Ministry of Higher Education
And Scientific Research
University of Diyala
College of Science
Department of
Computer Science

Design of Authorization Technique in Simulation Environment Blockchain

A Thesis

Submitted to College of Science/ University of Diyala in a Partial Fulfillment of the requirements for the Degree of Master in computer Science

By

Wasan Ahmed Ali

Supervised by

Naji M. Sahib
Professor

Dr.Jumana Waleed
Assistant Professor

2020 A.D. **1441 A.H.**

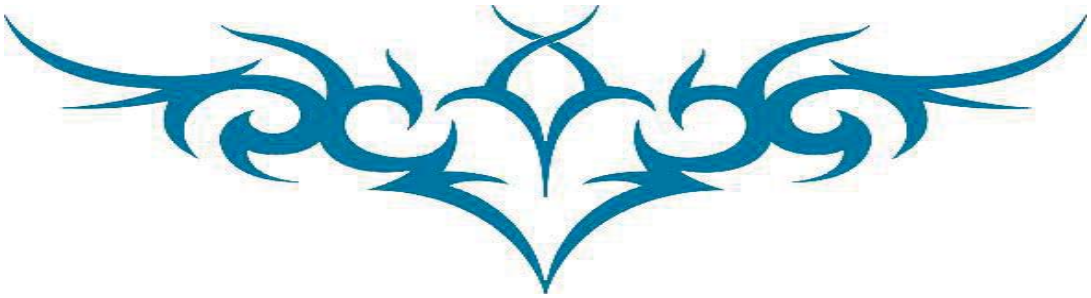
بسم الله الرحمن الرحيم

﴿ وَلِيَعْلَمَ الَّذِينَ أُوتُوا الْعِلْمَ أَنَّهُ الْحَقُّ مِن رَّبِّكَ فَيُؤْمِنُوا بِهِ فَتُخْبِتَ لَهُ قُلُوبُهُمْ وَإِنَّ اللَّهَ لَهَادِ الَّذِينَ آمَنُوا إِلَى صِرَاطٍ مُّسْتَقِيمٍ ﴾

صدق الله العظيم

سورة الحج

اية (54)



Dedication

And he has the first and last credit for lighting my way..... God Almighty

To those who said among them, "And lower them to the wing of humiliation of mercy, and say, My Lord, (24) have mercy on them as my little Lord" (Al-Israa)

".They are buried underneath. "Mom ... and Dad

To those who gave me a lot of giving and motivation ... ... my brothers ... and my sisters.

To those who foad my rhetoric and my life..... "My family".

To the sincere hands that helped me and shared me in fatigue and ignited the light of hope and will ..... my dear teachers.

Wasan Ahmed. Ali

Publication Papers

Wasan A.Ali, Naji M. Sahib, Jumana Waleed "The Preservation of authentication and authorization on the blockchain" "2019 2nd international Iraqi conference on engineering technology and its Applications (2nd IICETA)", Al-Najef, Iraq, 2019, pp, 83-88.

Acknowledgments

First and last, I thank God Almighty, who has helped me to finish this study first. And I extend my sincere thanks and gratitude to everyone who helped me and lend a hand to me. In the forefront of whom is the professor, the distinguished professor, "***Naji Matar Sahib"*** and Dr. "***Jumana Waleed*** " Who supervised this research, and their good guidance, valuable comments, and decent treatment have had a great impact on the research reaching this image.....

I also extend my sincere thanks and appreciation to all those who contributed and helped in the success and completion of this study of teachers and professors...

And to the department staff and all of my colleagues who did not strive to help me during the period of completing this study.

Wasan Ahmed. Ali

Linguistic Certification

This is to certify that this research entitled ***"Design of Authorization Technique in Simulation Environment Blockchain"*** *was prepared my linguistic supervision. It was amended to meet the style of English language.*

Signature:

Name: *Asst. Prof. Dr. Salam A. Noman.*

Date: / /2020

Scientific Certification

This is to certify that this research entitled ***"Design of Authorization Technique in Simulation Environment Blockchain"*** *was prepared my scientific supervision. It was amended to meet the style of scientific formula.*

Signature:

Name: *Asst. prof. Dr. Nada H. Mohamed Ali.*

Date: / /2020

Supervisor's Certification

We certify that this research entitled ***"Design of Authorization Technique in Simulation Environment Blockchain"*** was prepared by (***Wasan Ahmed Ali)*** under our supervisions at the University of Diyala collage of Science Department of Computer Science, as a partial fulfillment of the requirements needed to award the degree of Master of Science in Computer Science.

