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

# Secure Websites based on Blockchain Technology

A Thesis

Submitted to the Council of the College of Information Technology for Postgraduate Studies of University of Babylon in Partial Fulfillment of the Requirements for the Degree of Master in Information Technology - Software

**BY**

**MUSTAFA SAADI HUSSEIN SALEH**

**Supervised by**

**Lecturer. Dr. Mohannad Mohammad Jasim Al-Yasiry**

**2022 A.D.** **1444 A.H**

بسم الله الرحمن الرحيم

اقْرَأْ بِاسْمِ رَبِّكَ الَّذِي خَلَقَ

(العلق: 1)

صدق الله العظيم

# Declaration

I hereby declare that this Thesis entitled " Secure Websites based on Blockchain Technology", submitted to University of Babylon in partial fulfilment of requirements for the degree of Master in Information Technology \ Software, has not been submitted as an exercise for a similar degree at any other University. I also certify that this work described here is entirely my own except for experts and summaries whose source are appropriately cited in the references.

Signature:

Name: MUSTAFA SAADI HUSSEIN SALEH

Date:      /      /2022

# Supervisor Certification

I certify that the thesis entitled (Secure Websites based on Blockchain Technology) was prepared under my supervision at the department of Information Networks/College of Information Technology/University of Babylon as partial fulfillment of the requirements of the degree of Master in Information Technology-Information Networks.

Signature:

Supervisor Name: Dr. Mohannad Mohammad Jasim Al-Yasiry

Date: / / 2022

# The Head of the Department Certification

In view of the available recommendations, I forward the thesis entitled "Secure Websites based on Blockchain Technology" for debate by the examination committee.

Signature:

Assistant Professor Dr. Ahmed Saleem Abbas

Head of Software Department

Date: / / 2022

# Certification of the Examination Committee

We hereby certify that we have studied the dissertation entitled (**SECURE WEBSITES BASED ON BLOCKCHAIN TECHNOLOGY**) presented by the student (**Mustafa Saadi Hussein**) and examined him/her in its content and what is related to it, and that, in our opinion, it is adequate with (Viva Result) standing as a thesis for the degree of Master in Information Technology-Software.

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

Signature:
Name: Dr. Jumana Waleed Salih
Title: Asst. Prof.
Date: / / 2022
(**Member**)

Signature:
Name: Dr. Saif Al-Alak
Title: Asst. Prof.
Date: / / 2022
(**Member**)

Signature:
Name: Muhannad M. J. Al-yasiry
Title: Lecturer
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

This work is dedicated to…

The martyrs of Iraq of all sects and nationalities.

My father's soul,

I will always be your son who is proud of you, and I will not disappoint you, my beloved father.

My mother,

I ask Allah to protect you from all evil and I will not disappoint you.

My wife, children and loved ones.

Whom I can't force myself to stop loving.

And finally, My beloved brothers and sisters,

Who stands by me when things look very difficult.

# Acknowledgements

**In the name of Allah, the Most Gracious, the Most Merciful**

At first, the greatest praise is to Allah for assisting me to face the difficulty that I met throughout my study, and for always helping me to achieve my aims.

I owe a deep debt of gratitude to the College of Information Technology and the University of Babylon for offering me the opportunity to complete this work.

I would like to express my sincere thanks and appreciation to my supervisor (Dr. Mohannad Mohammad Al-Yasiry) who supports me from the beginning until the completion of the current thesis. I greatly appreciate his optimistic behavior, valuable advice and trust in me that have always encouraged me to complete this work. I am totally sure that this work would have never become true without his encouragement and guidance.

I also would like to express my wholehearted thanks to my family for their unlimited support, encouragement, love and great sacrifice they provided me with throughout my life.

Finally, sincere thanks and appreciation go to my true friends for their encouragement and friendship.

# Abstract

Day after day, websites are used extensively in terms of data deposit and retrieval, so it required continuous development and expansion. On the other hand, many ways to attack it are also being developed. Therefore, there is a need to propose a (refined) method as a countermeasure that keep tracks of existing attacks. A framework is proposed for using blockchain as a technology to secure websites. The blockchain network in general is a strong and proven security-wise network, therefore it’s naturally used to protect websites precious data.

The research methodology of the thesis consists of several stages. It included a preliminary plan for this research, a study of related works, as well as criticizing them, model design and implementation, validation and evaluation, and finally the work report.

This thesis introduces proposed system that builds a complete website within the blockchain network, where websites have been protected by adding them to the system using elements through which the real website can be known from others, namely (title, website link URL, user name and password (after registering with them on the real website)) as well as A complete website has been built inside the blockchain network that contains all the details of the existing websites. Thus, the characteristics of the blockchain of decentralization, stability and privacy were exploited to protect websites.

The proposed system is evaluated according to a set of standards, including the cost results ratio is about 119 dollars, which is less than if used TLS (Transport Layer Security) method was used, where it reaches 268 dollars, as well as the time results percentage O (n),, which is the same time used in building a website by traditional methods, but the time increases if the length of the chain increases. The work was evaluated by comparing it with the previous works, and it proved to be better than them in results. Based on the study conducted by (Cyber Security Cloud, Inc.) in the first half of 2021, as well as the annual report of (Positive Technologies Application Firewall ) for the year

2018.Where in the first study, proposed system will avoid more than 90% of the existing attacks, as it will avoid ( Blacklisted user agents, Web attack, Web scan, SQL injection, Brute force attack).As for the second study, it will avoid (SQL injection, Path Traversal, Cross-Site Scripting, Local File Inclusion, Information Leakage, Brute force ) that reach 82% of avoiding these attacks.

# Declaration Associated with this Thesis

Some of the works presented in this thesis have been published or accepted. Appendix A refers to the paper that has been published.

The published Paper:

Title: Study about the Ability to Secure Websites using Blockchain.
Author: Mustafa Saadi Hussein and Mohannad M. Al-Yasiry,
Journal: IEEE,
ISSN: 978-1-6654-7213-5
DOI: 10.1109/MICEST54286.2022.9790130
Pages: 152 - 157,
Year: 2022,
Publisher: 2nd ALMuthanna International Conference on Engineering Science and Technology (MICST-2022), Almuthana University, Almuthana, Iraq.

# Table of Contents

# List of Figures

# List of Tables

# List of Abbreviations

| Abbreviation | Description |
|---|---|
| POW | Proof-of-work |
| POS | Proof-of-stake |
| POSpace | Proof of Space |
| POI | Proof of Importance |
| PBFT | Practical Byzantine Fault Tolerance |
| XSS | Cross-Site Scripting |
| P2P | Pear to Pear |
| TLS | Transport Layer Security |
| SSL | secure sockets layer |
| CSS | Cascading Style Sheet |

# CHAPTER ONE

# GENERAL INTRODUCTION

## 1.1. Introduction

A website is a collection of data and information that can be accessed over the Internet. These files and resources are grouped together under a single domain name. A website is a collection of web pages scattered around the Internet that all have the same domain name. There is a distinction between a website and a web page, because a website is made up of a collection of web pages, which can number in the millions in certain cases [1].

The World Wide Web is made up of websites, which may be built by anybody or any organization to provide a variety of electronic services that vary based on the site's nature and kind. If the URL of the site is not known, a search engine can be used to locate the address of the website on the Internet within the browser's address bar [1].

Blockchain represents a rather recent approach to information technology, initially adverted in 2008 by Satoshi Nakamoto's white paper [2]. Satoshi Nakamto presented a solution to the issues of implementing and using digital currency, particularly the double spending issue [3]. Blockchain gives an open decentralized database for any form of transaction, including values like goods and money. Consequently, the technology of blockchain has slowly started to invade the internet as a guaranteed substitutional digital model that utilizes cryptography and mathematics [4].

The technology of blockchain has several basic properties such as decentralization, transparency, shared ledger based on consensus, immutability, and privacy, thereby realizing the features needed for authentication and authorization including security, decentralization and anonymity [5].

Scientific research presents a lot of after the emergence of the blockchain technology are presented, which helped solve the problems of the Internet of things, voting problems and the protection of electronic currency, so the vision was to use this technology to solve the problem of security and privacy for websites, where need a decentralized solution and distribution and this is one of the most important features of the blockchain technology [5].

## 1.2. Related Work

Several major concerned investigations are discovered throughout the literature scan of researches addressing the associated themes. Such studies contributed to identifying the path to achieving a realistic research contribution and instilling confidence in the researcher that he or she is on the correct track and at the cutting edge of the issue being addressed.

1. Faaroek,Panjaitan,Fauziah and Septiani [6] 2022, presented the results of research and system design, it can be concluded that the process of making blockchain technology as a medium for issuing certificates and their validation can be made using Ethereum's program, namely Geth, and storing data using smart contracts issued on the blockchain network. The results of the reliability testing of the system show that the system has successfully processed 200 transactions in approximately 8 seconds. For scalability testing, it is estimated that 10 million blocks require a storage capacity of 22.6 GB to become anode or miner on this blockchain network. This research can still be developed and researched further. One of the novelties in this research is to explore various applications of blockchain technology for various fields. For example, to increase reliability by using a boot node hosted on a web

service. System testing can also be improved by performing automated tests so that more transactions and data are tested.

2. Ramos, Melon and Ellul [7] 2022 discuss aspects of blockchains' technical vulnerabilities and related cyber-attacks in order to develop a deeper understanding of the extent and efficiency of possible regulatory remedies concerning crypto-assets in the EU. He present a regulatory overview of the emerging fields of cyber risk and blockchain in Europe and illustrate a techno- regulatory gap which requires further attention. He underlines the difficulty of assigning traditional cyber regulatory measures due to certain technical characteristics related to blockchains. He maintains how the relationship between cyber law and technology may evolve in the near future, as decentralized technologies and the cyber risks that go with them, continue to develop rapidly. By providing an interdisciplinary perspective of cyber security in the blockchain domain, heaim to bridge the gap that exists between legal and technical research, supporting policy makers in their regulatory decisions concerning crypto-assets, decentralized technologies and associated cyber risks.

3. Riadi, Umar and Lestari [8] 2021, used the blockchain in the Internet of Things to improve the security of the smart payment application so that the security and integrity of the data within the application is preserved, the blockchain has security features through decentralization as well as through the consensus algorithm, where it can eliminate data changes made by hackers and make improvements to it, where nodes containing different data are isolated from the network nodes and then deleted from the network. The result in this research against attacks (Cross-Site Scripting (XSS) , Man-In-The-Middle) before using the blockchain was very high, and after using the blockchain, the result was not found, meaning that its result was zero .

4. Dirsehan [9] 2020,presented the idea of creating a website with two safes on the ground in two different places, the first is the location information and the other is in a secret location for the purpose of intellectual protection, where anyone can subscribe to the site after paying the wages by installing his idea inside the site whose account will be built within the blockchain network and will have a Time stamp proves his eligibility for the idea and then the system officials save the idea inside the two safes in the form of hardware if the system collapses or is hacked. This study has several limitations. Only one website was used in order to test the model proposed in this study. Moreover, the sample size is limited, thus generalizations of the findings should be approached with caution.

5. Case, King, and A. Case [10] 2020, presented empirical study was done to evaluate blockchain adoption among the largest corporations, the Fortune 500, because of its significant potential benefits, particularly in terms of transaction security. According to an examination of the companies' websites, just 4% of the Fortune 500 disclose usage, whereas 20% of the Fortune 100 do. The majority of businesses are in the financial or technological industries, with commercial banking being the most popular. Furthermore, a content analysis suggests that more than half of companies are employing blockchain technology for internal applications or creating blockchain networks, with five companies having considerable coverage. IBM, Oracle, Microsoft, J.P. Morgan Chase, and Cisco are among these companies. When the search term "blockchain" is entered into IBM's search engine, it returns over 1.3 million hits. According to the content study, 52 percent of companies employ blockchain technology for internal applications or blockchain development. According to the findings, there may be significant competitive market advantages available

6. Singh, Tanwar and Sharma [11] 2019, presented concentrates on the utilization of one of the latest and most promising technologies, that

is, blockchain technology against DDoS attacks. The blockchain technology is rapidly finding use in various applications ranging from financial to gaming; this is because of its stable, decentralized, and secure architecture. The DDoS solutions based on blockchain are still in infancy and some solutions provide only architectural details without bothering about the implementation details.  Public blockchain is considered in almost all the proposals. In public blockchain information is not hidden and therefore can have privacy concerns. If private blockchain is considered by these mechanisms then it may have sustainability issues. In almost all of these mechanisms it is assumed that adversary cannot compromise the blockchain and DDoS attacks are not possible on blockchain verifiers/miners and smart contract.

7. Shorman and Allaymoun [12] 2019 developed a technical mechanism for authenticating personal pages on social networks that is both effective and simple. Anyone may use this approach to verify any account on social media, increasing the likelihood of identifying the true person behind social media profiles. Furthermore, in order to provide a more confident and safer social network atmosphere, this strategy will display false accounts. The Blockchain approach simply requires developers to make little changes to the platform's properties, as it is only a participation mechanism between Blockchain and personal data. It's then paired with personal pages to signify that these pages include the account holder's true personal information, which is saved in an encrypted block that's impossible to change, duplicate, or steal. Future work will include detailed verification of the technical aspect; in addition, a real scenario test will be performed. Once applied to social networking pages, analysis of the results will be performed to resolve any problems that may face the application of the block chain technology in the authentication process.

8. Dadkhah, Seno and Borchardt [13] 2017 , presented had a different type of scientific and literary contributions about scientific journals in terms of the concept of hijacked journals and predatory journals, as well as sheds light on the most important attacks against scientific journals and the seriousness of these attacks on correct information and the importance of publishing the information if it is false and the dependence of future scientific research on information False . It also highlights several ways to treat these attacks and ways to avoid them.

## 1.3. Problem Statements of Thesis

The importance of the website lies in the fact that it has entered all areas of daily modern life and cannot be dispensed with at the present time, as it is linked to banking, health, educational and institutional matters.

Despite the development of websites, they are constantly exposed to attacks in various ways, whether in the past or at the present time. These attacks take on the nature of continuous updating over time, as the mechanisms of the attacks speak according to the methods of building and protecting websites.

