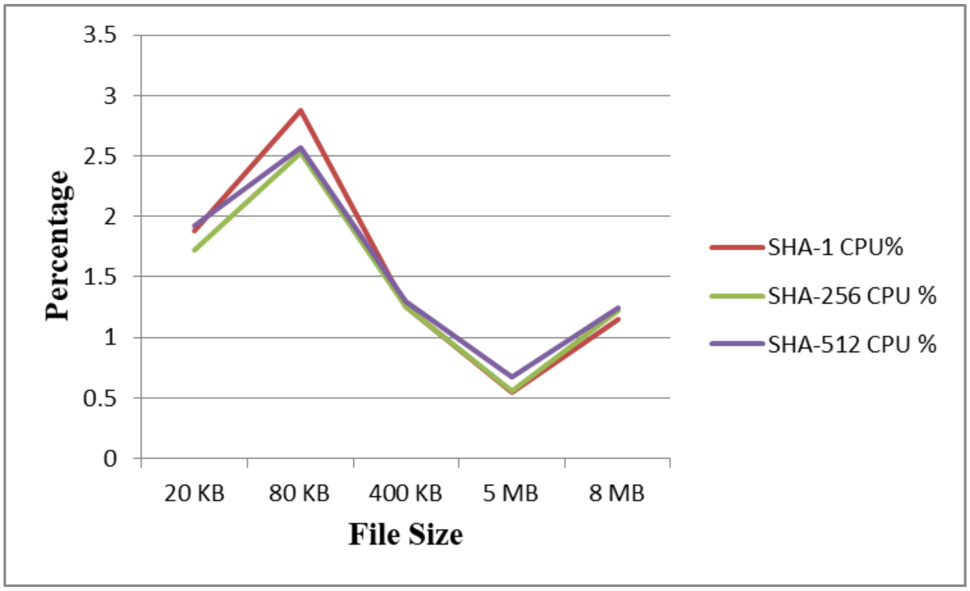
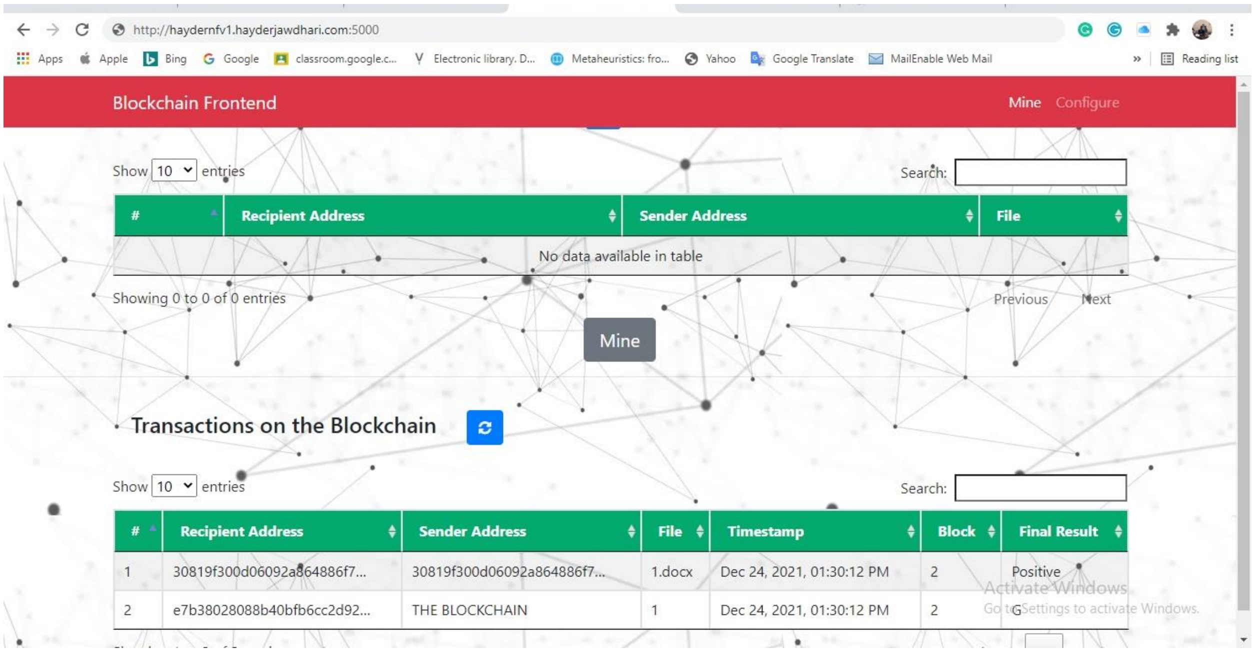


Figure 4.14: CPU percentage with NFV.

The three figures below refer to the interfaces of the functions that we got in virtual inside the node, where Figure (4.15, 4.16, and 4.17) refer to the first, second and third node respectively



Show 10 entries

Search:

#	Recipient Address	Sender Address	File
No data available in table			

Showing 0 to 0 of 0 entries

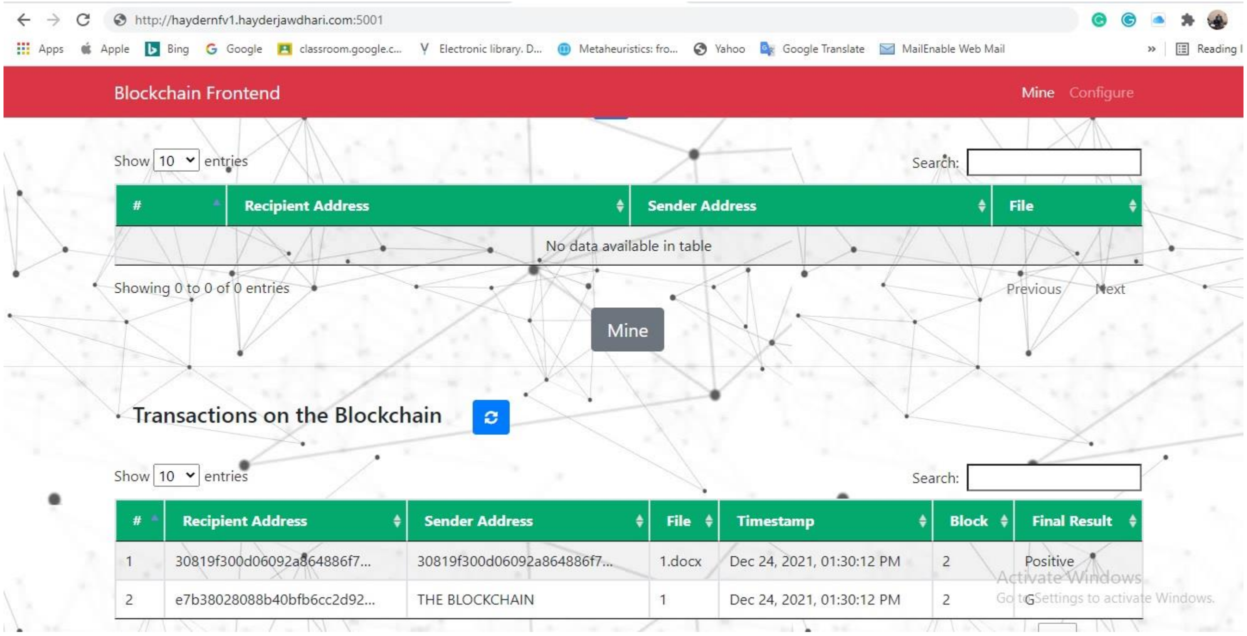
Transactions on the Blockchain

Show 10 entries

Search:

#	Recipient Address	Sender Address	File	Timestamp	Block	Final Result
1	30819f300d06092a864886f7...	30819f300d06092a864886f7...	1.docx	Dec 24, 2021, 01:30:12 PM	2	Positive
2	e7b38028088b40bfb6cc2d92...	THE BLOCKCHAIN	1	Dec 24, 2021, 01:30:12 PM	2	G

Figure 4.15: The virtual functions inside the first node.