(Supervisor) **(Supervisor)**

Signature: **Signature:**

Name: ***Prof. Naji M. Suhaib***. **Name:** ***Asst. Prof. Dr. Jumana W. Salih***

Date: / /2020 **Date: / /2020**

Approved by University of a Diyala collage of Science Department of Computer Science.

Signature:

Name: *Assist. Prof. Dr. Taha M. Hassan.*

Date: / / 2020.

(Head of Computer Science Department)

Examination Committee Certification

We certify that we have read this research entitled "***Design of Authorization Technique in Simulation Environment Blockchain***", and as an examining committee, examined the student "***Wasan Ahmed Ali"*** in its contents and that in our opinion, it is adequate as fulfill the requirements for the Degree of Master in Computer Science at the Computer Science Department, University of Diyala.

(Chairman)

Signature:

Name: ***Prof. Dr. Ziyad T. Mustafa***

Date: / /2020

(Member)

Signature:

Name: ***Prof Dr. Taha M. Hassan***

Date: / /2020

(Member)

Signature:

Name: ***Asst. Prof. Ahmed Salih Ahmed***

Date: / /2020

(Member/ Supervisor)

Signature:

Name: ***Prof. Naji M. Suhaib.***

Date: / /2020

(Member / Supervisor)

Signature:

Name: ***Asst. Prof. Dr. Jumana W. Salih***

Date: / /2020

Approved by the Dean of College of Science, University of Diyala.

(The Dean)

Signature:

Name: *Prof. Dr. Tahssen Hussein Mubarak*

Date: / /2020

Abstract

The massive growth of data and all applications used on networks requires great security and safety. Blockchain technology is a static and shared database that is not controlled by any third party. Blockchain technology can be combined with a variety of other technologies as it enters the digital, physical, and biological fields. Also; Authentication is an issue that needs to be thoroughly verified to be authenticated regardless of the traditional authentication methods used to prove that the person is authorized on it. In this thesis design Blockchain system is proposed to simulate each node in the system. The propose system of design Authorization technique in simulation environment blockchain named (ASBchain) consists of six stages to verify the transactions transmitted by user after the registration process, which based on the strong Rivest Shamir Adleman algorithm(RSA) for signature transaction and Secure Hash Algorithm 256. Then verified from any transaction performed based on matching hash function values that sending .Thus, the proposed system can prove that the sender is authorize by authorization process. This is done according to the value of the last hash function for block maintained by this sender based on the time stamp of it. The system was tested in terms of time for each stage and the phases were compared with each other and show that the time spent on Registration ,authentication, and Authorization processes were (00:01:43:0059 s), (00:01:02.0953 s) and (00:01:00.0102 s) respectively for 100 users. The system has proven that all people have equal rights in reliability and use the system. But not every person is authenticate do he is authorized. It is a collaborative environment and the main thing is reliability, safety, decentralization.

List of Contents

ACKNOWLEDGMENTS.....**I**

ABSTRACT.....**II**

List of Contents.....**III**
List of figures.....**VI**
List of Tables.....**VIII**
List of Algorithms.....**IX**
List of Abbreviations.....**X**

CHAPTER ONE Introduction…….……..……..… (1-9)

1.1 Overview…….……1
1.2 Related Work…..…….……4
1.3 Problem Statement …….……8
1.4 Aim of the Thesis ……..…….……9
1.5 Thesis Organization…….....9

CHAPTER TWO Theoretical Background ……..….. (10-40)