Website security solutions are either special or single solution. Sometime expensive (if tuned and robust (cost money and time)). Wasteful (centralized), or complicated (many ways).

On the other hand, the blockchain they are inexpensive (free sources), decentralized, many contributors, and simple (special link list).

## 1.4. Aim of Thesis

How to create a blockchain that represents the identity of the current website (hue). Hence it doing acts as a defense against multiple attacks.

The aim of this thesis is to protect the website from attacks. To achieve this aim there are serve objectives.

## 1.5. Objectives of Thesis

1-Securing websites against web security attacks.

2-Define and extract data or characteristics of a web identity.

3-Design and build a blockchain model that works as a defensive technology for the website instead of defending cryptocurrency.

## 1.6. Contributions of Thesis

1- More of the best solutions and procedures for website security.
2- Building a blockchain model that protects the website.
3- Inexpensive and robust solution (unlike existing roads).

## 1.7. Thesis Organization

**After Chapter 1** presents an introduction to the entire research, the rest of the thesis is structured as the following:

**Chapter Two** introduces theory part, which includes websites, secure websites, the blockchain, tools used in propose system and the criteria used in the evaluation.

**Chapter Three** provides the design and implementation of the proposed system.

**Chapter Four** presents the simulation parameters, explains the tools that were used and why they were used, the obstacles that faced the project and how they were resolved, System implementation stages and work evaluation.

**Chapter Five** includes the main conclusions and future works are also discussed in this chapter.

# Chapter Two
# Theoretical Background

## 2.1 Introduction

This chapter contains an overview of the five main axes: (websites, secure websites, the blockchain, tools used in propose system and the criteria used in the evaluation) and describes some of the basic terms used in building the proposed system for these axes separately to secure websites.

## 2.2 Website

There are already millions of websites on the World Wide Web [14], yet none of them have existed for over two decades, since the history of the first website goes back to 1991, precisely on August 6th. This site was created by British computer scientist Tim Berners-Lee and run on a NeXT computer at the CERN laboratory to provide information about the World Wide Web project. [15].

The British scientist refused to have the web technology patented for him because he wanted this network to be a free and open world so that it could develop quickly, and in 1993, the first web browser, known as (Mosaic), was released, followed by the launch of many websites in the following years. The number of websites reached more than 51 million in 2004,[15] and there are now more than 1.8 billion websites on the World Wide Web, with more than 570 thousand new websites being established every day [16].

### 2.2.1 Types of Websites

Websites are divided into two main types, which are the following: Static sites are pre-created electronic pages that are returned by the server without modification, and their content cannot be modified by regular users. When using the internet to make a request. Dynamic sites: They are websites whose content can be changed so that the existing databases can be modified via the site server. Making a joint change once across dynamic sites will reflect this change on all pages of the site. The following table 2.1 shows some comparison between static and dynamic sites: [17]

Table 2.1: Difference Between Static and Dynamic Websites

| Static Website | Dynamic Website |
|---|---|
| Content of Web pages can't be changed at runtime. | Content of Web pages can be changed. |
| No interaction with database possible. | Interaction with the database is possible. |
| It is faster to load as compared to dynamic website. | It is slower than a static website. |
| Cheaper Development costs. | More Development costs. |
| No feature of Content Management. | Feature of Content Management System. |
| HTML, CSS, JavaScript are used for developing the website. | Server-side languages such as PHP, Node.js are used. |
| The same content is delivered every time the page is loaded. | Content may change every time the page is loaded. |

### 2.2.2 Website Ranking

Websites can be classified according to the so-called Top-Level Domain (TLD) names, and this name appears at the end of the URL of the website, where this part determines the nature of the content and the type of website on the Internet. Table 2.2 lists some of the top-level domain names in addition to the type of site that each name represents [18].

Table 2.2: Domain Names at the Top Level

| Domain | Sites this name refers to |
|---|---|
| .com | Commercial Business |
| .edu | Education |
| .gov | U.S. government agency |
| .int | International Entity |
| .mil | U.S. military |
| .net | Networking organization |
| .org | Non-profit organization |

The World Wide Web is made up of all publicly accessible websites. Private websites, such as a company's internal website for its workers, can only be viewed over a private network.

News, education, commerce, entertainment, and social networking are all examples of websites that are dedicated to a certain topic or purpose. The navigation of the site, which commonly begins with a home page, is guided through hyperlinking between online pages [19].

Users can use a variety of devices to visit websites, including PCs, laptops, tablets, and smartphones. A web browser is the software program that is utilized on these devices.

There are several sorts of well-known websites [20]: (E-Commerce website, Business website, Entertainment website, Portfolio website, Media website, Brochure website, Nonprofit website, Education website, Infopreneur website, Personal website, Web portal and Wiki or community forum website).

Due to the large number of different types of devices connected to the network, as well as the variety of different types of users based on the variety of different types of websites, there has been an increase in data breaches, with the Malwarebytes Labs blog declaring 2018 the year of the data breach. A data breach stays unnoticed for an average of 197 days, according to the Ponemon Institute's 2018 Cost of a Data Breach research. The data leak will take another 69 days to be fixed. The damage had already been done by the time the security flaw was detected and corrected [21].

### 2.2.3 Reliable Scientific Journals

In order for the Journals to be reliable, it must meet several requirements:

1. It must have a website on the World Wide Web.
2. It must not be hijacked (as a second website is created other than the original site of the journal, and after publishing on this site, the search will not appear in the Scopus database).
3. It must own the scientific journal ISSN (International Standard Serial Number) is an 8-digit code used to identify newspapers, journals, magazines and periodicals of all kinds and in all media–print and electronic.
4. A solid scientific journal has a wide spread, and is known to the audience of readers on the one hand, and the audience of researchers on the other hand, and this spread is at the regional or international level.
5. The discreet scientific journal often stems from reputable universities and is a comprehensive and rigorous arbitration court

by specialized and qualified arbitration committees to carry out this task [22].

### 2.2.4 The Most Important Attacks on Scientific Journals.

There are several types of attacks that scientific journals have been subjected to, for the predatory of them, hijacked them, or defrauding students in order to transfer money, publishing scientific research and not publishing it, as well as stealing scientific ideas for the request. This phenomenon has increased with the use of scientific journals for websites, where previously scientific journals were limited to papers. One of the most important attacks against scientific journals is (phishing attacks, Spear phishing [23], Man-In-The-Middle Attack, Cross-Site Scripting (XSS), and others).

## 2.3 Security of Website

There are several ways to protect websites, for example, but not limited to (TLS) method, which is an encryption protocol that provides security in communications between computers and is used in e-mail and instant messaging, in addition to Internet websites (HTTPS), which is the most famous, but it has the advantage of protecting the internal data of the site and does not protect the external structure.

Web security, also referred to as "cyber security," entails safeguarding data by preventing, detecting, and responding to attacks.

In and of itself, a data breach isn't a threat or an assault. A data breach occurs when thieves gain illegal access to a computer system or network and steal the private, sensitive, or confidential personal and financial data of customers or users. The following are some of the most common cyberattacks employed in data breaches:

1-Spyware.

2-Phishing.

3-Broken or misconfigured access controls.

Cybercriminals seek to steal names, email addresses, usernames, passwords, and credit card numbers in the majority of data breaches. Cybercriminals will take any information that can be sold, used to hack into other accounts, steal your identity, or be used to make fraudulent purchases. Hackers will sometimes take your data only to prove that they can [24].

A data breach comes as a result of a cyberattack that allows cybercriminals to gain unauthorized access to a computer system or network and steal the private, sensitive, or confidential personal and financial data of the customers or users contained within [24].

He must implement proper security measures on each website component to keep your website safe. When it comes to operating systems or software, he may refer to the suppliers' security guidelines for all users and make sure to properly adjust the settings or install security patches. Web applications, on the other hand, are often tailored for each website; therefore, must protect each web application separately [25].

However, keep in mind that the following are the finest methods and techniques for securing a website [26]:

1- Keep yourself up to date.

2- Strengthen access control.

3- Make sure everything is up to date.

4- Increase the network's security.

5- Set up a firewall for web applications.

6- Download and install security software.

7- Hide administrative pages.

8- Set a limit on the number of files may upload.

9- Make use of SSL.

10- Turn off the auto-fill feature on the form.

11- Make regular backups.

12- They are unable to conceal your code.

Despite these ways to protect websites, there are other ways that it lacks an effective solution to the issue of website security. Therefore, will suggest that to solve this problem use blockchain techniques.

### 2.3.1 The Most Important Attacks on Websites

There are many types of attacks that websites are exposed to, but will discuss some of the most important of these attacks, either because of the many websites that are exposed to them or because of the financial losses that websites have incurred because of them. These attacks are:

#### 1 SQL Injection

This type of attack occurs when the attacker inserts a piece of code into a website, and when the user enters the username and password, he fetches it from the database to the attacker. This attack is one of the most dangerous types of attacks currently in existence and the most common, as it targets Internet sites and server databases directly.

#### 2 Cross-Site Scripting (XSS)

It is a type of injection where malicious scripts are injected into protected and trusted websites. It occurs when an attacker sends a web application to send malicious code, and it can be transmitted from one user to another. This is unpredictable because it comes from trusted websites and steals the data entered by the user to the website.

Even if it is more common and represents 40% of attacks today, it is not complicated as it is carried out by people who are inexperienced using programs developed by others [11].

### 3 Man-In-The-Middle Attack

Man-in-the-middle attacks are used by attackers to obtain (often sensitive) information. The data is intercepted while it is being exchanged between two parties by the suspect. If the data is not secured, an intruder will quickly read personal information, user credentials, and other confidential information when it travels through two sites on the Internet [11].

### 4 Phishing

It is an e-mail attack, which creates a feeling of urgency, curiosity, or fear in the victim, prompting her to reveal sensitive information by clicking on the malicious link. And the attack occurs as a result of human error; so, it is especially dangerous, because it is not an error or weakness in the system or programs, because it is less predictable, which makes the process of thwarting it difficult [10].

### 5 Spear Phishing

It is similar to the phishing attack, but it is more targeted than phishing because it targets individuals rather than institutions, and the attacks are less visible and require effort and experience to identify them [10].

### 6 Brute Force

It is when the attacker guesses the username and password to gain access to the user account. Where if the password is strong, it may take several years to access it, and using high quality and expensive computers (quantum) this time reduces dramatically and becomes some days [10].

Despite the fact that all currently available solutions have flaws and are ineffective, costly, or only operate on a certain site, they are all ineffective. As a result, will recommend that deal with this problem utilizing blockchain technology, which believe will solve practically all of the difficulties listed above.

For the first time, blockchain addresses a specific issue that has stymied past attempts to build digital money. Would presume that can utilize blockchain approaches in website security since the blockchain was used with money and is the most essential and expensive (data) object that can be stolen and found on websites.

This relationship explains the ship between blockchain and website and looking forward to building relationship between blockchain and website to secure website. Figure (2.1) explain relationship blockchain and website [23].

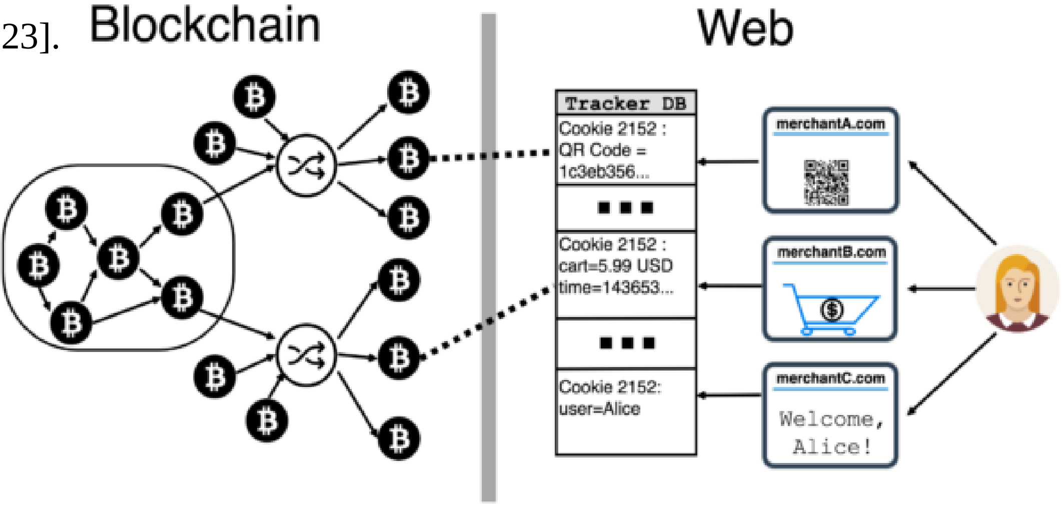


Figure (2.1) explain relationship blockchain and website in cryptocurrency [27]

## 2.4 Blockchain

The basic ideas behind Blockchain appeared at 1991 when a signed series of data as digitally signing by using as an electronic ledger for files in a way that might simply display none of the documents that are signed in the group had been altered [28]. Blockchain technology was adverted in 2008 by Satoshi Nakamoto’s white paper [29].

Blockchain and Bitcoin Technology as explained by Nakamoto solved the most important problems of computer science that represent a barrier to an effective digital pecuniary system for years: the problems of double spending. Double spending problem is that fund must be only once spent, unlike a file, which can be copied several times randomly [30].

The Blockchain is distributed ledger shared via everyone participants-based consensus protocol in the network of the Blockchain in which be most of the participants agree on the result [31]. Blockchain keeps a nonstop growing records list, named blocks. Every block includes transactions list and connects to the former generated block, up to the first block, called genesis block. The mining process appends a block and verifies the validity of transactions (avoid double spending) via a Proof of Stake (POS), or other consensus protocols, like Proof of Work (POW) [32].

New blocks are created via a process called mining via several nodes, called miners. These miners operate anonymously by working jointly and attempting to solve mathematical puzzles, which generates new blocks to the Blockchain. It takes several steps to construct and announce a new block. [33].

The ledger isn’t owned by any central servers or central authority. Instead of it is distributed to computers (peers) on the decentralized network [32]. Also; the Blockchain enables each user to be pseudonymous, which means the user is unknown but the user account is not all their transactions are noticeable public [34]. Its basic features are [35]:

1- Decentralized: - The core characteristic of the Blockchain, i.e. Blockchain no needs to rely on a central node at any time, where data can be stored, recorded, and updated by distribution.