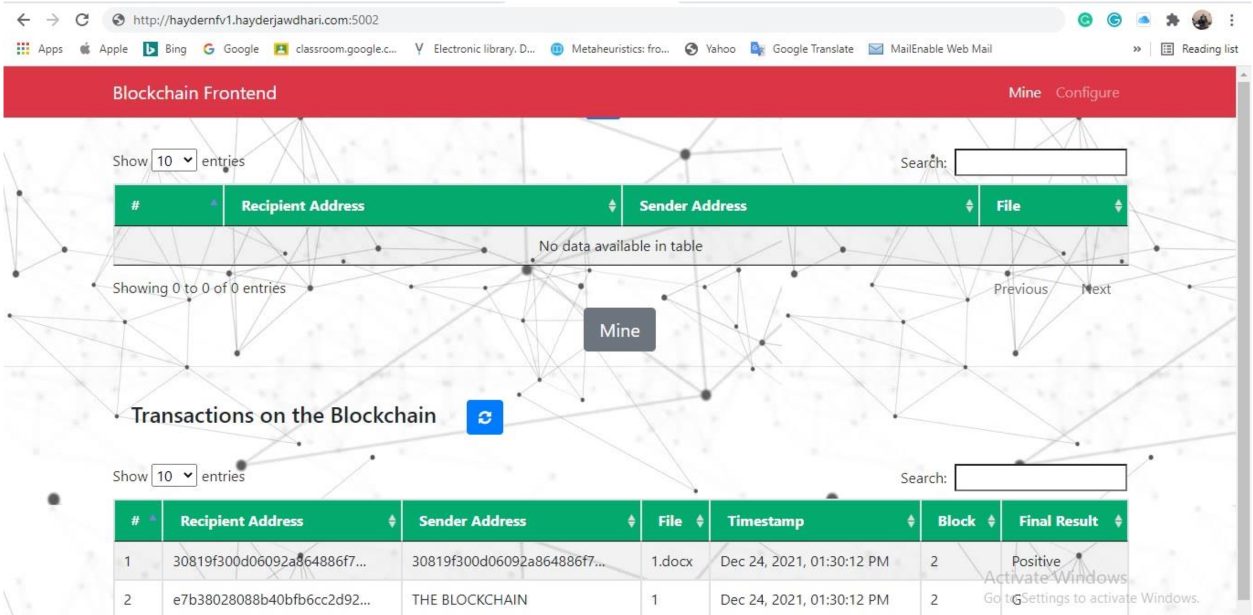
#	Recipient Address	Sender Address	File
No data available in table			

Showing 0 to 0 of 0 entries

Transactions on the Blockchain

#	Recipient Address	Sender Address	File	Timestamp	Block	Final Result
1	30819f300d06092a864886f7...	30819f300d06092a864886f7...	1.docx	Dec 24, 2021, 01:30:12 PM	2	Positive
2	e7b38028088b40bfb6cc2d92...	THE BLOCKCHAIN	1	Dec 24, 2021, 01:30:12 PM	2	

Figure 4.16: The virtual functions inside the second node.



#	Recipient Address	Sender Address	File
No data available in table			

Showing 0 to 0 of 0 entries

Transactions on the Blockchain

#	Recipient Address	Sender Address	File	Timestamp	Block	Final Result
1	30819f300d06092a864886f7...	30819f300d06092a864886f7...	1.docx	Dec 24, 2021, 01:30:12 PM	2	Positive
2	e7b38028088b40bfb6cc2d92...	THE BLOCKCHAIN	1	Dec 24, 2021, 01:30:12 PM	2	

Figure 4.17: The virtual functions inside the third node.

4.8.3 Evaluation of Virtual Blockchain

● Throughput

It shows the number of whole transactions that send within the blockchain. An allocated job may be specified for numerous clients to expand the throughput of our system.

● Latency

It shows the latent time for the separate transactions, where the standard number is based on literature is 7 transactions per second [111].

● Scalability

It shows the divagations between throughput and latency when the numeral of nodes begins expanding in a synchronized manner to the allocated work that is needed.

● Cost

As corresponded to time-honored blockchain systems, and make allowances for aspects such as their complicatedness and control methodology, the cost does absolutely be, whereas they rely on the essential booking in the cloud, furthermore the time and capability. This indicates that the expenditure is zero for the machines because the dependence was particularly based on virtual devices via the usage of network function virtualization. As for the common booking, whether it is a cloud or a server, the annual expense varies amidst 290 - 3000 dollars.

Different speeds have been shown through considerable blockchains for deploying, recalling, and executing smart contracts. The major objective of this work is to monitor the latency of throughput that depicts whole transactions per second Table (4.13). Also, based on equations (2.1, or 2.2) calculated the throughput, latency.

Table 4.13, Throughput, Latency and node without NFV.

Time (ms)	No. of Nodes	No. Transactions (tps)
1	2	420

2.46	3	1162
3	5	1260
5	7	2100
10	9	4200

Table (4.14) there is a big contrast seen in the average throughput via depending on Virtual Operations (NFV) in a relaxed environment like the blockchain system.

Table 4.14, Throughput, Latency and node with NFV.

Time	No. of Nodes	No. Transactions
1	2	540
2.46	3	1494
3	5	1620
5	7	2700
10	9	5400

4.8.4 Comparison Virtual Blockchain with Common Blockchain

By comparing the common blockchain system with the NFV-based system and Bitcoin based on a set of important elements as shown in Table (4.15):

1- Throughput

Blockchain technology relies on encryption to confirm credibility and security and is characterized by decentralized and tamper-resistant procedures and increased throughput, which enables promising applications in strategic areas, such as banking, healthcare, agriculture, voting, complex supply chains, energy, intellectual property, management, and digital identities, and this applies to the government sector also.

2- Reducing the Time

Blockchain can play an important role via permitting for faster transaction settlement because it eliminates the need for a lengthy confirmation, settlement, and certification procedure because all parties will have access to a specific duplicate of the approved data.

3- Security

When you attack a standard database, you're dropping a particular target. Because blockchain technology allows each end to keep a version of the original chain, the system can continue to function even if a substantial number of other nodes fail.

Table 4.15: Comparison between our BC, BC-NFV, Bitcoin and Ethereum

System	Throughput	Time (min)	Security
Proposed BC	4200 Tps	10	Asymmetric -key, hash functions, Proof of Work.
Proposed BC-NFV	5400 Tps	10	Double(Asymmetric -key, hash functions, Proof of Work)
Bitcon	3-7	10	P2PKH [110]
Ethereum	15-25	6	Solidity , Vyper [109]

Figures (4.18, and 4.19) indicate the throughput of our blockchain system as corresponded to the time and numeral of the nodes within the blockchain. It has been noticed that there is an opposite contrast amidst the down figures. When the first figure indicates the execution of the approach without NFV and the other indicates the approach as executed utilizing NFV. There is a discrepancy in every transaction that guides to a big contrast in the growth of time in addition to the growth of nodes.

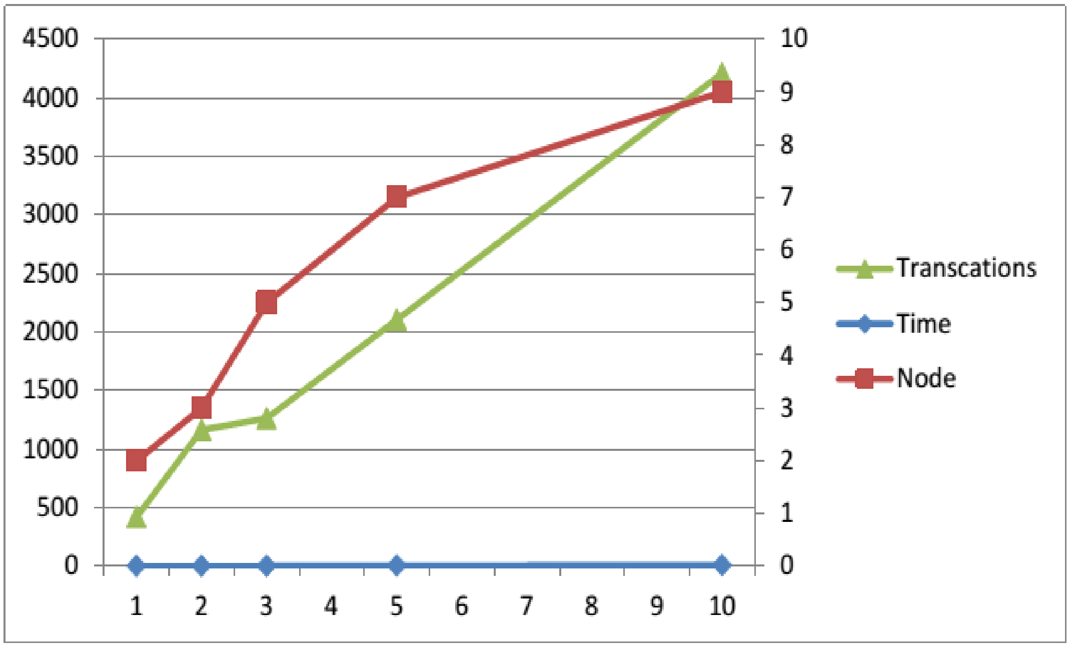


Figure 4.18: Throughput, Latency and node without NFV.

Where x axis indicated the **time**, and y axis indicates to the **No. of transactions**).