2.1 Blockchain Technology ……....10
2.1.1 Peer-to-Peer (P2P) Network …….……..……13
2.1.2 Block …….……13
2.1.3 Transaction …….……14
2.1.4 Ledger …….…….…….……..15
2.2 Blockchain Structure…….…….…….16
2.3 Distributed Blockchain……...17
2.4 Blockchain Security …….…..17
2.4.1 Cryptographic Hash Function ……17
2.4.2 Digital signature ……..21
2.4.3 Merkle Tree ……....22
2.5 Categorization of Blockchain system. …….....23
2.6 Distributed Consensus …….……..25
2.6.1 Proof-of-work …….……25
2.6.2 Proof-of-stake …….……26
2.7 Blockchain work…….....26

2.8 Authentication ……..29
2.8.1 Fingerprint Biometric……...29
2.8.1.1 Feature Extraction by Invariant Moment……31
2.8.2 Linear Congruential Generator (LCG)……..32
2.8.3 BigInteger ……..…….....32
2.8.4 Rabin Miller Algorithm ……..……33
2.8.2 RSA Algorithm ……35
2.9 Authorization ……36
2.10 Potential Vulnerabilities ……..…….…….…..…37
2.11 Blockchain Applications ……..……...……38
2.11.1 Financial Applications……...38
2.11.2 Non Financial Applications……...39

CHAPTER THREE The Proposed Design Of Authorization Technique In Simulation Environment Blockchain System…….…… (41-62)

3.1 Introduction ……..41
3.2 The block diagram of the ASBchain Proposed System ……41
3.3 The Proposed System ……..……43
3.3.1 Registration stage ……..……..……43
3.3.1.1 User Request for Great Transaction Step……....43
3.3.2 Authentication Stage…….……52
3.3.3 Builder Merkle Tree Stage……....54
3.3.4 Great Blocks stage……57
3.3.5 Authorization phase ……..……59
3.3.6 Linking Block to ASBchain System Stage……....61

CHAPTER FOUR Experimental Result and Evaluation……..…….…… (63-94)

4.1 Introduction…….…….....63
4.2 Initialization ……...63
4.3 Implementation of the proposed system…….…….…..……...63
4.3.1 Implementation of Registration…….....64
4.3.2 Implementation of Authentication……...….64
4.3.3 Implementation of the Builder Merkle Tree Stage…….…..…65
4.3.4 Implementation of the Create Blocks Stage……66
4.3.5 Implementation of the Authorization Stage……...……..67

4.3.6 Implementation of the Linking Blocks to ASBchain Stage…….67
4.4 Results of the Proposed ASBchain Network……..…...68
4.4.1 Results of Registration Stage…….…..…68
4.4.2 Results of Authentication Stage…….……83
4.4.3 Results of Builder Merkle Tree Stage…….…88
4.4.4 Results of Create Blocks Stage……..…..…89
4.4.5 Results of Authorization Stage……...90
4.4.6 Results of Linking Block to ASBchain Network Stage…..…..……92
4.5 Comparison between Three stages of the ASBchain System based On Total Execution Time……93

CHAPTER FIVE Conclusions and Suggestions for Future Work……..……. (95-98)

5.1 Introduction……95
5.2 Conclusions ……..…….……..…95
5.3 Suggestions for Future Works …….……..……97

REFERENCES……..……..,,….... (99-103)