2- Transparent: - The data is recorded via the system of Blockchain and it is transparent to the nodes, also it is transparent when updating the data, this will have led to the reason of being Blockchain is trusted.

3-Open Source: - The most systems of Blockchain are open to each node, the record can be verified publicly and also users can utilize the technologies of Blockchain for creating applications.

4- Autonomy: - Each node on the Blockchain system can safely update data or transmit, Because of they are based on consensus, the basic idea is a single person to trust to the entire system, and no one can intervene it.

5-Immutable: - Any records will be saved forever, and can't be altered unless certain node can have control more than fifty-one % nodes at the same time.

6- Anonymity: - The technologies of Blockchain addressed the issue of trust among the nodes, therefore, transaction or data transfer can be anonymous, only the address of the person on the Blockchain is needed to know.

Blockchain is considered as a distributed peer layer to peer net executed on the internet, as illustrated in Figure (2.2) [36].

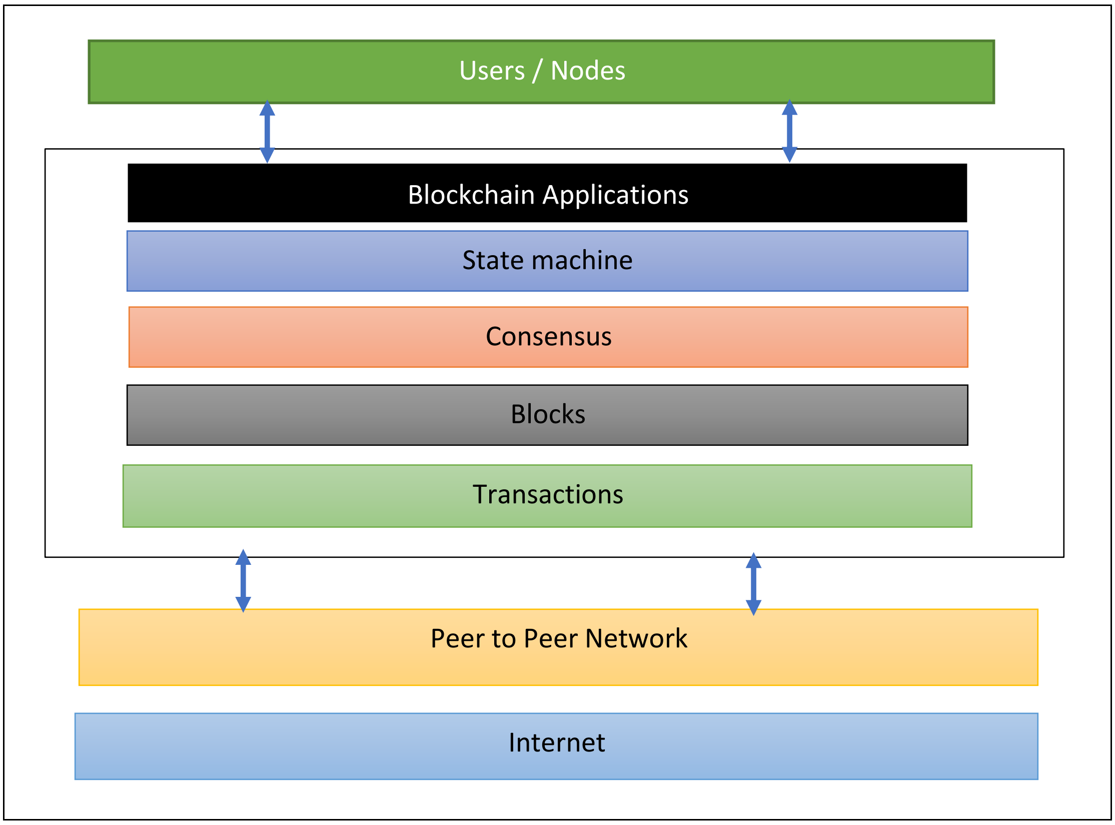


Figure (2.2): Network view of a Blockchain [36].

### 2.4.1 Peer to Peer (P2P) Network

It is a topology of a network when the whole peers can be connected in addition to transmitting and receiving messages [36]. It is a computer network dependent on nodes, (e.g. computers that are preserving the network worldwide). P2P is a decentralized network where each node shares information with another without anybody controlling the network [33].

The Blockchain relies on more than thousands of nodes in the P2P network, and at each node, the data is updated and replicated. Even in case the nodes become inaccessible or drop it from the network, this network as an entire persist to work, therefore, it becomes highly available [36].

There are two kinds of peers in the P2P network: validator and member peers. The validator peers (represents the special peers) are consuming the services of Blockchain besides validating and verifying the new Blockchain transactions. While member peers are consuming Blockchain services, and every miner holds exactly the same transactions history over the network and comprises a certain responsibility for maintaining and publishing the new transaction blocks to the network [32].

### 2.4.2 Block

It is a block building unite of Blockchain. It is consisting of set of a transactions with Meta data [32], see figure (2.3) . The block involves two part is the block header and the block body [37].

Block Header: it includes the following:

a) Block version: indicates which tuple of block validation rules to be applied.

b) Merkle tree root hash: is the value of hash to the entire block transactions.

c) Timestamp: is the present time at seconds in universal time.

d) N-Bits: target threshold of a valid block hash.

e) Nonce: Four-byte field, it usually starts with zeros (0) and increases for each hash calculation.

f) Parent block hash: a 256-bit hash value which indicates to the former block.

The block body consists of transactions and a transaction counter. The total number of transactions that can a block contain it relies on the block size and the size of every transaction [37].

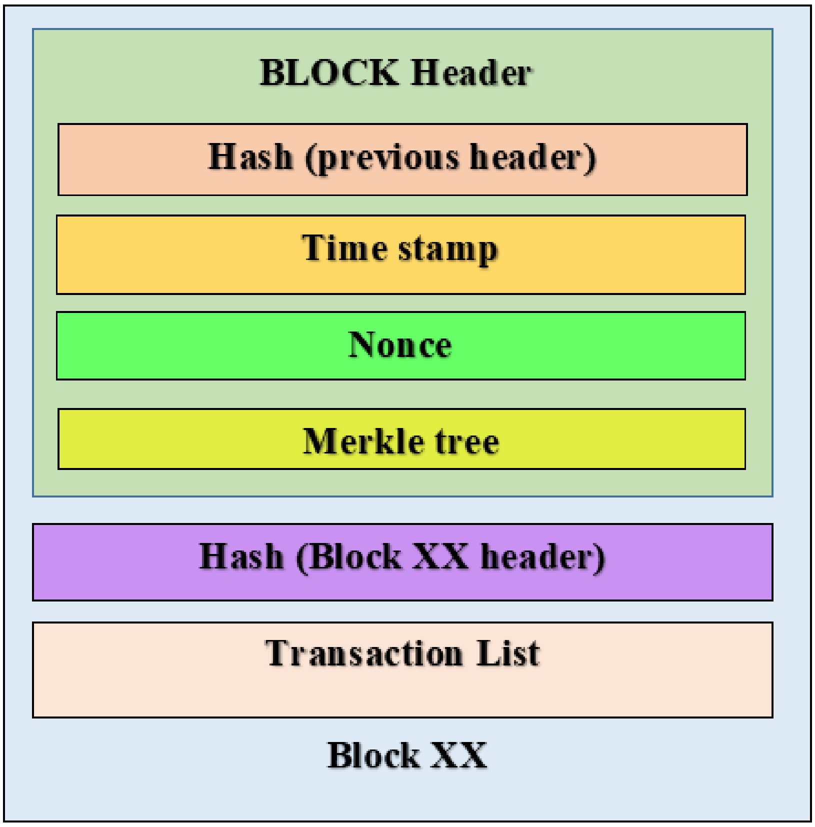


Figure (2.3): Block structure (Generalized)[38].

### 2.4.3 Transaction

A transaction refers to the interaction among nodes. With cryptocurrencies, e.g., a transaction refers to a movement the crypto-currency between the peers of the Blockchain network [34]. The transaction contains the sender and the receiver addresses, and other data. Before sending, could be signed the transaction by the private key relevant to the public key of the address [39].

Additionally, the transactions are not arranged based on of a generation because of the propagation delay in the P2P network. Accordingly, the transactions are grouped at a given time to create a block and publish these blocks to the network [32]. Before the broadcast, the transactions to its neighbors, each node that receives the transaction will first verify each transaction with a long checklist of criteria. This assures that only validated transactions are publishing on the network, whilst invalid transactions are rejected by all node that interviews them. Then every node creates a pool of only valid new transactions, nearly in the same order [40].

### 2.4.4 Ledger

Ledger is the technology upon it the records of transactions are published across multiples sites, companies or institutions, countries and are typically public. Blocks (collection of Transactions) are stored one after another in a continuous ledger, but they can only be inserted when consensus on it [41]. It is immutable in that once data is inserted to the ledger; it cannot be altered [30]. In the distributed ledger each record holds a timestamp and unrepeatable cryptographic signature, thusly making the ledger an auditable date of every transaction in the Blockchain network [42].

### 2.4.5 Blockchain Structure

Essentially, the Blockchain is a linked list of the block which utilizes hash pointers rather than usual pointers. Hash pointers are utilized for pointing to the former block [36]. Which consists of timestamp ordered, linked blocks that contain all of the transactions. The blocks are linked such that each block contains the ID of the previous block at the chain [31]. Each block is chained to other blocks via referencing a parent block. If any content in the header is altered, then its child block header will contain invalid hash. Transaction modification is will also detect. A block header also contains the Merkle root of the Merkle tree structure [43]. Consequently, this generates a tamper evident log that impossible to be altered. Furthermore, hash pointer used to trace even the first block named genesis block [32]. This led to the possibility of easily determining and rejecting the changed blocks as in Figure (2.4) [34].

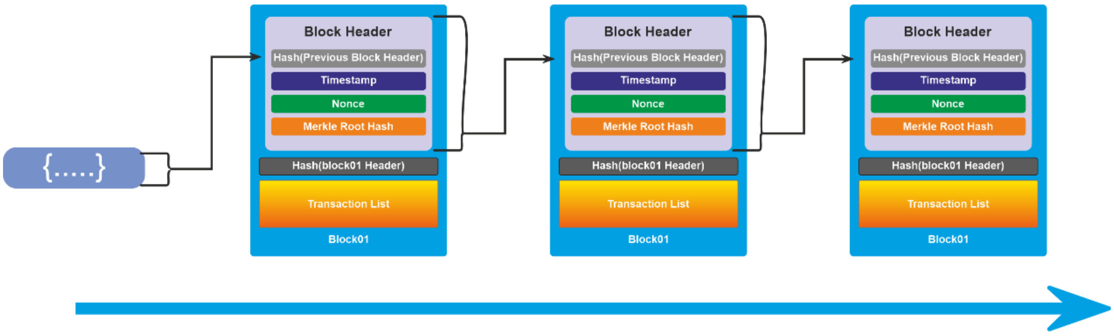


Figure (2.4): Generic chain blocks [36].

### 2.4.6 Smart Contract or Chain Code

Smart contracts are the business terms that are embedded in a blockchain transaction database and executed with transactions. This is also the rules component of a blockchain solution. It is needed to define the flow of value and state of each transaction. Figure (2.5) gives a good idea of shared ledger, smart contract, cryptography and trust system concepts:

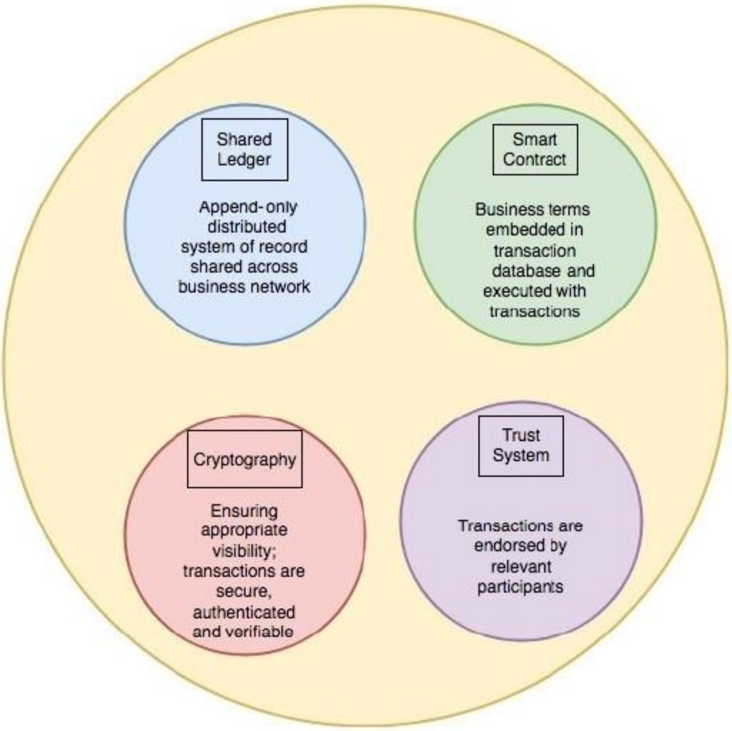

Shared Ledger
Append-only distributed system of record shared across business network
Smart Contract
Business terms embedded in transaction database and executed with transactions
Cryptography
Ensuring appropriate visibility; transactions are secure, authenticated and verifiable
Trust System
Transactions are endorsed by relevant participants

Figure (2.5) diagram gives a good idea of concepts [44]

The four building blocks are generally accepted and well understood. They have existed for decades prior to blockchain. Shared ledgers are an evolutionary change, similar to the move to computer-based spreadsheets, but the underlying business rules have stayed the same [44].

### 2.4.7 Distributed Blockchain

Distributed Blockchain is block distributed across the nodes of P2P blockchain and the whole nodes hold the same Blockchain copy. The utilization of distributed Blockchain led to the users do not require to equip email, social security number, or telephone number to authority or any central server. The users are capable of generating their digital identity and distributing their public key to the entire distributed network. So, management of distributed decentralized anonymous identity can be provided to the users. Every node in the distributed Blockchain has copies to the whole transactions, which means a node can to monitor the history of whole transactions [32].