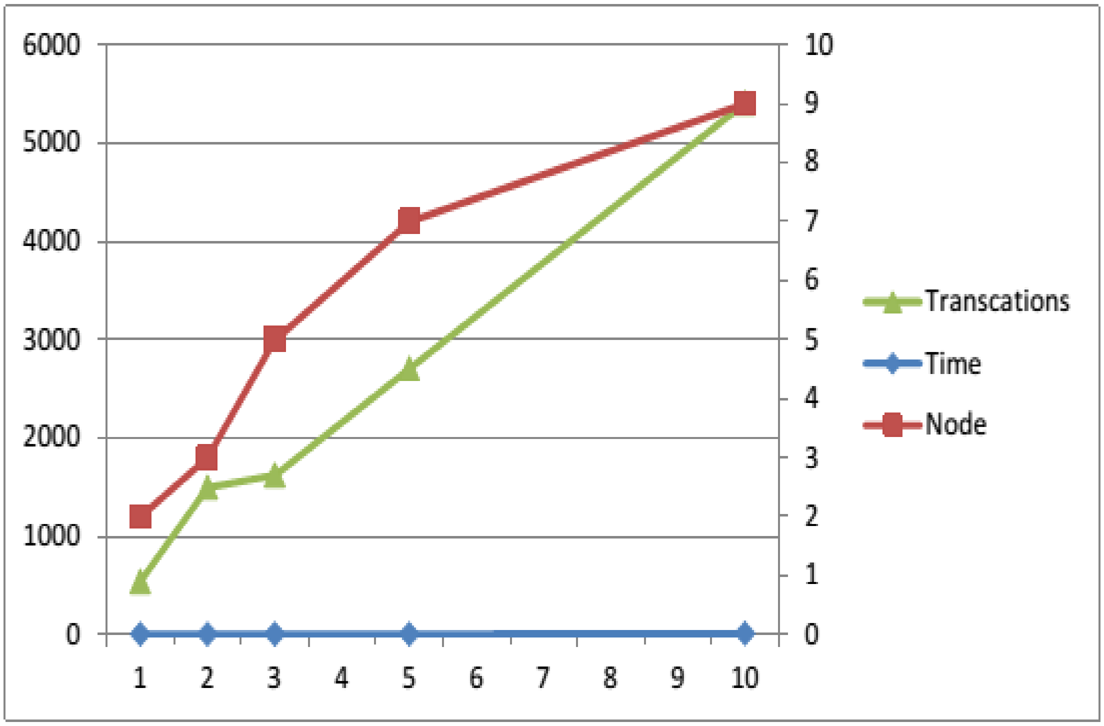


Figure 4.19: Throughput, Latency and node with NFV.

4.9 Blockchain for File Transfer

The goal is to create a safe file sharing program that can be used at random in smaller companies by utilizing a private Blockchain network. A higher degree of security is obtained by employing some key cryptographic techniques to strongly encrypt the file, guaranteeing that no one other than the intended recipient has access to it.

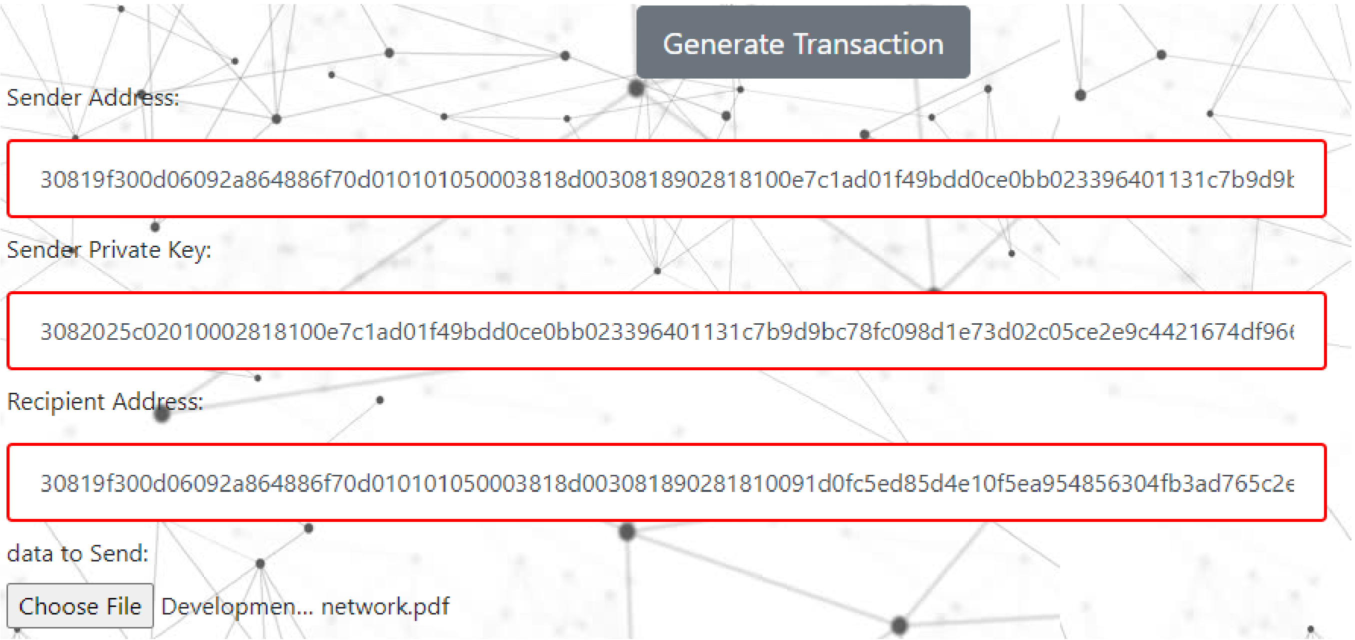
4.9.1 Results of File Sharing

The experiment is accomplished by utilizing the different types of files and different sizes to ensure the effectiveness of the algorithms used. Calculating the execution time for the process of creating a signature and the verification procedure is how testing is done. The results of the execution of the signature processing time using DSA and RSA on blockchain-NFV are shown in Table (4.16).

Table 4.16: RSA and DSA Execution Results

File Type	File size	RSAs Time (ms)	DSAs Time (ms)	RSAv Time (ms)	DSAv Time (ms)
Image file	522 KB	3.258	0.604	0.055	0.065
Image file	765 KB	4.354	0.688	0.065	0.045
Text file	1 MB	7.556	0.947	0.058	0.088
Text file	2 MB	8.361	0.995	0.022	0.078

Figure (4.20) illustrates the essential operation of the transfer of files that are basically not given in advance. That is accomplished via sharing an entire file with signing, behind which it is shared to all the nodes. Furthermore potential to mine them for whole transmitted files. Behind the mining, we give permission to the client to save all files in the cloud. Figure (4.21) shows the files after the transaction procedure.



Sender Address:

30819f300d06092a864886f70d010101050003818d0030818902818100e7c1ad01f49bdd0ce0bb023396401131c7b9d9b

Sender Private Key:

3082025c02010002818100e7c1ad01f49bdd0ce0bb023396401131c7b9d9bc78fc098d1e73d02c05ce2e9c4421674df966

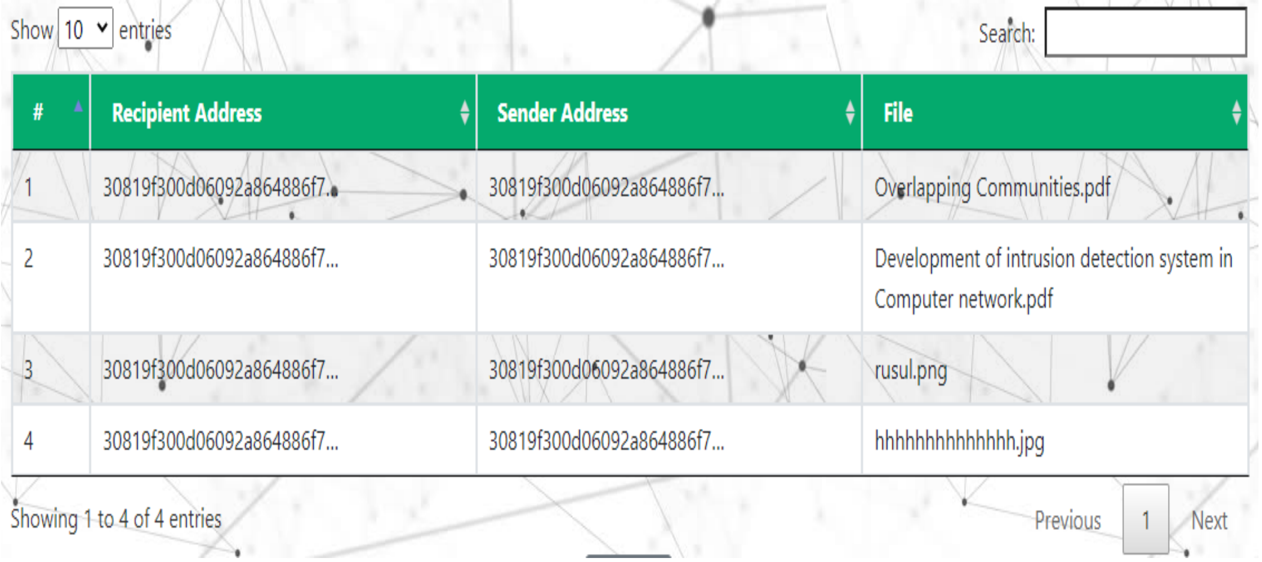
Recipient Address:

30819f300d06092a864886f70d010101050003818d0030818902818100 91d0fc5ed85d4e10f5ea954856304fb3ad765c2e

data to Send:

Developmen... network.pdf

Figure 4.20: The new transaction of the transfer of files.



#	Recipient Address	Sender Address	File
1	30819f300d06092a864886f7...	30819f300d06092a864886f7...	Overlapping Communities.pdf
2	30819f300d06092a864886f7...	30819f300d06092a864886f7...	Development of intrusion detection system in Computer network.pdf
3	30819f300d06092a864886f7...	30819f300d06092a864886f7...	rusul.png
4	30819f300d06092a864886f7...	30819f300d06092a864886f7...	hhhhhhhhhhhhhh.jpg

Showing 1 to 4 of 4 entries

Figure 4.21: Shows the files after the transaction procedure within nodes.