List of Figures

Figure (1.1): Basic block diagram of Blockchain……3
Figure (2.1): Network view of a Blockchain ……..12
Figure (2.2): Block structure (Generalized) ……...14
Figure (2.3): Generic chain blocks ……16
Figure (2.4): The interdependence of blocks ……..19
Figure (2.5): A single round of SHA256 function……..….21
Figure (2.6): Digital signature scheme …….……..……22
Figure (2.7): An example of Merkle tree ……23
Figure (2.8): Public Blockchain……..…24
Figure (2.9): Consortium Blockchain ……24
Figure (2.10): Private Blockchain ……..…25
Figure (2.11): Basic components of Blockchain ……27
Figure (2.12): How Blockchain work ……..…28
Figure (2.13): Ridges and valleys……....30
Figure (3.1): Block diagram of the Proposed ASBchain Network…….42
Figure (3.2): Block diagram of Generating Transaction Step……44
Figure (3.3): Example of Apply XOR Boolean Operation between 7 Moments Features M for User……....47
Figure (3.4): Example of the SHA-256 Hash Algorithm Step……48
Figure (3.5): Cryptography Process of Generate Transaction Stage…...52
Figure (3.6): Flowchart of the Authentication Transaction…….53
Figure (3.7): Merkle Tree with Even Number of Transaction Case……56
Figure (3.8): Merkle Tree with Odd Number of Transaction Case…….56
Figure (3.9): Example of the Create Block Stage……58
Figure (3.10): Flowchart of the Authorization Stage…….....60
Figure (3.11): Example of the Linking Blocks to ASBchain Network Stage……62
Figure (4.1): Implementation of Registration Stage……64
Figure (4.2): Implementation of Authentication Stage……65
Figure (4.3): Implementation of Builder Merkle Tree Stage……66
Figure (4.4): Implementation of Create Block Stage……..66
Figure (4.5): Implementation of the Authorization Stage……...67
Figure (4.6): Implementation of the linking blocks to ASBchain Stage……...68

Figure (4.7): Comparison between Case1 & Case2 based on No. (True)& No. (False)…….….76
Figure (4.8): Execution Time for each Signature of User Transaction in (Sec)……....80
Figure (4.9): Execution Time in Second for Create 10 Transaction…...83
Figure (4.10): Execution Time in Second of the Check Authentication of 10 Transaction…….…….87
Figure (4.11): Execution Time in Second of the Check Authentication of 100 Transaction…….....87
Figure (4.12): Execution time (in second) for check authorization of the 10 User request…….…..91
Figure (4.13): Execution time (in second) for check authorization of the 100 User request……...92
Figure (4.14): Execution time (in second) for three stages: Registration, Authentication, and Authorization…….…….94

List of Tables

Table (3.1): Hu's 7 Moments Feature of the One User……45
Table (3.2): Example of Truncate step of generate NewF……...46
Table (4.1): Original 7 Moment Feature of Fingerprint Image Data Set.69
Table (4.2): Result of Generate (NewF) for 10 users……..70
Table (4.3): Result of Generate (NewF) for 5 users……72
Table (4.4): Result of Generate SHA-256 Hashing of New Moment Feature……73
Table (4.5): Results of Generate Prim No. with Miller - Rabin Prime Test…….....74
Table (4.6): Results of Generate Prim No. with Miller - Rabin Prime Test …….....75
Table (4.7): Comparison of the Result of Rabin Miller Test based on No. (True) and No. (False)……..……76
Table (4.8): Result of Create Pair of Key, when user=10and key Size=1024……...77
Table (4.9): Result of Create Pair of Key, when user=5 and key size=250 ……..……78
Table (4.10): User signature using RSA algorithm with execution time In (Second)……78
Table (4.11): User Transaction with Execution Time in Second…….81
Table (4.12): Result of Authentication Stage……84
Table (4.13): Result of Merkle Tree for 8 (even) Transactions……..88
Table (4.14): Result of Merkle Tree for 7(odd) Transactions…….89
Table (4.15): Result of create blocks……..90
Table (4.16): Result of Authorization Stage……..…….90
Table (4.17): Result of Linking Block to ASBchain Network……...92
Table (4.18): Total Execution Time……93

List of Algorithms

Algorithm (2.1): SHA256 Algorithm……..19

Algorithm (2.2): Rabin miller Algorithm……34

Algorithm (2.3): RSA Algorithm…….…...35

Algorithm (3.1): Generating Public Key (P) based on LCG method…..49

Algorithm (3.2): Implemented RSA Algorithm…….....51

Algorithm (3.3): Authentication stage based on RSA algorithm……....54

Algorithm (3.4): Builder Merkle Tree Stage……...55

Algorithm (3.5): Authorization Stage…….59

List of Abbreviations

$\oplus$	XOR Gate.
ASBchain	Authorization Simulation on Blockchain.
Ethash	Etherum Algorithm.
H	Hash value.
HMT	Hash Merkle Tree.
ID	Identifier.
LCG	Linear Congruential Generators.
NewF	New Moment Feature.
NH	New hash
P2P	Peer 2 Peer network.
POS	Proof of Stake.
POW	Proof of Work.
Prev-hash	Previous Hash**.**
RSA	Rivest, Shamir and Adleman.
SHA256	Secure Hash Algorithm 256.
STR	Sender to Receiver.
T	Transaction.
M	Moment Feature.