### 2.4.8 Blockchain Security

Blockchain security is an important part of Blockchain technology so it can use asymmetric cryptography. Here, cryptography is often utilized for providing confidentiality service. It cannot be labeled as a perfect solution; however, it represents a decisive constructing block into a big system of security for processing the issue of security. Cryptography supplies different security, like authentication, integrity, confidentiality, authentication of the entity, and authentication of information origin and non-repudiation [32].

#### A-Cryptographic Hash Function

One of the essential Blockchain technology content is the utilization of a cryptographic hash function for various processes, like hashing the block content [34]. A cryptographic hash function is a mathematical model which takes any input of data (string) of any length and results in an alphanumeric string of constant sized. The resulted the string is named digest or hash value or digital fingerprint or checksum. Always, the function obtains the same hash to the same data, although the number of times recalculated.it can be used to validate the integrity of data because the hash cannot be reversed to get the input data and for this reason, it is named a one-way hash function [32].

The technologies of Blockchain take many of transactions and generate a hash fingerprint (the digest) to the list. Any user based on exact transactions list can create the exact digest (fingerprint). When changing a single value in a transaction inside the list, the fingerprint of this block will be altered, making it easy to detect cover till minor one-bit alters [34]. This would easily detectable to the full network because it would be clear that the digital fingerprints have been altered and all transactions would be refused by the nodes, which are responsible for validating transactions and blocks [41].

These hash codes are used in order to interconnect blocks together as in Figure (2.6) [45].

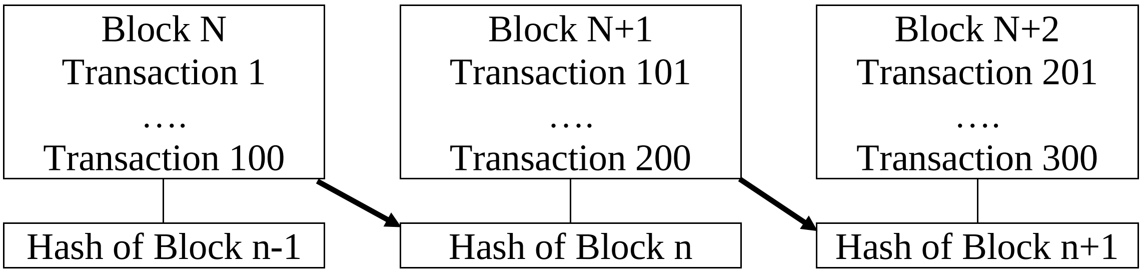


Figure (2.6): The interdependence of blocks [44].

### B -Digital Signature

Digital signature gives a facility to associate a message with an entity created from this message. It is utilized for providing nonrepudiation and data origin authentication [36]. It is required to authenticate the transaction when creating a transaction on the Blockchain [32]. Additionally, it is generated via utilizing public key cryptography. Public key cryptography utilizes a key that is a collection of private and public keys [46]. Any user has a pair of keys (private and public). The private key is utilized for signing the transactions. The digitally signed transactions are published over the entire network [37].

The public key is broadcasted publicly to determine the digital identity[38]. The typical digital signature is involved with two phases: signing phase and verification phase [37]. The figure (2.7) below explain digital signature scheme [47].

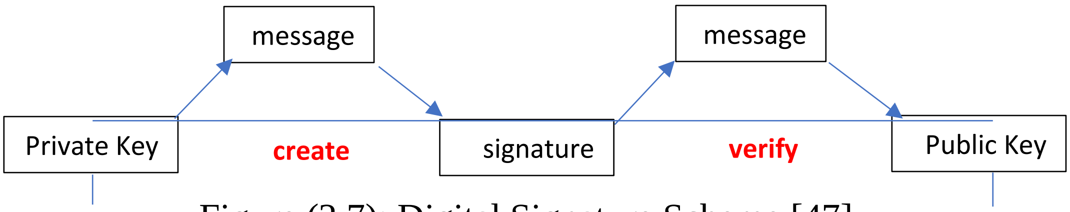


Figure (2.7): Digital Signature Scheme [47].

### C- Merkle Tree

The Blockchain based P2P network in which every peer should have an exact copy of transaction that must be propagated and verified over the P2P network. This is computationally expensive and time consuming. A Merkle tree is utilized to summarize the transactions in each block. This tree is an effective data structure, also named a binary hash tree, which works on summarizing and verifying the large data sets integrity [38]. In this tree, firstly, the inputs are located at the leaves. Secondly, the values of the pair of children nodes are hashed with each other for producing internal node value (parent-node) till a Merkle root (a value that is single-hash-) is obtained [36].

Therefore, The Merkle tree is utilized that rather than sending data only, the data hashed is transmitted and the receiver node matching the hash value against the root [32]. This is accomplished for freeing up the space of storage required to store the Blockchain on the nodes [46]. Figure (2.8) shows an example of a Merkle tree [36].

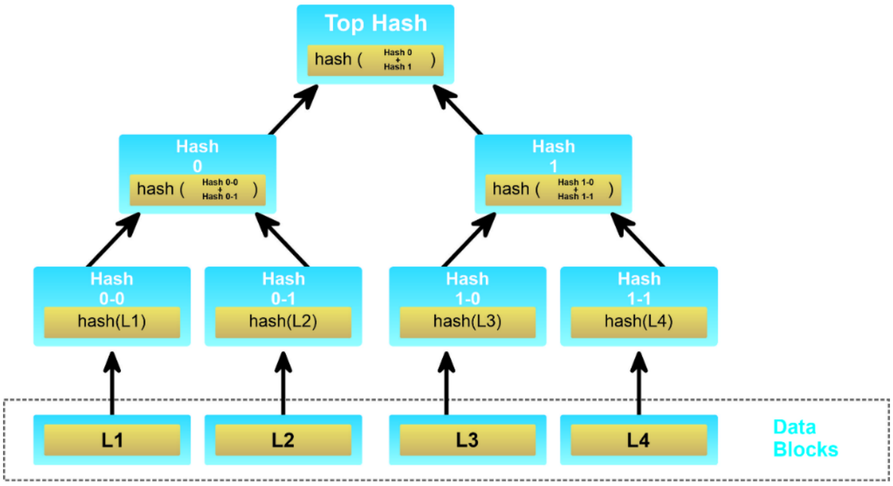


Figure (2.8): An example of a Merkle tree [36].

### 2.4.9 Type of Blockchain

There are four kinds of blockchain networks [48][49].

#### A. Public Blockchain.

A shared blockchain is a permission-less digital ledger where everyone may enter and conduct transactions. It is a non-restrictive variant of the ledger of which each peer has a duplicate. This also ensures that anybody with an internet link may use a public blockchain. The decentralized bitcoin network was one of the first public blockchains to be made available to the general public. It enabled everyone with an internet connection to conduct decentralized transactions. Consensus techniques, including Proof-of-Work (PoW), Proof-of-Stake (PoS), and others, are used to verify the transactions. The participating nodes must do the heavy lifting, like validating transactions, in order for the public blockchain to function. A shared blockchain may become non-functional if it does not have the requisite peers involved in transaction processing.

#### B. Private Blockchain.

A private blockchain is a blockchain that operates in a restricted area, such as a locked network. It is just a permissioned blockchain that a single person runs. Private blockchains are suitable for usage inside a privately owned corporation or entity for internal purposes. Then will easily utilize the blockchain and enable only chosen users to enter the blockchain network this way. The company may also control the network's criteria, such as entry, approval, etc.!

### C. Consortium Blockchain.

A consortium blockchain (as well recognized as Federated blockchains) is a novel way to address companies' needs that need public and private blockchain capabilities. Any facets of the organizations are made available through a consortium blockchain, while others are kept confidential. The preset nodes in a consortium blockchain monitor the consensus procedures. Furthermore, if it is not accessible to the general public, it retains its autonomous existence. Why can do it? A consortium blockchain, on the other side, is operated by several organizations. As a result, there is not a single centralized power at work here. The consortium seems to have a validator node that will verify transactions and initiate or receive transactions to ensure full functionality. The participant node, on the other hand, will both receive and execute transactions. In a nutshell, it provides all of the benefits of a private blockchain, such as confidentiality, anonymity, and reliability, without relying on a single entity to consolidate control.

### D. Hybrid Blockchain.

While hybrid blockchain can tend to be a consortium blockchain, it is not. There might, though, be any parallels between them. A hybrid blockchain combines the benefits of both private and public blockchains. It has applications in organizations that wish to deploy the best of all worlds and do not want to adopt either proprietary or public blockchain.

### 2.4.10 Distributed Consensus

Consensus of distributed protocol is the cornerstone of the Blockchain [28]. For reaching an approval on that transactions must be inserted to the distributed ledger, the Blockchain utilizes the protocol of distributed consensus [32]. The next subsections refer to the major consensus models that exist today [41].

#### A. Proof-of-work (POW)

Ethereum and Bitcoin uses the PoW mining process, which is still utilized for several other blockchain technologies. It allows mining nodes to resolve a difficult mathematical problem updated regularly and has been decided upon by all miners. The block is sent to the blockchain network after a node validates the transfers and solves the puzzle. Other mining nodes search the block to see whether the submitter is telling the facts. The block will be applied to the blockchain, and the submitter could indeed be credited until the miners accept that it is valid. The agreement, in this case, is focused on a plurality vote. As a result, faking is impossible until the attackers have control over more than half of the mining nodes. The trouble with this method is that it wastes many processing resources to solve the mathematical puzzle [50].

#### B. Proof-of-stake (POS)

Proof of Stake: PoS, unlike PoW, would not necessitate the mining nodes solving a computationally costly mathematical puzzle. Instead, a pseudo-random process is used to choose the next block generator or miner. The likelihood of a node being selected to build a new block is proportional to its wealth or stake. To put it another way, the more capital a node has, the more likely it is to mine a block. The miner is not rewarded in the native version of PoS; however, the programmers are rewarded and punished depending on their success in the expanded versions. Selection centered on the richest account could lead to a single account overseeing all of the creations, resulting in an unequal allocation and even centralization. As a result, two methods of node choice were suggested: random node choice and coin age-based selection. Users who have not built a block in the previous 30 days are qualified for mining in the coin age-based process. [28].

### C. Proof of Space (POSpace)

PoSpace is similar to PoW, but the puzzle necessitates a large amount of room. By allocating the necessary storage space to conduct mining, a miner proves its capacity to produce a new block. In other terms, the mining node must have a great storage capacity rather than a high computing capability. PoSpace has some theoretical and functional implementations; nevertheless, the requisite large memory space is an obstacle, close to the PoW computing challenge [51].

### D. Proof of Importance (POI)

PoI is a mining strategy that decides the value of a node depending on the number of transactions and the node's balance. The more important nodes are given a preference based on a hash calculation. Furthermore, for the next block formation, the node with the top importance is selected. [45].

### E. Practical Byzantine Fault Tolerance (PBFT)

Unlike others, is a consensus mechanism that does not rely on some form of resource and instead depends on blockchain consensus focused on the Byzantine fault tolerance strategy. First, a leader is chosen and decided upon by the nodes in this process. The blockchain network's chief agrees on transaction confirmation and releases a block to all network nodes. Only when two-thirds of the mining nodes confirm a transaction is right is it committed to a new stack. Since the leader varies regularly, the strategy is not considered unified. PBFT was demonstrated to be quicker than other methods, but, owing to the resultant transmission overhead, it has scalability problems, as described in [52].

There are also other types of consensus algorithms, for no room to mention all of them. Only the most important and the most used ones are mentioned. Table 2.3 shows a comparison of the types of consensus algorithms.

Table 2.3: Different Comparison Mining Methods

| **Mining method** | **Resources needed** | **Randomness** | **Implementations** | **Reward miner?** | **Tolerated power of the adversary** |
|---|---|---|---|---|---|
| POW | High computation power | No | Bitcoin | Yes | < 25% computing power |
| PoS | Wealth or stake | Yes | Ethereum | No | < 51% stake |
| PBFT | None | No | Hyperledger | No | < 33.3% faulty replicas |
| PoSpace | High memory | No | Permacoin | Yes | 50% token wealth |
| MoT | Trustworthiness | No | Not implemented | Yes | 50% token wealth |
| PoI | Node significance | No | NEM | Yes | 50% token wealth |
| Minimum block hash | None | Yes | Bitcoin extension | Yes | 50% token wealth |
| DPoS | Wealth or stake | Yes | BitShares, Steemit | Yes | < 51% validators |
| PoET | None timer | Yes | Hyperledger Sawtooth | Yes | 50% IDs (33% if BFT used) |
| PoA | reputation-based | No | Aura, Clique | Yes | 50% TEEs (33% if BFT used) |

### 2.4.10 The Difference between Blockchain and Linked List

Data of any kind can be stored within the blockchain network, as the blockchain is linked lists, but there are simple differences between them:

a) It cannot change or delete data in blockchain, but can edit it in linked list.

b) It cannot re-arrange the blocks in blockchain but can do it in linked list.

c) It can only store ledger or receipts on blockchain, but it's not the same in-linked list.

d) It cannot remove or add a block in the middle of a blockchain.

e) Blockchain is single linked list, only different is the single linked list holds data-type int. -float-string… etc. Blockchain holds ledgers.

## 2.5 Important Tools

### 2.5.1 Node.js

Node.js is an open source server environment that allows to run JavaScript on the server; uses asynchronous programming to eliminate waiting and simply move on to the next request; runs single-threaded and non-blocking, and is very memory efficient. A common task for a web server is to open a file on the server and return the content to the client.

### 2.5.2 Truffle

It is a set of tools inside portfolios that help us manage the linking process between the website and smart contracts, not software tools, and it is widely used with Ethereum and makes life easier.

### 2.5.3 Web 3 (Meta Mask)

The terms "Web 1.0" and "Web 2.0" relate to different periods in the history of the World Wide Web as it progressed via different technologies and forms. Web 1.0 refers to the time roughly between 1991 and 2004, when most websites were static webpages, referred to as the "read only" version of the internet by some, and the great majority of users were content consumers rather than producers. Web 2.0 is centered on user-created content published to social media and networking platforms, blogs, and wikis, among other services, and is founded on the concept of "the web as platform." Web 2.0 is widely thought to have started about 2004 and is still going strong today; some refer to it as the "read/write" version of the internet.