4.9.2 Evaluation and Comparison of File Sharing

The current work is analogized to different corresponding works in two essential characteristics which are believed to be fundamental in the evaluation of producing a system or unique technology, i.e. speed and security.

- Speed is investigated amidst FTP, Ethereum, and the suggested environment as exhibited in Table (4.17). We tested files with various sizes until 400 MB at an arbitrary internet rate. Therefore, a sumptuous rate in data transmit is reached, above 25% of the rates utilized in the remains of the environments.

Table 4.17: Speed compression between FTP, Ethereum and the proposed system.

FTP	Ethereum	Proposed Private blockchain
3.30 minutes [112]	5 minutes (20 transactions) [113]	1.23 Minutes.

- The security side is tested along with some recent literature outcomes associated with blockchain, furthermore with technologies their functions are similar to the blockchain functions that are exhibited in Table (4.18). Strong libraries are added to this system, like (Pycryptodomex), which is characterized this environment from the rest of the environments and made this system gives jobs with significant confidentiality and powerful security.

Table 4.18: Security differentiation between FTP, Ethereum and the proposed system.

FTP	Ethereum	Proposed Private blockchain
Weak [114]	Strong (with vulnerabilities) [115]	Strong

4.10 Blockchain for Secure Healthcare Files

Figure (4.22) depicts the time it takes to uploaded health records utilizing client and Blockchain-NFV and the established basic ledger health care systems as the number of records grows.

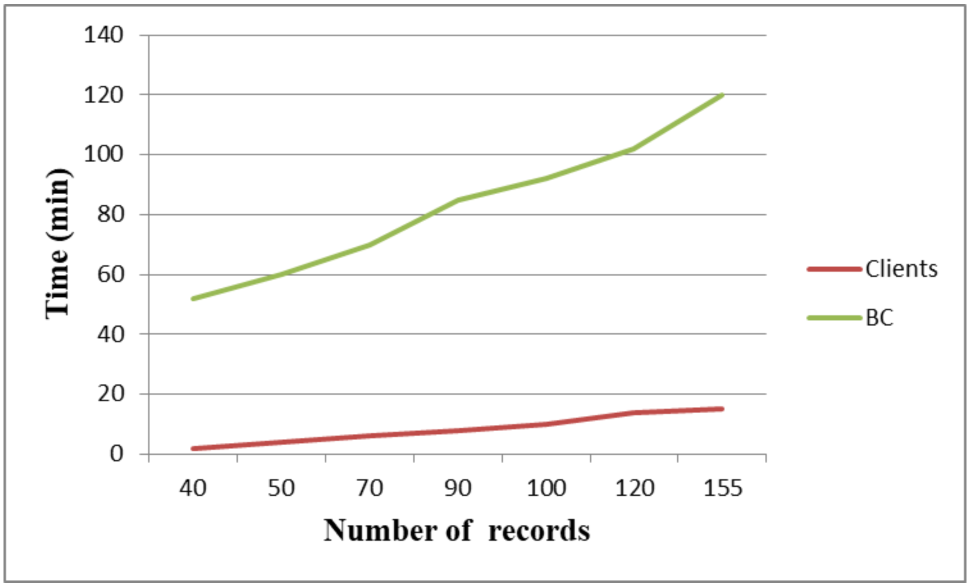
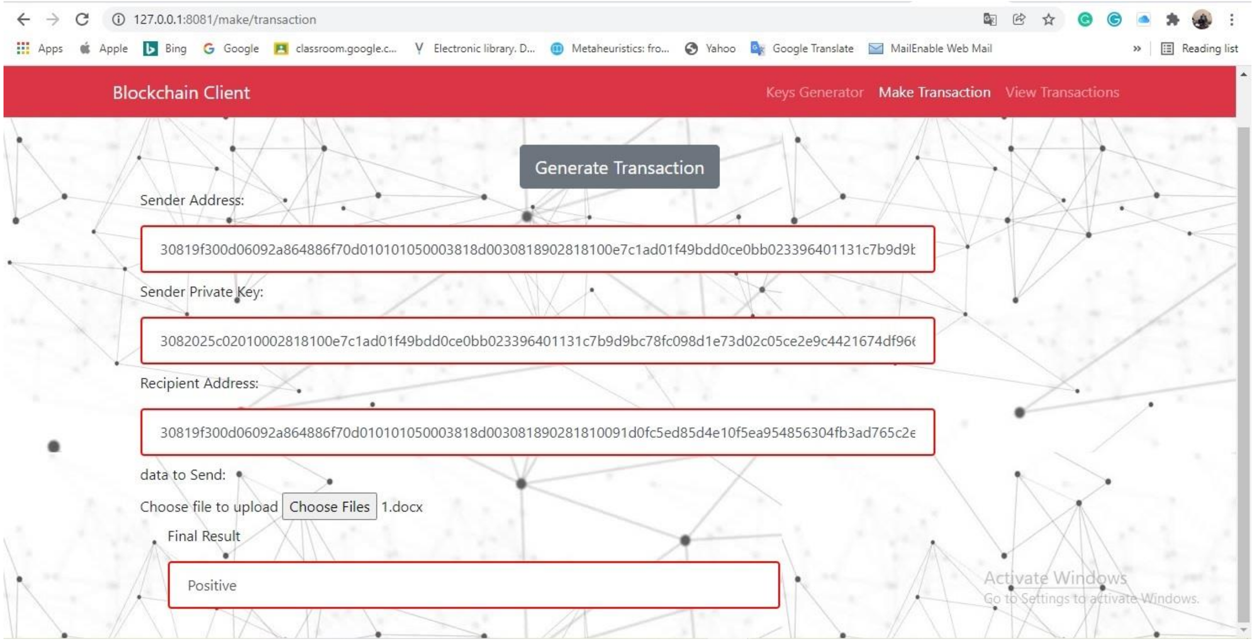


Figure 4.22: Time Execution for health files.

Can be seen that as the number of health records grows, the execution time for clients and blockchain models grows exponentially. The client's system, on the other hand, takes fewer times to execute than blockchain. This is due to the blockchain's data validation and replication consensus process.

In Figures (4.23 ,4.24 ,4.25 and 4.26) below, we used the blockchain as an incubator for health care files, and these files are reports related to patients with a mention of the patient about his health condition through the final result field.



Sender Address:

30819f300d06092a864886f70d010101050003818d0030818902818100e7c1ad01f49bdd0ce0bb023396401131c7b9d9b

Sender Private Key:

3082025c02010002818100e7c1ad01f49bdd0ce0bb023396401131c7b9d9bc78fc098d1e73d02c05ce2e9c4421674df96

Recipient Address:

30819f300d06092a864886f70d010101050003818d003081890281810091d0fc5ed85d4e10f5ea954856304fb3ad765c2e

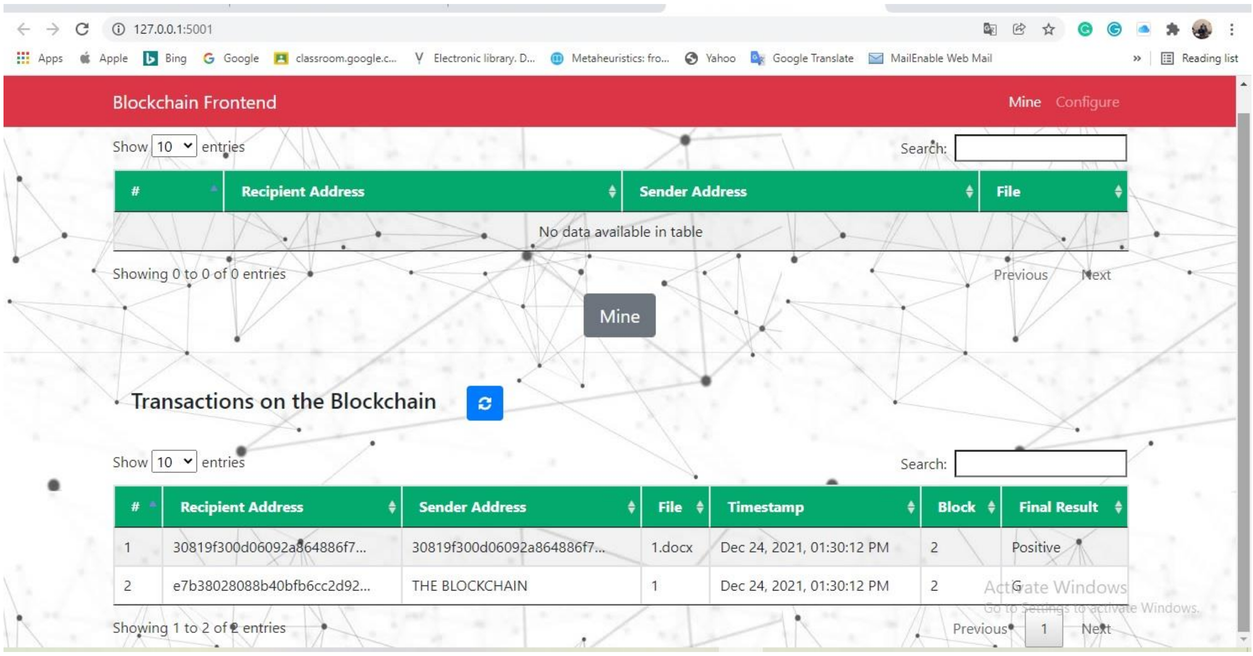
data to Send:

Choose file to upload Choose Files 1.docx

Final Result

Positive

Figure 4.23: The interface of healthcare transaction generation.