Chapter One

Introduction

Chapter One

Introduction

1.1 Overview

The new technologies such as video and voice calls, pictures, emails, and messages permit individuals to communicate directly. These technologies are used to travel directly from the transmitter to the recipient through the internet with keeping the trustworthy between individuals no matter how far apart they are. Nevertheless, if it related to money, individuals should trust a third party to be capable of completing the transaction [1].

So in order to create a digital identity, the users should have to register at the server. Here the users must supply personal sensitive data, user-name, email, phone number, and the details of a credit card. These data are kept on the centralized server across data multicenter. Also; the users must create multiple-identities across multiple-suppliers to access their services. Studies have shown that this procedure of creating multi-identities is cumbersome and inconvenient since the users must be repeated the same process of registration many times and remember the passwords for various services. But these data are vulnerabilities to attacking, and the centralized servers of the suppliers are targets for hackers as primly [2].

Blockchain technology is a relatively new approach to information technology. The first application of blockchain technology is bitcoin which is used in financial exchange [3]. Blockchain technology was adverted in 2008 by Satoshi Nakamoto's white paper [4]. The work of

Satoshi Nakamto present a solution to the issues which implement and use digital currency, particularly, the double spending issue [3].

Blockchain gives an open decentralized database to any transaction including value like goods, and money. Consequently, the technology of blockchain has been started to slowly invade the internet as a guaranteed substitutional digital model by utilizing cryptography and mathematics [1].

The technology of blockchain has several basic properties; decentralization, transparency, shared ledger based on consensus, immutability, and privacy. Here, it can realize the needed features for authentication and authorization such as secure, decentralized, anonymity [5].

Although the basic features of blockchain that may bring us more reliable, secure, and convenient services, The security problems and challenges of this innovative technique is also a necessary topical that we need to concern it [6].

For a user to join the permission blockchain, there is the need for membership authentication. The researchers have been worked on improving privacy during authentication through depending authentication on attributes, instead of identities. It is confirmation of identity which the entity claims utilizing credentials [7]. Authentication systems are used biometric characteristics that are unique for each entity. The basic feature of the biometrics is that the entity has always with a way to authenticate himself. For example, you can forget a password or may be stolen an access card that you have. But in reality, you cannot forget your fingerprint, your signature, your gait. Biometric is more process as to remember several passwords for the user. So it can be used

to verify the identity of the person because these characteristics are unique for each user. Also, it is difficult to restore their production and it is impossible to exchange it [6]. The process of authentication is used to determine the user's validity who supposed to be. The process of authorization is to determine which resources the user is allowed to access. Authorization determines the permissions of users in concepts of access to and use of resources to create some actions such as append, update, delete, etc. but not every person is right authenticated is authorizer , this via according to some rules based on it [8].

The Technology of Blockchain could be described as a public ledger and every transaction is stored in a block as a list of transactions [9].Figure (1.1) explains the basic block diagram of Blockchain which will explain the components of the block in detail in the next chapter. [10].