Web 3 is the next generation of the internet, focusing on moving power away from huge tech corporations and toward ordinary consumers.

Web 3 – sometimes known as "Web 3" or "Web 3.0″ – is a word you've probably heard a lot recently. It simply refers to the internet's next generation, which encourages decentralized protocols and strives to lessen reliance on giant digital corporations like Youtube, Netflix, and Amazon.

The "read/write/own" phase of the Internet is referred to as Web 3. Users may engage in the administration and management of the protocols directly, rather than merely using free tech platforms in return for our data. This means that individuals, not simply consumers or things, may become participants and stockholders.

MetaMask is a global community of developers and designers dedicated to making the world a better place with blockchain technology. The mission is to democratize access to the decentralized web, and through this mission, to transform the internet and world economy to one that empowers individuals through interactions based on consent, privacy, and free association.

### 2.5.4 Ganache

Ganache is part of the Truffle Suite ecosystem. It is a program that can be downloaded from the Internet and installed on a personal computer and works on Windows as well as Mac and Linux operating systems. It contains an IP and a port, which makes it a suitable working environment for the implementation of the project.

## 2.6 The Criteria Used in the Evaluation

There is a set of criteria that have been selected to evaluate the proposed system, despite the lack of evaluation methods for the blockchain system being a recent system, but a set of these criteria has been proposed, and will explain each criterion separately.

### 2.6.1 Time Complexities

It is the period of time that the programming code takes to execute, and there are two methods for calculating the amount of time. The first is to calculate the exact amount of time for each function or procedure that performs a certain work, and that amount is fixed. This measure is used if the proposed program uses one programming language. The second method: calculates the time estimator for all the programming codes by analyzing and designing the algorithms, and the output is in the form of a mathematical equation. The second method will be adopted because it will be more accurate and also because the proposed system will be in more than one programming language.

### 2.6.2 The Cost of Ethereum

It is the cost of designing, raising and building a website within the blockchain network, as the blockchain network, when working on it, needs a wallet, and any action that takes place within it will require funds to complete the work. Therefore, will calculate the cost of building the site, where the cost will be calculated first in the digital currency Ethereum, and then convert the estimate into the dollar currency. There are two ways to calculate the cost of Ethereum; the first: the cost of each block is calculated, and the final cost of the exchange is calculated. One Gwei is equal to 0.000000001 ETH or 10^-9Ethereum.And calculate total cost multiplication Gwei will get the price in Ethereum [53]. The second method is according to the yellow paper [54].

# Chapter Three

# Proposed System

## 3.1 Introduction

The chapter three is planned as follows: section (3.2) explains the Environment of proposed system, section(3.3) The mechanics of the Proposed System and how to enter the list of journals, section (3.4) Framework of Proposed System, section (3.5) The Architecture for the building a detailed outline of the proposed system, section (3.6) presents the details of the Algorithms used to implement the system. and in last section (3.7) the Summary.

## 3.2 Environment of Proposed System

The basic idea of the proposed system is to build a website inside a public blockchain network. This website includes most of the sites of reliable scientific journals that the student needs. The site also contains articles, research, and scientific books, as well as pictures and titles of research and everything that can be included in the real website of the scientific journal where it can be added to it, where The blockchain network contains a number of blocks (nodes), and each node contains all the transactions and information in the network. Thus, the process of storing data in a decentralized manner and the process of modification in it is a impossible process because it requires modification in more than half of the nodes in the network.

The website cannot be linked directly to the Blockchain network, as the site must be linked to a server, and then the server should be connected to smart contracts, (The contract is write the terms of the agreement between the seller and the buyer at a third party, a smart contract is a program or a transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement, Its aim is to reduce the need for third party control, losses and fraud) by using web 3.0, and then linked with the Blockchain network, which is a group of nodes connected to each other. Figure 3.1 explain the connection between the main components of the system.

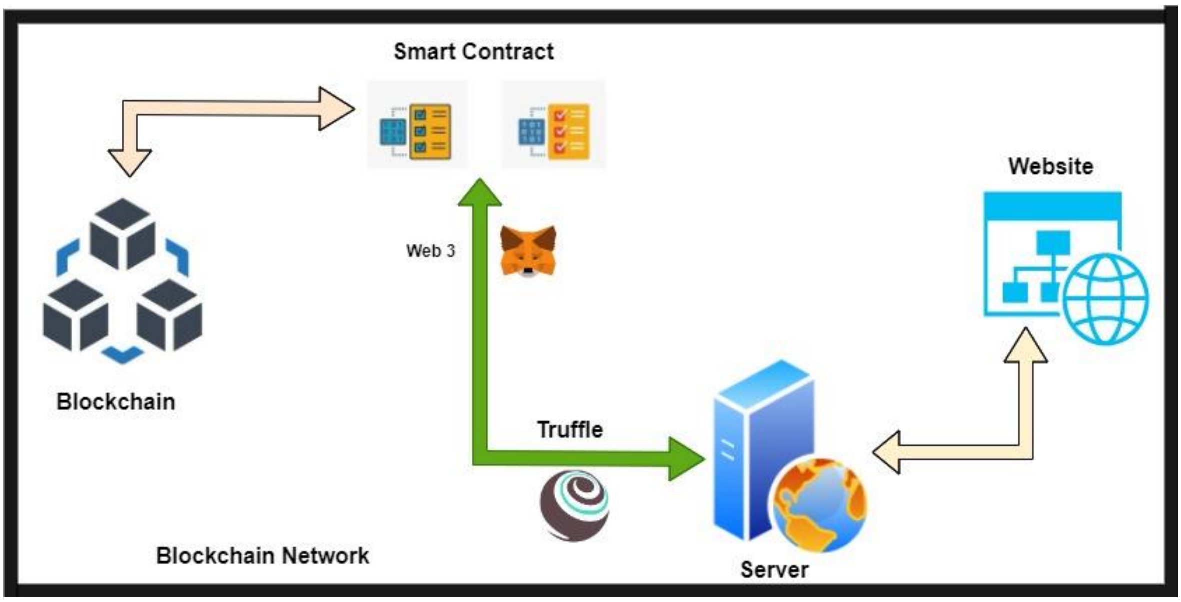


Figure 3.1 Main Components of the System

## 3.3 The Mechanism of the Proposed System

The goal of the proposed system is to protect the website from the attacks that it is currently exposed to, as most of the current attacks, are carried out through the site’s databases or the login , where most of the attacks focus on account theft (username and password) or money theft (PayPal or Visa) or ideas. Figure 3.2 shows how the data set is transmitted within the parts of the proposed system. Therefore, the proposed system consists of the following parts:

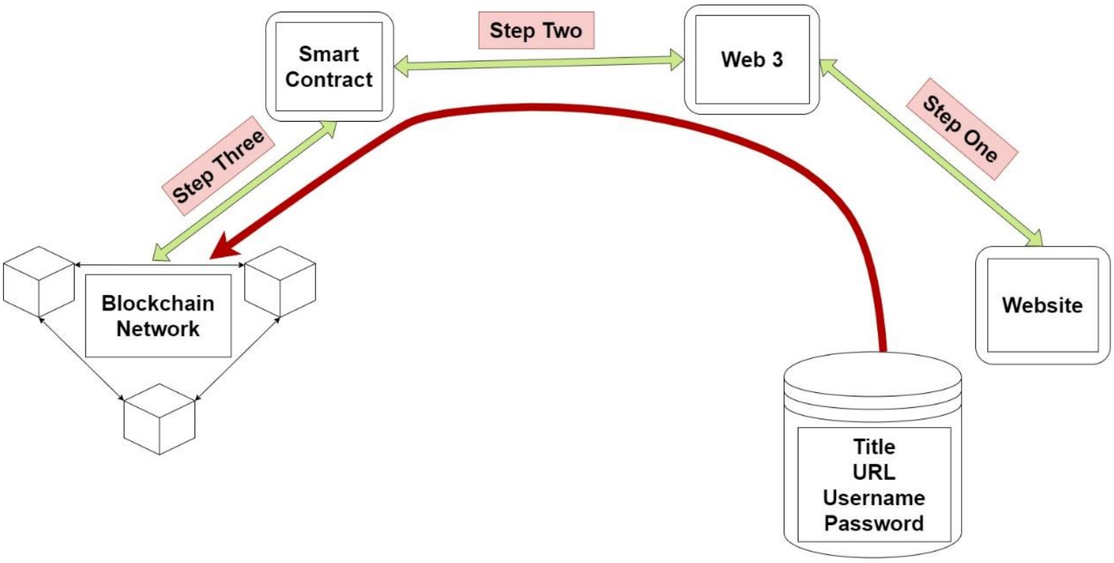


Figure 3.2 The stages of data set passing through the system

### 3.3.1 Website

The process of building a website to include all the websites to be protected and that have been agreed upon to protect them, the entire website will be built inside the page, with the same real information as the original website, and it will be save inside the blockchain network. As for the sites that have not been agreed with and whose purpose is to increase the length of the chain of the blockchain network (the longer the chain, the more difficult the process of breaking the chain becomes and it takes longer) The proposed system works with reliable scientific journals, so a distinction must be made between reliable scientific journals and predatory journals. This is done through a group of approved websites like (https://www.scopus.com/sources.uri) or (https://beallslist.net/). Would assume that the website that will be built is a reliable website, register inside each website that wanted to protect with an official account (after verifying the real site) and take the link to the website URL .As well as the name of the website or journals and stored it in a database. With these components (username, password, URL and title) fed them to the website that has been built and are stored inside the blockchain network, passing through all the components of the proposed system. This website in order to be linked to the blockchain network, needs to communicate with smart contracts, which is the door to enter into the network. The website cannot link directly to smart contracts for the reason that the programming languages used to program websites do not have the special functions to deal with smart contracts. Therefore, there must be a mediator, and this mediator is Web 3.0.

### 3.3.2 Web 3.0

It is a library have code that can send a request and receive data between the website and smart contracts.

### 3.3.3 Smart Contracts

It is a fictional name for a part of the code that is stored on the blockchain to be run by the blockchain transactions, which reads and writes data in the blockchain database. It was chosen that the data be entered into the blockchain network manually, because if it was agreed with the smart contracts to withdraw this data from an external source, it is imperative that all nodes pull this data independently for each node from the external source (outside the blockchain network). There is not a guarantee that every node in the network will receive the same answer as a result of changing external data (journal dropping out of a particular category, changing the name of the journal, etc.) with no possible way of sequencing the differences. At the point in which there is a difference between two honest contracts (mining nodes) about the state of the chain, the whole system becomes useless or worthless.

### 3.3.4 Blockchain Network

Ganache has been used as a blockchain network to store and protect data is a group and series of blocks that are linked to each other to form a chain. It is similar to the linked lists, but differs from them by some features (can review the second chapter) and it has the ability to store data inside each node of its nodes, the process of penetrating it is a difficult process and requires time and effort Great because they are built on the basis of different algorithms called consensus algorithms. These algorithms eliminate attacks on half of the network nodes in order to penetrate the network. Therefore, the longer the chain becomes, the more difficult the process of penetration becomes.

## 3.4 The Architecture for the Building a Detailed Outline of the Proposed System

The system that was created consists of four main layers. In this section, a detailed explanation will be given of all the processes that occur within each layer. Figure 3.3 represents the outline of the parts of the system.

### 3.4.1 First Layer Websites Journals

The list of journals is the first data entered into the system as it consists of (username - password- URL-title) in the case of the website refraining from providing our service to it, as well as data (research title - description - authors - cited by... etc.) in the case of the web site is satisfied with our service offered to it.

### 3.4.2 Second Layer Website Record

All this data (list of journals) enters a processing operation, where the data obtained from the refraining websites is arranged, link that appears at the bottom of the page, where the visitor can visit any website that was added for the purpose of protecting it. The data obtained from convinced websites is also processed by arranging the data and articles according to the real website of the journals, and it can be followed up through the first link, which is the page that was created within the blockchain network, which organizes all the data and articles that have to protected, among this processes are:

### A. Check (Validate)

The website (journals websites) is being evaluated, and is it a valid website or a predatory site or a hijacked site and then test if the URL website is correct and working or not.

### B. Compare

This website is compared with a special table of reputable journals (pre-configured) (from the Scopus website or the clarivate website) and is it a real website for the journals or a fake website? Are the journals predatory or sober journals?

### C. Generate ID

When adding each website, a special ID is generated for that journals (title-URL-username -password) as well as the ID of the account that made the addition (where the account that is reading or writing or adding a new link is known through the ID) and in every addition process a new ID is generated and thus There is no similarity to the network identifier values.