Show 10 entries Search:

#	Recipient Address	Sender Address	File
No data available in table			

Showing 0 to 0 of 0 entries Previous Next

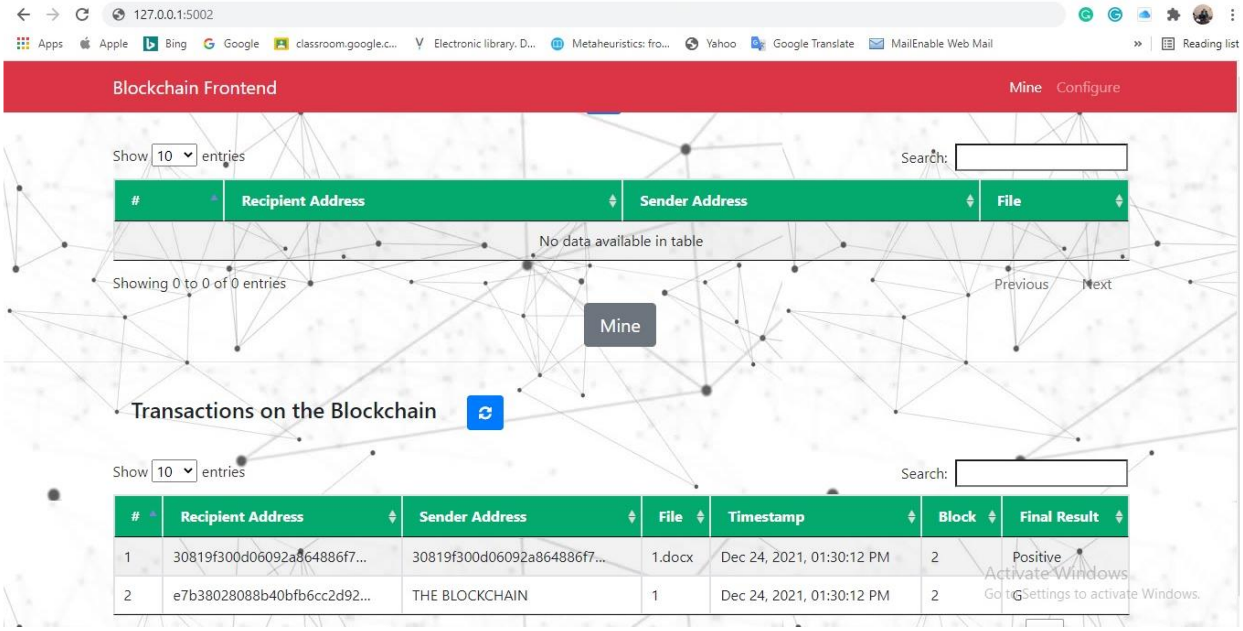
Transactions on the Blockchain

Show 10 entries Search:

#	Recipient Address	Sender Address	File	Timestamp	Block	Final Result
1	30819f300d06092a864886f7...	30819f300d06092a864886f7...	1.docx	Dec 24, 2021, 01:30:12 PM	2	Positive
2	e7b38028088b40bfb6cc2d92...	THE BLOCKCHAIN	1	Dec 24, 2021, 01:30:12 PM	2	G

Showing 1 to 2 of 2 entries Previous 1 Next

Figure 4.24:The first node that incubator for health care files based smart contract.



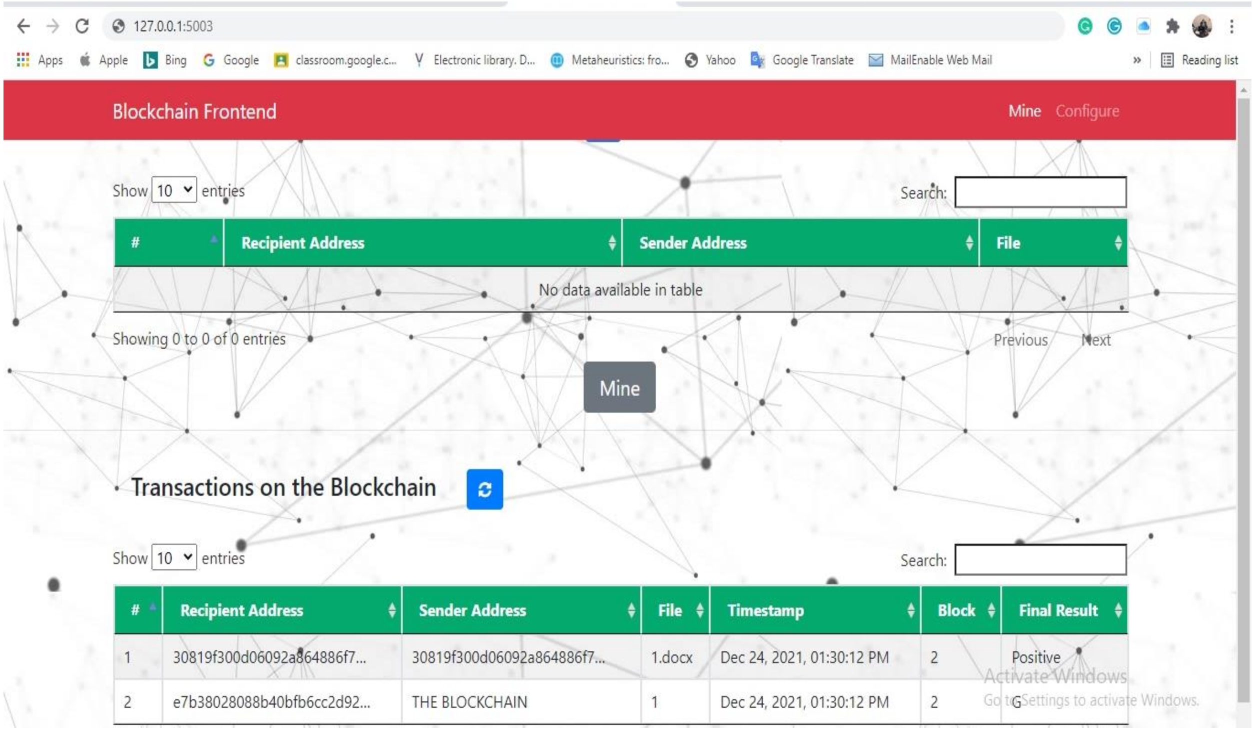
#	Recipient Address	Sender Address	File
No data available in table			

Showing 0 to 0 of 0 entries

Transactions on the Blockchain

#	Recipient Address	Sender Address	File	Timestamp	Block	Final Result
1	30819f300d06092a864886f7...	30819f300d06092a864886f7...	1.docx	Dec 24, 2021, 01:30:12 PM	2	Positive
2	e7b38028088b40bfb6cc2d92...	THE BLOCKCHAIN	1	Dec 24, 2021, 01:30:12 PM	2	G

Figure 4.25: The second node that incubator for health care files based smart contract.



#	Recipient Address	Sender Address	File
No data available in table			

Showing 0 to 0 of 0 entries

Transactions on the Blockchain

#	Recipient Address	Sender Address	File	Timestamp	Block	Final Result
1	30819f300d06092a864886f7...	30819f300d06092a864886f7...	1.docx	Dec 24, 2021, 01:30:12 PM	2	Positive
2	e7b38028088b40bfb6cc2d92...	THE BLOCKCHAIN	1	Dec 24, 2021, 01:30:12 PM	2	G

Figure 4.26: The third node that incubator for health care files based smart contract.

CHAPTER FIVE
CONCLUSIONS AND FUTURE WORKS

5.1 Conclusions

1. The proposed system that included applied NFV to the blockchain Giving a system with high throughput increased by 20%. with a good gain of time that decreased by 50%.

2. The throughput of three known algorithms and the proposed technique were compared using data of varying sizes. The results revealed that RSA had the optimum throughput in regards to encryption execution time and decryption execution time, respectively, when compared to DSA, ECC, and the suggested algorithm.

3. The proposed system that used the SHA algorithm The output bits of SHA-1, SHA-512, and SHA-256 are not equivalent as an outcome.

4. Two loops used with hash function, On localhost, the configuration is run, and the outputs of numerous samples are compiled and examined.

5. In proposed system the smart contract that had been developed had been very fast, had enough security for each of the nodes, and its speed decreased very gradually as the number of nodes increased.

6. In the proposed system, the smart contract is developed to work in synchronization with transfers files such as (pdf and images).

7. Built auto smart contract that work with all nodes, and execute automatically with virtual functions of blockchain.

8. The suggested system is thoroughly compared to the most popular blockchain systems on the basis of the tokens used, security, price, and smart contracts.