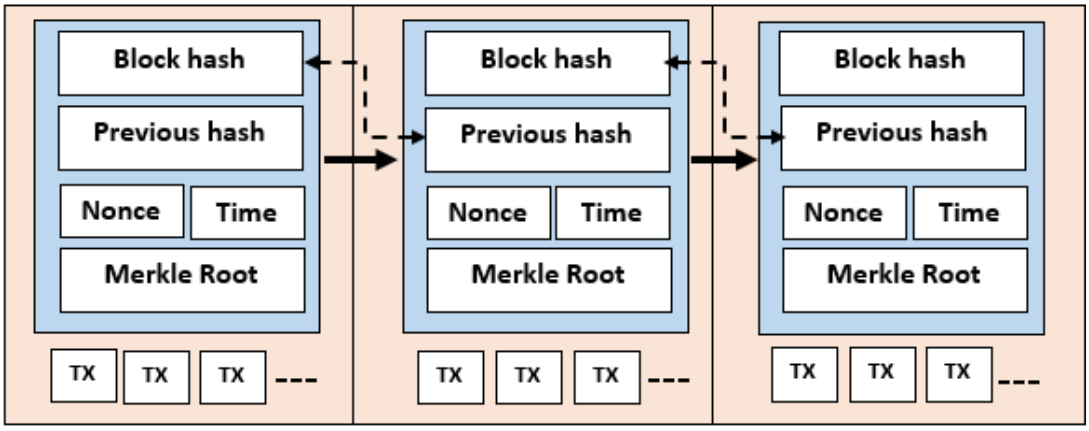


Figure (1.1): A basic block diagram of Blockchain [10].

Therefore, this thesis concentrates on how to prove that a person is authenticated by all of the network and without relying on a central party in a safe and transparent manner, and how to prove that he is authorized

on the network. So here will design and implement system work on blockchain technology called ASBchain system based on secure hash algorithm (SHA256) and strong cryptography RSA Algorithm. It is consisting of three stages Registration, Authentication, Authorization, with each stage have several steps to reach the desired goal. This thesis is dealing with a prototype system. The main objective of the thesis is to understand how blockchain works and how can prove sender is authenticated and authorized consecutively without depending on third party.

1.2 Related Work

Several previous studies suggested by numerous investigators about the Blockchain network. Several studies and researchers that can related their works to the suggested scheme in this thesis:-

- In (2017), Chen, Z., & Zhu, Y. [5] showed how the Personal Archive Service System using Blockchain Technology works and what's different between traditional Third-party verification agencies. Their main contribution is to present a framework of utilizing the technology of Blockchain to exploit its desirable features for building a personal archive that associated certifications. There is no need for Inquisitors. A subject is capable of deciding what to reveal to when and who depending on the request nature.
- In (2017), Grech, A., & Camilleri, A. F. [12]. Proposed a technique that can access to a student's personal information by using blockchain via using biometric identification on a smartphone. Every service from these services would be capable of identifying the student with no requirement for asking for or storing any private data again. Meaning that the right student is the only one who can

hold data. Also, the organization does not need to run complicated systems for accessing rights. It just requires securing the network or device where the verifications initial verification is performed. This would provide considerable resources spent in hardening the network contra data breaches.

- In (2017), Kikitamara, et al [13]. Analyzed the utilization of blockchain in digital identity as one of the steps for building an open model system. The digital identity and Blockchain introduce a system for preserving people's credentials for their public services. The management of digital identity combined with the technology of blockchain delivers decentralized online identities. Whereat Blockchain's implementation in the management of a digital identity leads to different properties (entity, attribute ...) especially needed on the authentication technique. And they used a handshake mechanism that includes procedures involving a public key infrastructure PKI verification mechanism.
- In (2017) Xia, Qi, et al. [14]. They proposed a blockchain-based data-sharing framework that adequately addresses the access control challenges associated with sensitive data stored in the cloud using the static characteristics and independence built into the blockchain. Their system is based on an authorized blockchain that allows access only to invited users, and thus authorized users. As all users are already known and a record of their actions is kept by the blockchain. The system allows users to request data from the shared pool after which their identities and encryption keys are verified.