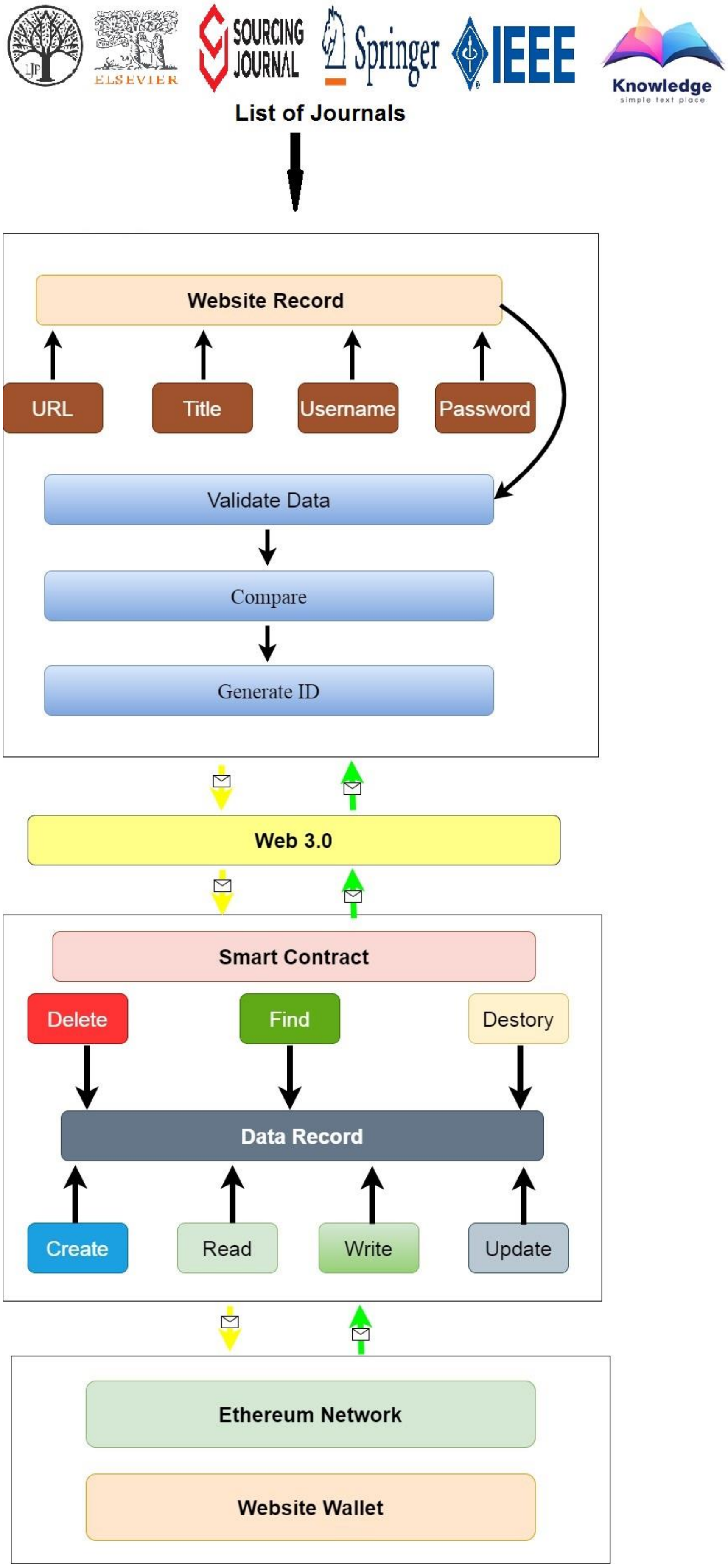


Figure 3.3 Detailed main parts of the system

After performing the processing process, the list of journals goes to web 3, which is the channel that connects the website with smart contracts and transfers data from the website to smart contracts in case of writing and from smart contracts to the website in case of reading. It also shows the account (private key) that performs this operation (reading and writing) on the website so that the blockchain network can know the validity of this account and the approval admin node and miner nodes, as well as whether this account has a wallet to pay the costs of the writing process because the process of writing or modifying requires money (Ethereum, bitcoin) As for reading, it does not require any expenses Arithmetic.

### 3.4.3 Third Layer Smart Contract

After that, the data is entered into the smart contracts, where when entering it, several operations are carried out on this data and these operations:

**Create:** Its usefulness is to store data within the blockchain network.

**Read:** This process pulls the data stored inside the blockchain and then displays it on our website.

**Write:** This process inserts data from the website into the blockchain network and stabilized it on the network and stabilized the identifier who performed the writing process to be stored with the data stored within the network so that the person who performed the writing process is known.

**Update:** The process is similar to the reading process in terms of pulling data from the blockchain network and displaying it on the website, but it is not limited to this extent, but goes beyond that by modifying the data and then sending it from the website to the blockchain network to be stored inside it in the form that has been modified .This matter it is caused by several office functions and software codes between the website, as well as the web 3 and smart contracts.

**Delete:** This process deletes data from the blockchain network

**Find:** This function searches within the blockchain network for a word, term, or anything else.

### 3.4.4 Fourth Layer Blockchain

After that, the data is transmitted to the network, which is the last station in which the data is settled, and it is called (Ethereum Network) where every person who adds a website to the network must have a wallet, which is the account that made the addition, and that any process of adding, writing or modifying must pay money and each wallet (Account) Before that can add must have digital money (Bitcoin, Ethereum,...). In the case of reading, and do not need to pay money. Each wallet has its own (private key) for each wallet.

## 3.5 Algorithms Used to Implement the System

In this section, the algorithm that are used to complete the system will be presented, as shown in Algorithm (3.1), and this algorithm will be explained.

```
Algorithm (3.1): Implementation of the proposed system
Input: Site Title, Site Link, Username, Password.
Output: Website build inside blockchain.
Step1 Setup parameter
          Str ← na                //title
          Str ← li                //link
          Str ← us                //username
          Str ← pa                //password
```

```
Step2 Setup program like CMD write the path of the location of code.
            Open Node.js
            Truffle migrate-reset
             upload smart contract to Ganache and delate the old.
Step3 Setup Convert Site.sol to Site.json
             Build the Contract artifacts & generate .json file
Step4 Setup Run Ganache program
            Start Blockchain Network
Step5 Setup Starting the server and open window
             Npm run dev
Step6 Setup upload website it is the first website in the system
          Load the Window
         call the function Init // that start to load web3 and smart contract
            Start init
Step7 Setup Return wallet
            Return to the Web3
           X = window Ethereum
           Init web3 call x
           IF x is Enable then
          Return Error     // user denied account access.
     Else
           Load APP.web3provider(http://localhost:7545).
Step8 Setup Get the necessary contract artifact file and instantiate it
with
           Get Site.json(data).
            truffle/contract
           Site artifact = data
Step9 Setup Set the provider for our contract
```

```
            App contracts Site = Truffle contract (Site artifact)
Step10 Setup Use our contract to retrieve and mark the adopted pets
           App contracts Site set provider (App. web3 Provider)
Step11 Setup Return
           Return load App
Step12 Setup Create Array
          Create Array Site []
          OUTPUT "Site Title:"
           Na = INPUT ()
          OUTPUT "Site URL:"
           Li = INPUT ()
           OUTPUT "Username:"
           Us = INPUT ()
           OUTPUT " Password:"
           Pa = INPUT ()
           Nextid =0
         Foreach (i= Start_Location; i< End_Location; i++)
                     SiteInformation (nextId, Na, Li, Us, Pa)
                     Nextid=nextid+1
        Endfor
Step13 Setup Compare the Title and URL link of website with the
table
          IF Title && URL not match then
                 Return " fake website "
          Else
 Step14 Setup That library can write, update and delete in Ethereum
                 Call experimental ABIEEncoderV2
                 Write in array Site []
                 Read from array Site []
                 Delete from array Site []
                 Find in array Site []
                 Update in array Site []
         ENDIF
Step15 END
```

The algorithm used is the algorithm for creating a website within the blockchain network, where start by opening the program Node.js and writing instructions inside it .After creating a website and it became possible to enter the websites to be protected into the system, must first make sure that the website to be added to the system is a real website or not, and whether it is the real site of the journals or a website for a predatory journals and bears the same name as the real journals.

This data will be entered through the (Web 3) channel to the smart contracts on which the processing process need is carried out, whether it is (reading, writing, updating, etc.).

After that, the information comes out from the smart contracts to the blockchain network. Here, in this section, the Ethereum platform was used, which uses the POS algorithm, which is one of the consensus algorithms used by the many blockchain networks.

The miner commits the currency (stake) he has to the blockchain network to get an opportunity to mine. A chosen random miner with a stake validates the block transaction. If a miner cannot commit to the stake, the miner can join a stake pool to participate in the mining. In POS, the miners are also called forgers. A Miner gets paid a transaction fee for successfully validating a block in the POS system.

POS system introduced the Ethereum 2.0 standards-based POS algorithm (Casper two) to solve the Byzantine General problem (BGP). In this, a two-thirds majority is required among the nodes to reach a consensus.

In POS, security is easier to achieve because a half stake is a vast amount for a single entity to lose if the malicious activity miner is caught in the blockchain. Double spending is still possible where one who has half of the stake can do malicious spending. The same technique of approving and validating transactions before committing to the blockchain will help mitigate this attack. Algorithm (3.2): pseudocode of a Proof of Stake [Chapter Two Section 2.4.10.B].[54]

Algorithm (3.2): pseudocode of a Proof of Stake (Randomized block selection) mechanism:

```
INPUT: Block_header (prev_block_hash), target value, forger_pool
Output: Fixed size valid block hash: Block_hash
        //Select forger with particular target value
Init c=0
Array selected_node[size_of_forger_pool]
For every forger I in forger_pool
//compute hash value from previous hash value of block and forgers's private key
Compute H = SHA256(prev_block_hash, private_key)
hit_value = substring (H,0,64) //extract initial 64 bits as hit value
//Compare hit value with target value
If (hit_value <=target_value)
```

```
Then selected_nods[s]=forger
Set c=c++
End if
End for
If(size(selected_node)>1)
Then
For every node n in array selected_node
Calculate difficulty_level of every node
Return node f as Forger whose difficulty level is maximum
Grant block write permissions to node f
End for
Else if (size(selected_node) =1)
Grant block write permissions to selected_node
Else
Return false // wait for either other nodes to became forger or adjust
target value
Stop
```

# Chapter Four

# Implementation and Evaluation, Analysis of Results

## 4.1 Introduction

In this chapter, the proposed system will be implemented and transformed into a viable system, and then the evaluation of results of the system built within the blockchain network will be evaluated.

In this chapter, the proposed system will be implemented, as section (4.2) simulation parameters, as section (4.3) explains the tools that were used and why they were used, in section (4.4) the obstacles that faced the project and how they were resolved? And in section (4.5) System implementation stages. And in section (4.6) Calculate time complexity. And the last section (4.7) work evaluation.

## 4.2 Simulation Parameters

The proposed system is executed in HTML, CSS, JavaScript and solidity using a laptop computer. The examinations were performed on the processor Intel(R) Core (TM)i7-4510U @ 2.00GHz (4 CPUs), ~2.6GHz 64-bit operating System, and Memory 8192 MB RAM.

## 4.3 implementation Tools of Proposed System

Among the most important tools that were used to implement this system are:

### 4.3.1 HTML, CSS, & JavaScript

**HTML** provides the basic structure of sites, which is enhanced and modified by other technologies like CSS and JavaScript. The website was built using this simple language instead of other complex and more advanced programming languages to demonstrate the work force in protecting the website from attacks.

**CSS** is used to control presentation, formatting, and layout.

**JavaScript** is used to control the behavior of different elements.

### 4.3.2 Node.js

Node.js is a program that can be downloaded from the website as in Figure (4.1A) and when it is installed on the PC. It contains all the JavaScript libraries. Any developer who develops a function in JavaScript will upload it to this website. Figure (4.1B) shows the interface of writing to node.js while writing the instructions inside it. where it is written by CMD.

A file request is handled in PHP or ASP in the following way:

1-Sends the job to the file system of the computer.

2-Waits for the file system to open and read it.

3-Returns the client's content.

4-Ready to take on the next task.

A file request is handled in Node.js in the following way:

1-Sends the job to the file system of the computer.

2-Ready to take on the next task.

3-The server returns the content to the client when the file system has opened and read the file.

*npm* is a command for JavaScript, it allows to install any library inside JavaScript, example:

*npm -v*

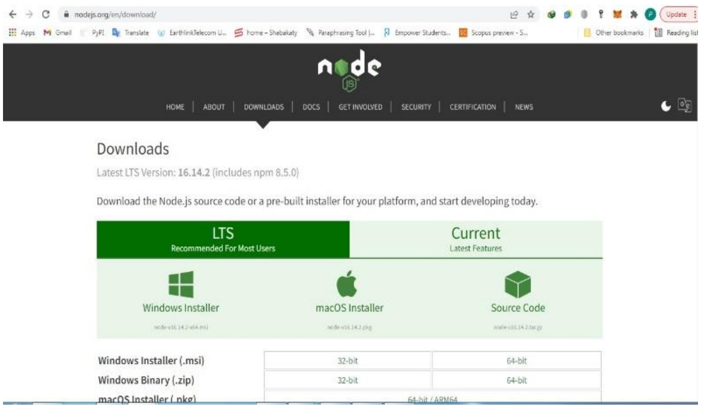
This instruction comes in the version.

*npm install (name of library) /g*

g: global.

This library can be downloaded to your personal computer.

There is a library that makes an account to make a blockchain and an account in the Ethereum currency.



Downloads

Latest LTS Version: **16.14.2** (includes npm 8.5.0)

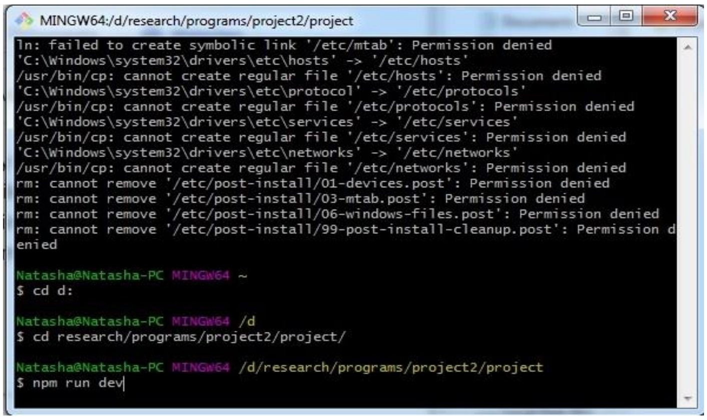
Download the Node.js source code or a pre-built installer for your platform, and start developing today.

| LTS<br>Recommended For Most Users | Current<br>Latest Features |
|---|---|

| Windows Installer | macOS Installer | Source Code |
|---|---|---|
| node-v16.14.2-x64.msi | node-v16.14.2.pkg | node-v16.14.2.tar.gz |

| | | |
|---|---|---|
| **Windows Installer (.msi)** | 32-bit | 64-bit |
| **Windows Binary (.zip)** | 32-bit | 64-bit |
| **macOS Installer (.pkg)** | 64-bit / ARM64 | |

Figure: 4.1A Website of Node.js



```
ln: failed to create symbolic link '/etc/mtab': Permission denied
'C:\Windows\system32\drivers\etc\hosts' -> '/etc/hosts'
/usr/bin/cp: cannot create regular file '/etc/hosts': Permission denied
'C:\Windows\system32\drivers\etc\protocol' -> '/etc/protocols'
/usr/bin/cp: cannot create regular file '/etc/protocols': Permission denied
'C:\Windows\system32\drivers\etc\services' -> '/etc/services'
/usr/bin/cp: cannot create regular file '/etc/services': Permission denied
'C:\Windows\system32\drivers\etc\networks' -> '/etc/networks'
/usr/bin/cp: cannot create regular file '/etc/networks': Permission denied
rm: cannot remove '/etc/post-install/01-devices.post': Permission denied
rm: cannot remove '/etc/post-install/03-mtab.post': Permission denied
rm: cannot remove '/etc/post-install/06-windows-files.post': Permission denied
rm: cannot remove '/etc/post-install/99-post-install-cleanup.post': Permission d
enied

Natasha@Natasha-PC MINGW64 ~
$ cd d:

Natasha@Natasha-PC MINGW64 /d
$ cd research/programs/project2/project/

Natasha@Natasha-PC MINGW64 /d/research/programs/project2/project
$ npm run dev
```

Figure: 4.1B Window of Node.js

### 4.3.3 Truffle

Framework, which is a set of folders arranged (classified) for the programmer to use to program smart contracts using Ethereum Structural truffle, Figure (4.2) have the important folder in truffle.

build ~~inside~~ → . json

contract ~~inside~~ → .sol solidity

migrations ~~inside~~ → .js JavaScripter

Figure: 4.2: Truffle contains

It has a set of injunctions, a set of which have been used:

**Truffle compile:** This injunction will be used in the case of creating new smart contracts for the purpose of creating an image of a contract in the formula json.