9. Virtual DLT speeds up transactions by about 120 transactions per second when compared to DLT.

10. A network of sixty nodes was constructed for the proposed system. A constant block size of 65 transactions per block and a transaction arrival rate of 77 transactions per second have been established.

11. Several experiments were carried out on a variety of data of varying sizes to determine how the hash impacts these data and the amount of CPU is

consumed. As a result, a comparison was made between SHA-1, SHA-256, and SHA-512 before and after the hash function was implemented in NFV.

12. Implementing a standard hash to encrypt the files in the virtual ledger, there was a discernible difference in the decrease in CPU utilization.

13. The asymmetric-keys, hash function, and Proof of Work had been used to secure the proposed system.

14. Testing of the proposed system's speed with FTP, Ethereum, and transactions with sizes up to 400 MB over an unspecified internet speed. As a result, a high rate of data transmission is achieved, which is greater than 25% of the speeds used in the remaining situations.

15. Blockchain-NFV for the healthcare system has been used with smart contract that deal with files and report results.

5.2 Future Works

While this dissertation attempts to accomplish a comprehensive study of a blockchain-NFV system, there is significant work and strategies to be accomplished.

1. Deeply examination of the blockchain system and application of NFV inside blockchain technology to get a virtual blockchain-NFV-cloud such as transmission data include many types such as video, audio, and applications files.
2. Blockchain technology on social networks will assist in resolving built-in issues like privacy violations, data control, or content validity. This technology will therefore continue to grow in popularity in social networking.
3. MedicalChain - Provides a blockchain-based method for developing a user-centric digital health record that may be distributed equally with doctors. All data is stored in a transparent, safe, and fully transparent state.
4. In the healthcare industry, data privacy is essential. Blockchain technology is therefore highly sought after in this country. There are also other

blockchain trends in healthcare besides the security of medical records. The development of medication supply chains is assisted by this technology.

5. Blockchain-NFV-based traceability environment ought to be experimented within a live environment to evaluate virtuality and the costs of executing and maintaining this environment**.**

References

[1] Wagdy, M., Babulak, E., & Al-Dabass, D. (2021). Network Function Virtualization over Cloud-Cloud Computing as Business Continuity Solution. Intechopen, Published: July 14th.

[2] Aljuhani, A., & Alharbi, T. (2017, January). Virtualized network functions security attacks and vulnerabilities. In 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 1-4). IEEE.

[3] ETSI, E. G. N. (2). V1. 1.1: Network Functions Virtualisation (NFV); Architectural Framework, 2013. URL: https://www. etsi. org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_NFV002v010 101p. pdf,[Accessed: May 7, 2020].

[4] Adoga, H. U., & Pezaros, D. P. (2022). Network Function Virtualization and Service Function Chaining Frameworks: A Comprehensive Review of Requirements, Objectives, Implementations, and Open Research Challenges. Future Internet, 14(2), 59.

[5] Pei, X., Telekom, D., Martiny, K., DOCOMO, N., Obana, K., Gamelas, A., ... & Lee, D. K. Network Functions Virtualisation (NFV).

[6] R. Vilalta, A. Mayoral, D. Pubill, R. Casellas, R. Martnez, J. Serra, C. Verikoukis, and R. Muoz, “End-to-end sdn orchestration of iot services using an sdn/nfv-enabled edge node,” in Proc. of Optical Fiber Comm. Conf. and Exhibition, March 2016, pp. 1–3.

[7] J. Batalle, J. F. Riera, E. Escalona, and J. A. Garcia-Espin, “On the implementation of nfv over an openflow infrastructure: Routing function virtualization,” in Future Networks and Services (SDN4FNS), IEEE SDN for. IEEE, 2013, pp. 1–6.

[8] Medhat, A. M., Taleb, T., Elmangoush, A., Carella, G. A., Covaci, S., & Magedanz, T. (2016). Service function chaining in next generation networks: State of the art and research challenges. IEEE Communications Magazine, 55(2), 216-223.

[9] Li, F., Lai, A., & Ddl, D. (2011, October). Evidence of advanced persistent threat: A case study of malware for political espionage. In 2011 6th International Conference on Malicious and Unwanted Software (pp. 102-109). IEEE

[10] P. Massonet, L. Deru, A. Achour, S. Dupont, L. M. Croisez, A. Levin, and M. Villari, “Security in lightweight network function virtualization for federated cloud and iot,” in Proc. of Int. Conf. on Future Internet of Things and Cloud (FiCloud), August 2017, pp. 148–154.

[11] Kaur, J., & Bahl, K. (2018). Cloud Computing–An on Demand Service Platform and Different Service Models. International Journal of Innovative Science, Engineering & Technology, 5(2), 92-96

[12] Kshetri, N. (2017a). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications policy, 41(10), 1027-1038.

[13] Mansfield-Devine, S. (2017). Beyond Bitcoin: using blockchain technology to provide assurance in the commercial world. Computer Fraud & Security, 2017(5), 14-18.

[14] Kshetri, N. (2017). Can blockchain strengthen the internet of things?. IT professional, 19(4), 68-72.

[15] Casado-Vara, R., Prieto, J., De la Prieta, F., & Corchado, J. M. (2018). How blockchain improves the supply chain: Case study alimentary supply chain. Procedia computer science, 134, 393-398.

[16] Balakrishna Reddy, G., & Ratna Kumar, K. (2020). Quality improvement in organic food supply chain using blockchain technology. In Innovative product design and intelligent manufacturing systems (pp. 887-896). Springer, Singapore.

[17] Dujak, D., & Sajter, D. (2019). Blockchain applications in supply chain. In SMART supply network (pp. 21-46). Springer, Cham.

[18] Trautman, L. J. (2016). Is disruptive blockchain technology the future of financial services?.

[19] Monem, M., Ahmad, A., Ahmed, R., & Arif, H. (2020, June). Efficient Blockchain System based on Proof of Segmented Work. In 2020 IEEE Region 10 Symposium (TENSYMP) (pp. 989-992). IEEE.

[20] Talukder, S., Roy, S., & Al Mahmud, T. (2019, January). An approach for an distributed anti-malware system based on blockchain technology. In 2019 11th International Conference on Communication Systems & Networks (COMSNETS) (pp. 1-6). IEEE.

[21] Rebello, G. A. F., Alvarenga, I. D., Sanz, I. J., & Duarte, O. C. M. (2019, May). BSec-NFVO: A blockchain-based security for network

function virtualization orchestration. In ICC 2019-2019 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[22] Yi, B., Wang, X., Li, K., & Huang, M. (2018). A comprehensive survey of network function virtualization. Computer Networks, 133, 212-262.

[23] Zhang, T., Qiu, H., Linguaglossa, L., Cerroni, W., & Giaccone, P. (2020). NFV platforms: Taxonomy, design choices and future challenges. IEEE Transactions on Network and Service Management, 18(1), 30-48.

[24] Linguaglossa, L., Lange, S., Pontarelli, S., Rétvári, G., Rossi, D., Zinner, T., ... & Bianchi, G. (2019). Survey of performance acceleration techniques for network function virtualization. Proceedings of the IEEE, 107(4), 746-764.

[25] Li, J., Altman, E., & Touati, C. (2015). A general SDN-based IoT framework with NVF implementation. ZTE communications, 13(3), 42-45.

[26] Balon, M., & Liau, B. (2012, October). Mobile virtual network operator. In 2012 15th International Telecommunications Network Strategy and Planning Symposium (NETWORKS) (pp. 1-6). IEEE.

[27] Ayankoya, F. Y., Agbaje, M. O., & Ohwo, B. O. (2019). Appraisal on Cloud Computing and Network Functions Virtualization. IJCSNS, 19(7), 38.

[28] Kuribayashi, S. I. (2019). Allocation of virtual firewall functions in NFV-based networks with minimum network cost. International Journal of Computer Networks & Communications (IJCNC) Vol, 11.

[29] Yu, F. R., & He, Y. (2019). A service-oriented blockchain system with virtualization. Trans. Blockchain Technol. Appl., 1(1), 1-10.

[30] Tripathi, G., Ahad, M. A., & Paiva, S. (2020, March). S2HS-A blockchain based approach for smart healthcare system. In Healthcare (Vol. 8, No. 1, p. 100391). Elsevier.

[31] Jain, P., Anand, A., Saria, M., Kumari, R., Bothra, P., & Sultana, M. (2020, June). A Prototype Proposal for AI based Smart Integrated Platform for Doctors and Patients. In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 998-1003). IEEE.

[32] Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A proposed solution and future direction for blockchain-based

heterogeneous medicare data in cloud environment. Journal of medical systems, 42(8), 1-11.

[33] Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: applying blockchain to securely and scalably share clinical data. Computational and structural biotechnology journal, 16, 267-278.

[34] Yong, B., Shen, J., Liu, X., Li, F., Chen, H., & Zhou, Q. (2020). An intelligent blockchain-based system for safe vaccine supply and supervision. International Journal of Information Management, 52, 102024.

[35] Nusrat, S. A., Ferdous, J., Ajmat, S. B., Ali, A., & Sorwar, G. (2019, December). Telemedicine system design using blockchain in Bangladesh. In 2019 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE) (pp. 1-5). IEEE.