- In (2017), Moinet, et al. [15] proposed an application for the blockchain as secured decentralized storage for cryptographic keys, in addition to trust information in the independent Wireless Sensor Networks concept. The authors showed how The Blockchain Authentication and Trust module and the human-like knowledge-based trust model demonstrate how to use blockchain persistence to provide solutions to high-level issues in the decentralized ad hoc networking space. More accurate, they showed the capability of building solutions supplying mechanisms of authentication, in addition to trust evaluation in an evaluative and self-organized network.
- In (2017), Hammudoglu, J. S., et al [16]. They have created a biometric mobile authentication system that relies only on local processing, as their open-source Android solution explores the ability of current smartphones to acquire, process and match fingerprints using only their embedded devices. Independently, it does not require any cloud service, server, or authorized access to fingerprint readers. It includes three main stages, obtaining fingerprints, obtaining fine detail features and matching with other fingerprints stored locally, and this made them able to capture and process a fingerprint in a matter of seconds using blockchain technology. This work is specifically designed to be the building block for a self-governing identity solution and integration with the unauthorized blockchain for identity proof and key certification.
- In (2018), Gao, et al.[17].They proposed a system that verifies the original data stored on a blockchain network that reflects the actual reliability of the data, in particular the information provided by the

persons involved in the exchange of the goods. They proposed the BlockID system, which provides a framework that verifies the ID issued by the government institution in a digital certificate, through user authentication based on biometrics, which is also associated with the smartphone. They have analyzed security in their BlockID system and have shown that it meets the purpose of confidentiality and safety but the system cannot authorize someone to access certain network sources to do some operations that a person wants to do.

- In (2018) Yin, Wei, et al. [18] They proposed a new blockchain signature authentication scheme, which differs from the elliptical signature scheme in current blockchain technology, in that it can withstand a quantum algorithm attack in the future. Moreover, their scheme realizes the security that cannot be tampered with under the chosen message attack. Their signature security can reduce a difficult SIS issue on the network. Their work has important theoretical significance and provides new thinking to design and develop counter-blockchain technology in the coming decades, but is authentication sufficient to authorize the user to access network resources? This is what their research lacks
- In (2019), Huh, Jun-Ho, and Kyungryong Seo [11].In their research, they have come up with a fingerprint-based entry pad based on the technology of blockchain. Where they designed and implemented the registration system to enter automatically and securely using smart phones. Their focus is on using the most secure authentication methods - fingerprints that provide safety opportunities and ensure personal information and vital sensitive

data. But their search is void of authorizing the user and authorizing him to access certain sources.

- In (2019), Pawade, Dipti, et al. [19]. In their paper, they designed the system to demonstrate the important advantages of safe storage in blockchain and non-static biometric technology. In their search, new technology was introduced and implemented using blockchain technology to protect biometric data. In this system, to extract features, dynamic data is stored permanently and then obliterated from the system. Additionally, biometric data was kept in vector method characteristics on the blockchain that was fragmented. Hence, will prevent tampering with biometric data, construction the system with protection. Agreeing to the results that are experimental, their accuracy of the system is "82.55%" and the rate of the error is "17.48%".but in their system did not address the process of authorization, but they were satisfied with the status of authentication only on the network of the blockchain.

1.3 Problem Statement

The main problem in this work is the privacy of information from manipulation on networks and because each user has a public and private key and to be able share public keys with other users on the network and prove their authentication without interference from any third party and tampering with data, and how can prevent centralize and self-control. And to protect sensitive user data during Sent across multiple servers without controlling it.

1.4 Aim of the Thesis

The thesis main goal is to design system to users as independent access to network without third-party and to enhancement asymmetric cryptography (signature via RSA) based on big-integer. And design and implementing a way to be more reliable to verify and compare user data based on hash function value, and how reliable and consistent database can be used at a later date. Also implement a way for using on the blockchain to prove authorize the user to access sources to perform some operations for creating and linking blocks on blockchain.

1.5 Thesis Organization

The rest of the thesis chapters are clarified as follow:

Chapter Two: Theoretical Background

This chapter provides a background and overview of blockchain network technology. Architecture and how it works, how the process can be validated, and approach of authentication based on fingerprint and authorization and some of the algorithms used.

Chapter Three: "The Proposed System"

This aim of chapter clarifies and explains the suggested ASBchain System design and its execution.

Chapter Four: Results and Evaluation of the Experimental

This chapter clarifies the outcomes and analysis that have been receiving from the suggested system.

Chapter Five: Conclusions and Suggestions for Future work

This chapter produce work conclusions. Additionally, it produces future work proposals.

Chapter Two

Theoretical Background