**Truffle migrate:** This injunction is used for the purpose of uploading smart contracts on the Ethereum network. This injunction must be implemented whenever update the code inside the smart contracts. Delete the migrate and make a new one.

**Truffle console:** This injunction is used to open truffle development where it gives a CMD console and from which I can do development.

**Npm run dev:** This injunction is used to start the server and open the website (Proposed System).

### 4.3.4 Meta Mask

It is an electronic wallet through which the exchange process takes place, and it is a gateway to the applications of the blockchain. It can be obtained as an extension with a browser or as an application on the mobile. It is a solution to the problem of trust between the two parties ( user & blockchain network), and it is considered a safe way to connect to applications built with the blockchain, and it is considered a key safe and entry Security, a token wallet, and everything a person needs to manage digital assets. Where it can be linked with the server of the blockchain network after creating an account inside it via the private key and placing electronic money (Ethereum) inside the wallet to be used in the completion of the programming process. Where in every process of adding information (node) to the blockchain network or modifying it, money will be required, as well as when uploading the code, and in every case of testing the code, it will need money. Figure (4.3) MetaMask in the browser.

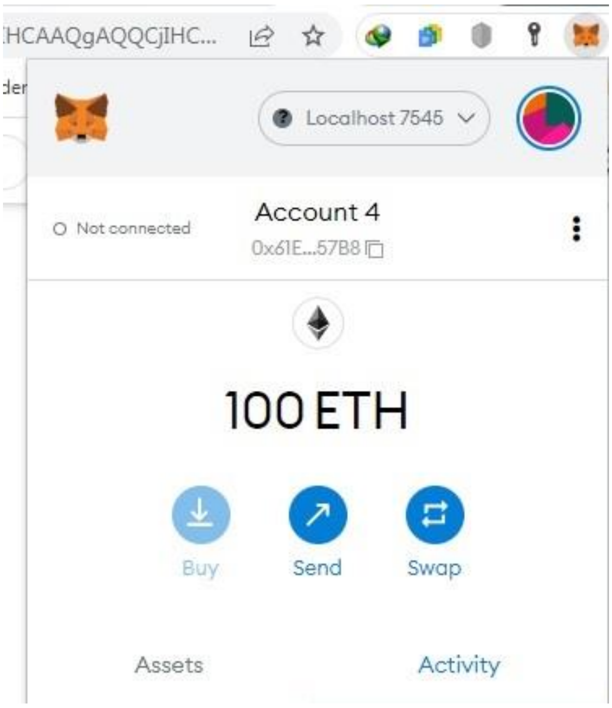
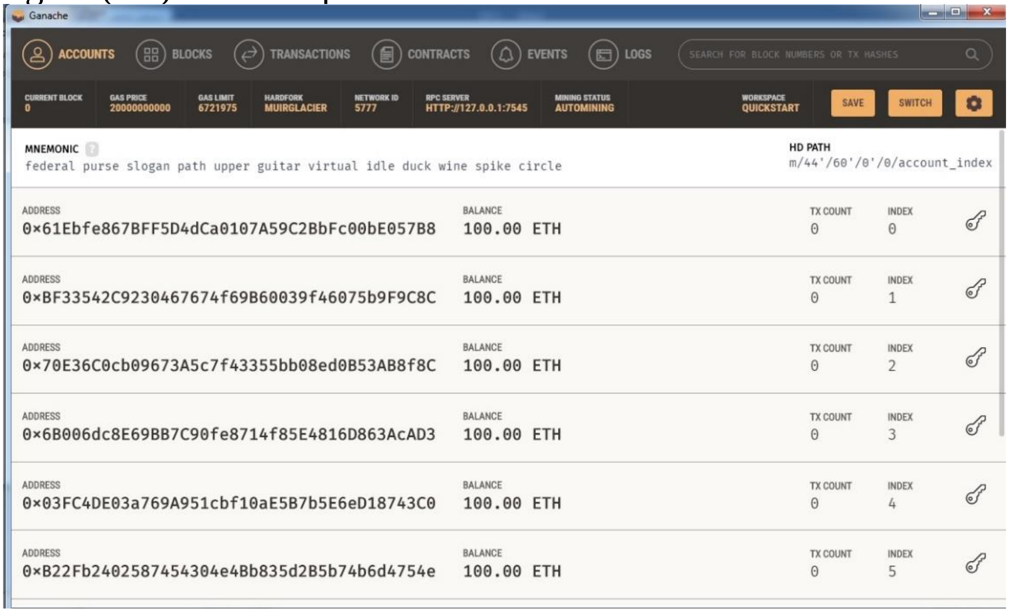


Figure: 4.3 MetaMask and 100 Ethereum

### 4.3.5 Ganache

Ganache is part of the Truffle Suite ecosystem. It is a program that can be downloaded from the Internet and installed on a personal computer and works on Windows operating systems in addition to Mac and Linux. Where it contains IP and a port, which makes it a suitable work environment for the implementation of the project. It can also be linked to truffle through the file it owns (truffle -config.js) where IP is placed and the port in the program ganache. It can also be viewed quickly, to see the current status of all accounts, including their addresses, private keys, transactions, and balances. It can be used to deploy contracts, develop applications, and run tests with quite easily.

The other feature of choosing it is a free program, where when building the system, then need to perform several tests, and the cost will become large if a program that requires costs when testing is used, and can wait until the smart contracts become free from defects to be deployed by paying the costs. It is also characterized by the speed of completion of the process, as it is considered one of the fastest platforms built with blockchain technology, as there are no obstacles hindering the process inside. Figure (4.4) Ganache platform.



CURRENT BLOCK 0 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MUIRGLACIER | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE QUICKSTART

MNEMONIC
federal purse slogan path upper guitar virtual idle duck wine spike circle

HD PATH
m/44'/60'/0'/0/account_index

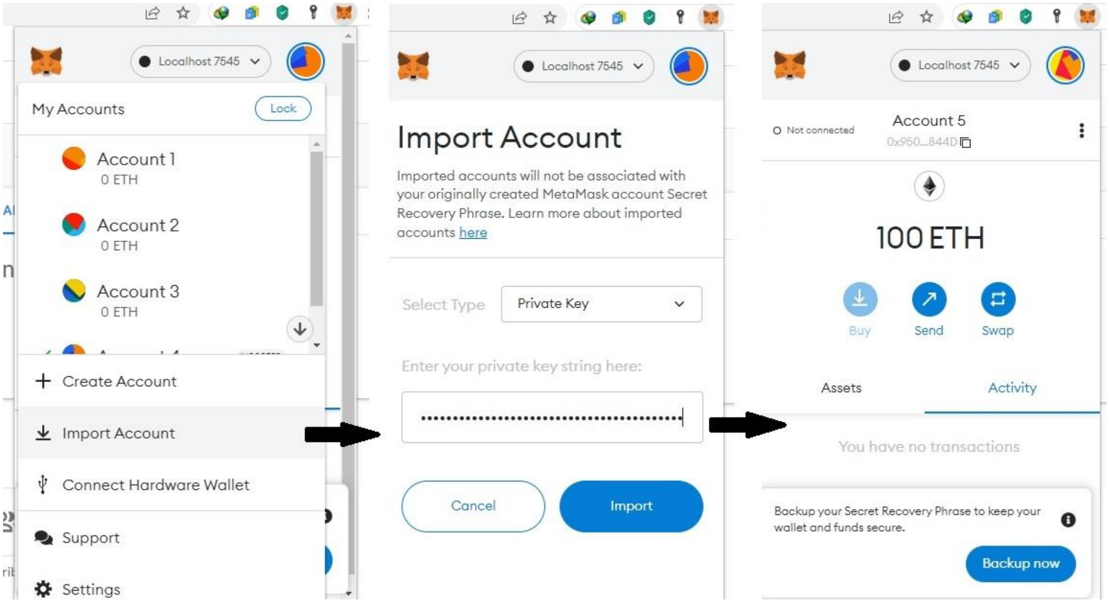
| ADDRESS | BALANCE | TX COUNT | INDEX |
|---|---|---|---|
| 0×61Ebfe867BFF5D4dCa0107A59C2BbFc00bE057B8 | 100.00 ETH | 0 | 0 |
| 0×BF33542C9230467674f69B60039f46075b9F9C8C | 100.00 ETH | 0 | 1 |
| 0×70E36C0cb09673A5c7f43355bb08ed0B53AB8f8C | 100.00 ETH | 0 | 2 |
| 0×6B006dc8E69BB7C90fe8714f85E4816D863AcAD3 | 100.00 ETH | 0 | 3 |
| 0×03FC4DE03a769A951cbf10aE5B7b5E6eD18743C0 | 100.00 ETH | 0 | 4 |
| 0×B22Fb2402587454304e4Bb835d2B5b74b6d4754e | 100.00 ETH | 0 | 5 |

Figure: 4.4 Ganache platform

## 4.4 System Implementation Stages

**The first step** before starting the process of implementation is to configure the server (Ganache) after its installation and put the settings (IP and Port) of the program and keep the server open during the execution process.

**The second stage** is going to (MetaMask) and create an account (wallet) where got the private key and then completed the procedures for creating the account and put digital money (Ethereum) inside it to be used when run tests or implement the program because every test process or implementation of any work inside The program requires a referral to this portfolio and the execution will be paid. Figure (4.5) explains how to create a wallet in MetaMask.



Imported accounts will not be associated with your originally created MetaMask account Secret Recovery Phrase. Learn more about imported accounts here

Select Type: Private Key

Enter your private key string here:

••••••••••••••••••••••••••••••••••••••

You have no transactions

Backup your Secret Recovery Phrase to keep your wallet and funds secure.

Figure (4.5): Steps for Great Wallet

**The third stage** of implementing the system, open a program (Node.js), and, using CMD directives, write the path to the folder containing the program's code in order to reach it, and then write the first directive (truffle migrate --reset) that uploads smart contracts to the blockchain network. (See 4-3-3) After that, write the instruction (npm run dev) that runs the server and opens the first Internet website, which is the site registration website.

After opening the website, the communication channel will be opened web3(MetaMask) in which a wallet was previously created.

For the purpose of registering the website of a new journal into the system, it is **first:** to verify the link of the scientific journal to be added to the program and whether it is a solid or predatory journal through solid and recognized websites. **Second:** Register within the journal's real website with the username and password so that can verify the real website if another website comes and claims that it is the real website after registering the first website.

**The first website** contains four fields for registering a new journal website:

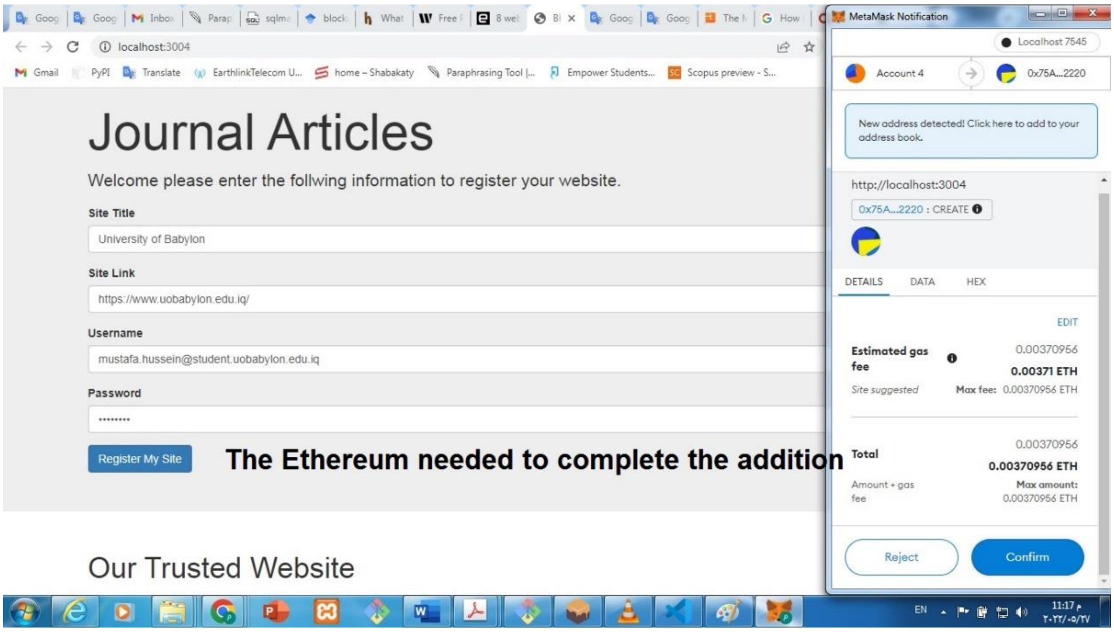
**Site Title:** It is the field in which the title of the journal is written.

**Site Link:** It is the field in which the journal link (URL) is written.

**Username:** It is the field that writes the name of the user that was previously registered on the real website of the journal.