[36] Krishnan, S., Balas, V. E., Golden, J., Robinson, Y. H., Balaji, S., & Kumar, R. (Eds.). (2020). Handbook of research on blockchain technology. Academic Press.

[37] Wallace, A. (2019). Protection of Personal Data in Blockchain Technology: An investigation on the compatibility of the General Data Protection Regulation and the public blockchain.

[38] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and informatics, 36, 55-81.

[39] Salapura, V. (2012, September). Cloud computing: Virtualization and resiliency for data center computing. In 2012 IEEE 30th International Conference on Computer Design (ICCD) (pp. 1-2). IEEE.

[40] Padilla Pinedo, J. (2020). Network Function Virtualization technologies applied to cellular systems (Master's thesis, Universitat Politècnica de Catalunya).

[41] Akyildiz, I. F., Lin, S. C., & Wang, P. (2015). Wireless software-defined networks (W-SDNs) and network function virtualization (NFV) for 5G cellular systems: An overview and qualitative evaluation. Computer Networks, 93, 66-79.

[42] Malik, M. I., Wani, S. H., & Rashid, A. (2018). Cloud computing-technologies. International Journal of Advanced Research in Computer Science, 9(2).

[43] Haber, M. J., Chappell, B., & Hills, C. (2022). Cloud computing. In Cloud Attack Vectors (pp. 9-25). Apress, Berkeley, CA.

[44] Thukral, M. K. (2021). Emergence of blockchain-technology application in peer-to-peer electrical-energy trading: A review. Clean Energy, 5(1), 104-123.

[45] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.

[46] Qiu, T., Liu, X., Li, K., Hu, Q., Sangaiah, A. K., & Chen, N. (2018). Community-aware data propagation with small world feature for internet of vehicles. IEEE Communications Magazine, 56(1), 86-91.

[47] Guo, H., & Yu, X. (2022). A Survey on Blockchain Technology and its security. Blockchain: Research and Applications, 100067.

[48] Antonopoulos, A. M. (2019). Mastering bitcoin (No. 1, pp. 1-xxxii). O'Reilly,.

[49] Savron, L. (2019). How blockchain technology could change our lives. Ursidae: The Undergraduate Research Journal at the University of Northern Colorado, 8(1), 10.

[50] Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). Blockchain: A distributed solution to automotive security and privacy. IEEE Communications Magazine, 55(12), 119-125.

[51] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.

[52] Liu, F., Fan, H. Y., & Qi, J. Y. (2022). Blockchain Technology, Cryptocurrency: Entropy-Based Perspective. Entropy, 24(4), 557.

[53] Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

[54] Shekhtman, L., & Waisbard, E. (2021). Engravechain: A blockchain-based tamper-proof distributed log system. Future Internet, 13(6), 143.

[55] Singhal, B., Dhameja, G., & Panda, P. S. (2018). How blockchain works. In Beginning blockchain (pp. 31-148). Apress, Berkeley, CA.

[56] Nadeem, S., Rizwan, M., Ahmad, F., & Manzoor, J. (2019). Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture. International Journal of Advanced Computer Science and Applications, 10(1), 288-295.

[57] Joshi, K., & Benson, T. (2016). Network function virtualization. IEEE Internet Computing, 20(6), 7-9.

[58] Han, B., Gopalakrishnan, V., Ji, L., & Lee, S. (2015). Network function virtualization: Challenges and opportunities for innovations. IEEE communications magazine, 53(2), 90-97.

[59] Alwakeel, A. M., Alnaim, A. K., & Fernandez, E. B. (2019, May). Toward a Reference Architecture for NFV. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6). IEEE.

[60] Rebahi, Y., S Ghamsi, M., Herbaut, N., Negru, D., M Comi, P., S Crosta, P., ... & Markakis, E. (2016). Virtual Network Functions Deployment between Business Expectations and Technical Challenges: The T-NOVA Approach. Recent Advances in Communications and Networking Technology (Formerly Recent Patents on Telecommunication)(Discontinued), 5(1), 49-64.

[61] Bari, M. F., Chowdhury, S. R., Ahmed, R., & Boutaba, R. (2015, November). On orchestrating virtual network functions. In 2015 11th international conference on network and service management (CNSM) (pp. 50-56). IEEE.

[62] Mijumbi, R., Serrat, J., Gorricho, J. L., Latre, S., Charalambides, M., & Lopez, D. (2016). Management and orchestration challenges in network functions virtualization. IEEE Communications Magazine, 54(1), 98-105.

[63] Roig, J. S. P., Gutierrez-Estevez, D. M., & Gündüz, D. (2019). Management and orchestration of virtual network functions via deep reinforcement learning. IEEE Journal on Selected Areas in Communications, 38(2), 304-317.

[64] Gonzalez, A. J., Nencioni, G., Kamisiński, A., Helvik, B. E., & Heegaard, P. E. (2018). Dependability of the NFV orchestrator: State of the art and research challenges. IEEE Communications Surveys & Tutorials, 20(4), 3307-3329.

[65] Venâncio, G., Garcia, V. F., da Cruz Marcuzzo, L., Tavares, T. N., Franco, M. F., Bondan, L., ... & P. Duarte Jr, E. (2021). Beyond VNFM: Filling the gaps of the ETSI VNF manager to fully support VNF life cycle operations. International Journal of Network Management, 31(5), e2068.

[66] Sechkova, T., Paolino, M., & Raho, D. (2018, June). Virtualized infrastructure managers for edge computing: Openvim and openstack comparison. In 2018 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB) (pp. 1-6). IEEE.

[67] Medhat, A. M., Taleb, T., Elmangoush, A., Carella, G. A., Covaci, S., & Magedanz, T. (2016). Service function chaining in next generation networks: State of the art and research challenges. IEEE Communications Magazine, 55(2), 216-223.

[68] Li, F., Lai, A., & Ddl, D. (2011, October). Evidence of advanced persistent threat: A case study of malware for political espionage. In 2011 6th International Conference on Malicious and Unwanted Software (pp. 102-109). IEEE.

[69] Lal, S., Taleb, T., & Dutta, A. (2017). NFV: Security threats and best practices. IEEE Communications Magazine, 55(8), 211-217.

[70] http://portal.etsi.org/NFV/NFV_White_Paper.pdf.

[71] Herbaut, N., Negru, D., Magoni, D., & Frangoudis, P. A. (2016, July). Deploying a content delivery service function chain on an SDN-NFV operator infrastructure. In 2016 International Conference on Telecommunications and Multimedia (TEMU) (pp. 1-7). IEEE.

[72] Elbouanani, S., El Kiram, M. A., & Achbarou, O. (2015, December). Introduction to the Internet of Things security: Standardization and research challenges. In 2015 11th International Conference on Information Assurance and Security (IAS) (pp. 32-37). IEEE.

[73] Bizanis, N., & Kuipers, F. A. (2016). SDN and virtualization solutions for the Internet of Things: A survey. IEEE Access, 4, 5591-5606.

[74] Fernandez, F., & Pallis, G. C. (2014, November). Opportunities and challenges of the Internet of Things for healthcare: Systems engineering perspective. In 2014 4th international conference on wireless mobile communication and healthcare-transforming healthcare through innovations in mobile and wireless technologies (MOBIHEALTH) (pp. 263-266). IEEE.

[75] Darwish, A., Hassanien, A. E., Elhoseny, M., Sangaiah, A. K., & Muhammad, K. (2019). The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. Journal of Ambient Intelligence and Humanized Computing, 10(10), 4151-4166.

[76] Darshan, K. R., & Anandakumar, K. R. (2015, December). A comprehensive review on usage of Internet of Things (IoT) in healthcare system. In 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT) (pp. 132-136). IEEE.

[77] Joyia, G. J., Liaqat, R. M., Farooq, A., & Rehman, S. (2017). Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain. J. Commun., 12(4), 240-247.

[78] Mohammed, A. H., Khaleefah, R. M., & Abdulateef, I. A. (2020, June). A review software defined networking for internet of things. In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-8). IEEE.

[79] Thilakarathne, N. N., Kagita, M. K., & Gadekallu, T. R. (2020). The role of the internet of things in health care: a systematic and comprehensive study. Available at SSRN 3690815.

[80] Massonet, P., Deru, L., Achour, A., Dupont, S., Croisez, L. M., Levin, A., & Villari, M. (2017, August). Security in lightweight network function virtualisation for federated cloud and IoT. In 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 148-154). IEEE.

[81] Al-Shaboti, M., Welch, I., Chen, A., & Mahmood, M. A. (2018, May). Towards secure smart home iot: Manufacturer and user network access control framework. In 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA) (pp. 892-899). IEEE.

[82] AbdelSalam, A. M., Elkilani, W. S., & Amin, K. M. (2014). An automated approach for preventing ARP spoofing attack using static ARP entries. International Journal of Advanced Computer Science and Applications, 5(1).

[83] ETSI, “Network functions virtualisation white paper,” SDN and OpenFlow World Congress, 2013.

[84] Gember, A., Akella, A., Anand, A., Benson, T., & Grandl, R. (2012). Stratos: Virtual middleboxes as first-class entities.

[85] Jiang, J. W., Lan, T., Ha, S., Chen, M., & Chiang, M. (2012, March). Joint VM placement and routing for data center traffic engineering. In 2012 Proceedings IEEE INFOCOM (pp. 2876-2880). IEEE.

[86] Meng, X., Pappas, V., & Zhang, L. (2010, March). Improving the scalability of data center networks with traffic-aware virtual machine placement. In 2010 Proceedings IEEE INFOCOM (pp. 1-9). IEEE.

[87] Jain, S., Kumar, A., Mandal, S., Ong, J., Poutievski, L., Singh, A., ... & Vahdat, A. (2013). B4: Experience with a globally-deployed software defined WAN. ACM SIGCOMM Computer Communication Review, 43(4), 3-14.

[88] Sekar, V., Egi, N., Ratnasamy, S., Reiter, M. K., & Shi, G. (2012). Design and implementation of a consolidated middlebox architecture. In 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12) (pp. 323-336).

[89] Gember, A., Prabhu, P., Ghadiyali, Z., & Akella, A. (2012, October). Toward software-defined middlebox networking. In Proceedings of the 11th ACM Workshop on Hot Topics in Networks (pp. 7-12).

[90] Martins, J., Ahmed, M., Raiciu, C., Olteanu, V., Honda, M., Bifulco, R., & Huici, F. (2014). {ClickOS} and the Art of Network Function Virtualization. In 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14) (pp. 459-473).

[91] Vilalta, R., Mayoral, A., Muñoz, R., Casellas, R., & Martínez, R. (2015, April). The SDN/NFV cloud computing platform and transport network of the ADRENALINE testbed. In Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft) (pp. 1-5). IEEE.

[92] Briscoe, B. (2014). Network functions virtualisation (NFV)-NFV security: Problem statement. White paper, ETSI NFV ISG.

[93] Firoozjaei, M. D., Jeong, J. P., Ko, H., & Kim, H. (2017). Security challenges with network functions virtualization. Future Generation Computer Systems, 67, 315-324.

[94] Chaudhuri, A., Ferrer, H., Prafullchandra, H., Sherry, J., Ng, K., Xiaoyu, G., ... & Por, H. Y. (2015). Best practices for mitigating risks in virtualized environments. Cloud Security Alliance.

[95] Gervais, A., Ritzdorf, H., Karame, G. O., & Capkun, S. (2015, October). Tampering with the delivery of blocks and transactions in bitcoin. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 692-705).

[96] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future generation computer systems, 88, 173-190.

[97] el houda Nouar, N., Yangui, S., Faci, N., Drira, K., & Tazi, S. (2021). A Semantic virtualized network functions description and discovery model. Computer Networks, 195, 108152.

[98] Kiran, N., Liu, X., Wang, S., & Yin, C. (2021). Optimising resource allocation for virtual network functions in SDN/NFV-enabled MEC networks. IET Communications, 15(13), 1710-1722.

[99] Shrimali, B., & Patel, H. B. (2021). Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. Journal of King Saud University-Computer and Information Sciences.

[100] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. arXiv preprint arXiv:1906.11078.

[101] King, S. T., & Smith, S. W. (2008). Virtualization and security: Back to the future. IEEE Security & Privacy, 6(5), 15-15.

[102] Salapura, V. (2012, September). Cloud computing: Virtualization and resiliency for data center computing. In 2012 IEEE 30th International Conference on Computer Design (ICCD) (pp. 1-2). IEEE.

[103] Morabito, R., Cozzolino, V., Ding, A. Y., Beijar, N., & Ott, J. (2018). Consolidate IoT edge computing with lightweight virtualization. IEEE network, 32(1), 102-111.

[104] Han, B., Gopalakrishnan, V., Ji, L., & Lee, S. (2015). Network function virtualization: Challenges and opportunities for innovations. IEEE communications magazine, 53(2), 90-97.

[105] Georgiadis, E. (2019). How many transactions per second can bitcoin really handle? Theoretically. Cryptology ePrint Archive.

[106] Li, A., Wei, X., & He, Z. (2020). Robust proof of stake: A new consensus protocol for sustainable blockchain systems. Sustainability, 12(7), 2824.

[107] https://bitcoinops.org/en/tools/calc-size/

[108] Harsha, A., & Patil, B. (2016). A Review: Security of Data in Cloud Storage using ECC Algorithm. Bonfring International Journal of Software Engineering and Soft Computing, 6(Special Issue Special Issue on Advances in Computer Science and Engineering and Workshop on Big Data Analytics Editors: Dr. SB Kulkarni, Dr. UP Kulkarni, Dr. SM Joshi and JV Vadavi), 143-146.

[109] Kaleem, M., Mavridou, A., & Laszka, A. (2020, September). Vyper: A security comparison with solidity based on common vulnerabilities. In 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) (pp. 107-111). IEEE.

[110] Zaghloul, E., Li, T., Mutka, M. W., & Ren, J. (2020). Bitcoin and blockchain: Security and privacy. IEEE Internet of Things Journal, 7(10), 10288-10313.

[111] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). Ieee.

[112] SriBalaji, Vignesh Mohan, Soundarya, "Secure and Decentralized File Transfer Application using Blockchain" , http://troindia.in/journal/ijcesr/vol4iss4/169- 175.pdf.

[113] Vujičić, D., Jagodić, D., & Ranđić, S. (2018, March). Blockchain technology, bitcoin, and Ethereum: A brief overview. In 2018 17th international symposium infoteh-jahorina (infoteh) (pp. 1-6). IEEE.

[114] Lindroos, S., Hakkala, A., & Virtanen, S. (2021). A systematic methodology for continuous WLAN abundance and security analysis. Computer Networks, 197, 108359.

[115] Chen, H., Pendleton, M., Njilla, L., & Xu, S. (2020). A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. ACM Computing Surveys (CSUR), 53(3), 1-43.

المستخلص

في أطروحتنا ، تم بناء سلسلة الكتل خاص للتغلب على جانب الأمان من خلال شبكة مشاركة ملفات آمنة. يمكن استخدام سلسلة الكتل الخاص في مؤسسات مختلفة. يتم الحصول على مستوى عالٍ من الأمان من خلال استخدام تقنيات مهمة تأخذ في الاعتبار جزءًا مهمًا من مجال التشفير لتشفير الملفات بقوة. يضمن هذا الأخير عدم قدرة أي فرد باستثناء المتلقي على الوصول إلى الملفات. كذلك ، تم الحصول على سرعة كافية عند نقل الملفات ، مقارنة بـ الايثيريوم مع بروتوكول نقل الملفات. بعد ذلك ، تم تصميم العقود الذكية لتناسب نقل الملفات بين العقد.

يتم تقديم طريقة جديدة لإضفاء الطابع الافتراضي على عمل سلسلة الكتل استنادًا إلى المحاكاة الافتراضية لوظيفة الشبكة مع العمل التلقائي للعقد الذكي بين العقد الافتراضية القائمة على الحوسبة السحابية. من خلال دمج المحاكاة الافتراضية لوظيفة الشبكة مع سلسلة الكتل، تم التغلب على جميع التحديات المذكورة أعلاه من خلال الانتقال إلى بيئات البرامج من خلال إنشاء العقد الافتراضية ، بالإضافة إلى التفاعل السلس فيما بينها وإدارة المعاملات بين العقد والعملاء ، مما يشير إلى إدارة الشبكة المثالية. من خلال العمل المقترح ، يتم الحصول على إنتاجية تصل إلى 20٪ من خلال تطبيق المحاكاة الافتراضية لوظيفة الشبكة مقارنة بعدم تطبيق المحاكاة الافتراضية لوظيفة الشبكة على سلسلة الكتل . بالإضافة إلى ذلك ، يتم التخلص من تكاليف الأجهزة وفي النهاية يتم استخدام بيئة آمنة تبعد النظام عن الهجمات الافتراضية.

نقدم عينة فريدة تحتوي على (المحاكاة الافتراضية لوظيفة الشبكة- سلسلة الكتل) المرخصة للتعامل مع السجلات الصحية الإلكترونية واحتفاظها بتقرير المرضى. تضمن هذه التقنية الشفافية والثبات على وجه التحديد، وهما أمران ضروريان للإدارة والتخزين المحمية، مما يضمن أسلوبًا منظمًا جيدًا بشكل مشترك فيما يتعلق بالأطباء والمرضى بالإضافة إلى ذلك، وبتفاؤل، يجلب الثقة فيما يتعلق بسيناريو الصحة العامة. أيضًا، الغرض المطلوب هو أن مهمتنا قدمت لتحقيق سرعة نظام سلسلة الكتل إلى السجلات الصحية الإلكترونية وتشجيع المناقشات المختلفة مع المنظمات الصحية للاستفادة الكاملة من إمكانية التكنولوجيا المذكورة.

جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة بابل- كلية تكنولوجيا المعلومات

قسم البرمجيات

وظيفة الشبكة الافتراضية لتطوير سلسلة الكتل في الحوسبة السحابية

أطروحة مقدمة

الى مجلس كلية تكنولوجيا المعلومات في جامعة بابل وهي جزء من متطلبات نيل درجة الدكتوراه فلسفة في تكنولوجيا المعلومات – برمجيات

من قبل

حيدر عبد الستار ناهي عبد عون

إشراف

أ.م. د. الحارث عبد الكريم عبد الله

2022 م

1443 هـ