**Password:** It is the field in which the password that was previously registered on the real website of the journal is written.

Then will press the button (Register My Site) where the wallet is opened inside (MetaMask) and according to the figure (4.6) shows the Ethereum of withdrawn funds in order to add a new website to the network. After pressing (Confirm) to confirm the payment process, the information and the website will be uploaded to the blockchain network.



# Journal Articles

Welcome please enter the follwing information to register your website.

Site Title: University of Babylon

Site Link: https://www.uobabylon.edu.iq/

Username: mustafa.hussein@student.uobabylon.edu.iq

Password: ••••••••

The Ethereum needed to complete the addition

Our Trusted Website

MetaMask Notification

Localhost 7545

Account 4 → 0x75A...2220

New address detected! Click here to add to your address book.

http://localhost:3004

0x75A...2220 : CREATE

Estimated gas fee: 0.00370956 — 0.00371 ETH

Site suggested — Max fee: 0.00370956 ETH

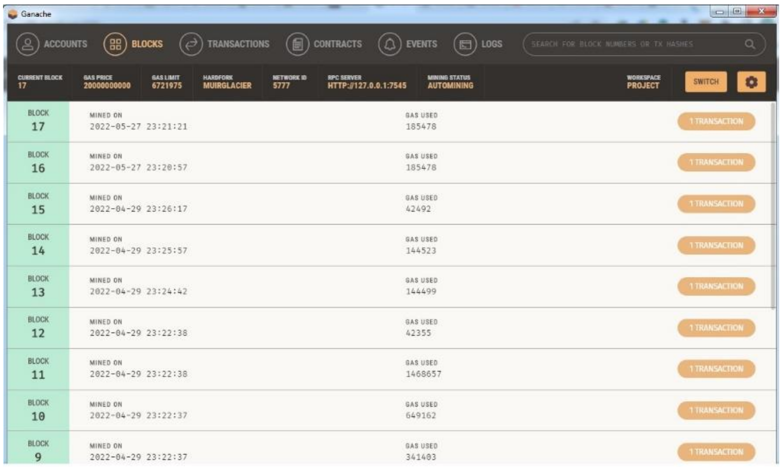
Total: 0.00370956 — 0.00370956 ETH

Amount + gas fee — Max amount: 0.00370956 ETH

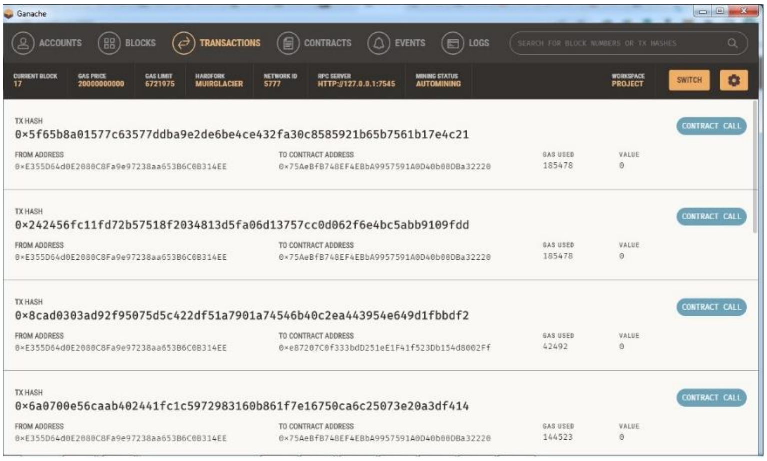
Figure (4.6): Add New Website to the System

After registering the website, will be going to the server (Ganache) where it appears on the (Blocks) page, the number of blocks (nodes) in the chain, as well as the date of creation of each node and the amount of (Ethereum) needed to create it.

On the (Transactions) page, the account that added it and the public key that sent and received it will appear. Figure (4.7, A-B) shows the page of blocks and transactions within the server Ganache.



```
CURRENT BLOCK  GAS PRICE    GAS LIMIT  HARDFORK     NETWORK ID  RPC SERVER             MINING STATUS  WORKSPACE
17             20000000000  6721975    MUIRGLACIER  5777        HTTP://127.0.0.1:7545  AUTOMINING     PROJECT

BLOCK 17   MINED ON 2022-05-27 23:21:21   GAS USED 185478    1 TRANSACTION
BLOCK 16   MINED ON 2022-05-27 23:20:57   GAS USED 185478    1 TRANSACTION
BLOCK 15   MINED ON 2022-04-29 23:26:17   GAS USED 42492     1 TRANSACTION
BLOCK 14   MINED ON 2022-04-29 23:25:57   GAS USED 144523    1 TRANSACTION
BLOCK 13   MINED ON 2022-04-29 23:24:42   GAS USED 144499    1 TRANSACTION
BLOCK 12   MINED ON 2022-04-29 23:22:38   GAS USED 42355     1 TRANSACTION
BLOCK 11   MINED ON 2022-04-29 23:22:38   GAS USED 1468657   1 TRANSACTION
BLOCK 10   MINED ON 2022-04-29 23:22:37   GAS USED 649162    1 TRANSACTION
BLOCK 9    MINED ON 2022-04-29 23:22:37   GAS USED 341403    1 TRANSACTION
```

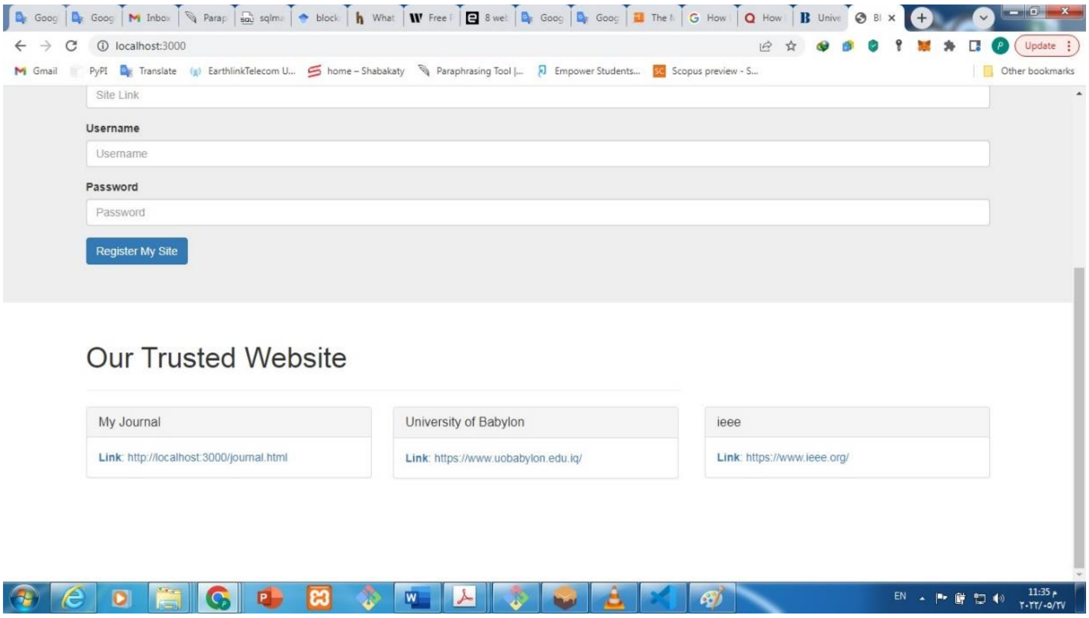


```
CURRENT BLOCK  GAS PRICE    GAS LIMIT  HARDFORK     NETWORK ID  RPC SERVER             MINING STATUS  WORKSPACE
17             20000000000  6721975    MUIRGLACIER  5777        HTTP://127.0.0.1:7545  AUTOMINING     PROJECT

TX HASH
0×5f65b8a01577c63577ddba9e2de6be4ce432fa30c8585921b65b7561b17e4c21                          CONTRACT CALL
FROM ADDRESS                                 TO CONTRACT ADDRESS                           GAS USED  VALUE
0×E355D64d0E2080C8Fa9e97238aa653B6C0B314EE   0×75AeBfB748EF4EBbA9957591A0D40b00DBa32220   185478    0

TX HASH
0×242456fc11fd72b57518f2034813d5fa06d13757cc0d062f6e4bc5abb9109fdd                          CONTRACT CALL
FROM ADDRESS                                 TO CONTRACT ADDRESS                           GAS USED  VALUE
0×E355D64d0E2080C8Fa9e97238aa653B6C0B314EE   0×75AeBfB748EF4EBbA9957591A0D40b00DBa32220   185478    0

TX HASH
0×8cad0303ad92f95075d5c422df51a7901a74546b40c2ea443954e649d1fbbdf2                          CONTRACT CALL
FROM ADDRESS                                 TO CONTRACT ADDRESS                           GAS USED  VALUE
0×E355D64d0E2080C8Fa9e97238aa653B6C0B314EE   0×e87207C0f333bdD251eE1F41f523Db154d8002Ff   42492     0

TX HASH
0×6a0700e56caab402441fc1c5972983160b861f7e16750ca6c25073e20a3df414                          CONTRACT CALL
FROM ADDRESS                                 TO CONTRACT ADDRESS                           GAS USED  VALUE
0×E355D64d0E2080C8Fa9e97238aa653B6C0B314EE   0×75AeBfB748EF4EBbA9957591A0D40b00DBa32220   144523    0
```

Figure(4.7A): Blocks

Figure(4.7B): Transactions

In order to find out where the website is stored in the program, they will be at the bottom of the website's registration fields, where they will show us the link of the journal that was registered with the rest of the journals that were previously registered. Where the journal title appears, as well as the journal link, and when click on the journal link, it will take us to the actual journal website. Figure (4.8) show the location of store the website.



Site Link

**Username**

Username

**Password**

Password

Register My Site

Our Trusted Website

My Journal
Link: http://localhost:3000/journal.html

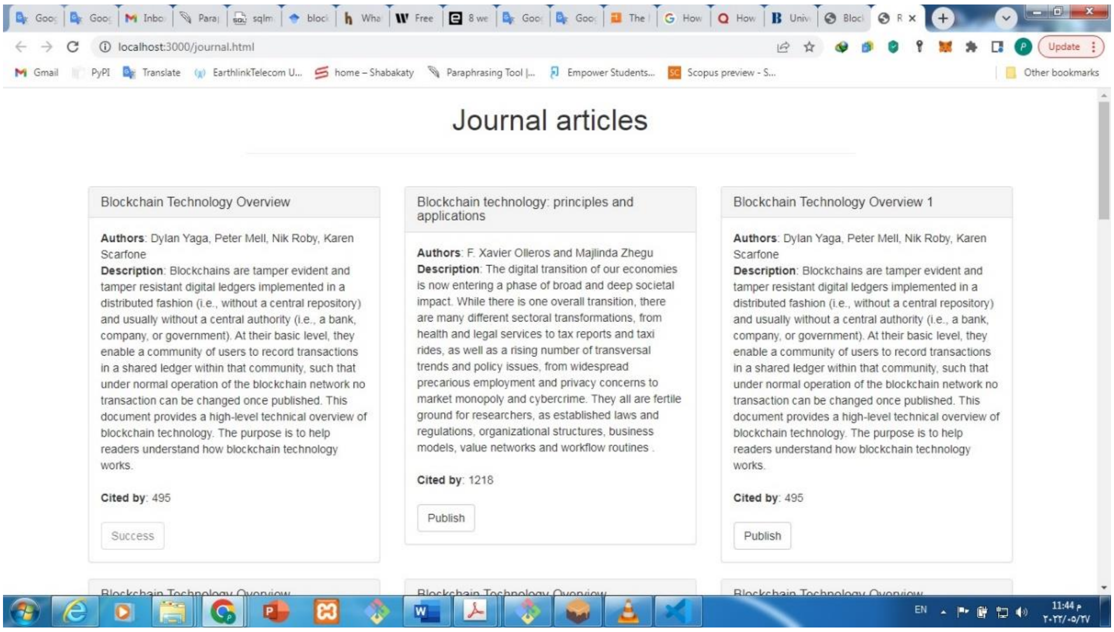
University of Babylon
Link: https://www.uobabylon.edu.iq/

ieee
Link: https://www.ieee.org/

Figure (4.8) the location of websites

The first box has its title (My Journal), where when clicking on it, it will take us to the **second website** of the program, which is the website of the scientific journal website that was created within the Blockchain network, which contains within it scientific research and published articles, where each research consists of the title of the research and then the authors And the description about the search and the last search, the number of views for this search.

And at the bottom of each search there is a button (Publish) where when press it, it will open the wallet and withdraw funds to complete the process of adding this search to the Blockchain network and make it never adjustable. The (Publish) button becomes a word (Success) and is hidden as in the figure (4.9).



localhost:3000/journal.html

Journal articles

Blockchain Technology Overview

**Authors**: Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone
**Description**: Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company, or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published. This document provides a high-level technical overview of blockchain technology. The purpose is to help readers understand how blockchain technology works.

**Cited by**: 495

Success

Blockchain technology: principles and applications

**Authors**: F. Xavier Olleros and Majlinda Zhegu
**Description**: The digital transition of our economies is now entering a phase of broad and deep societal impact. While there is one overall transition, there are many different sectoral transformations, from health and legal services to tax reports and taxi rides, as well as a rising number of transversal trends and policy issues, from widespread precarious employment and privacy concerns to market monopoly and cybercrime. They all are fertile ground for researchers, as established laws and regulations, organizational structures, business models, value networks and workflow routines .

**Cited by**: 1218

Publish

Blockchain Technology Overview 1

**Authors**: Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone
**Description**: Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company, or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published. This document provides a high-level technical overview of blockchain technology. The purpose is to help readers understand how blockchain technology works.

**Cited by**: 495

Publish

Figure (4.9) Second Website (My Journal)

## 4.5 Evaluation System

### 4.5.1- Evaluation by Previous Scientific Studies

This system was evaluated based on the study conducted by (Cyber Security Cloud, Inc.) in the first half of 2021[61], as well as the annual report of (Positive Technologies Application Firewall ) for the year 2018[62].Where in the first study, our new system will avoid more than 90% of the existing attacks, as it will avoid ( Blacklisted user agents, Web attack, Web scan, SQL injection, Brute force attack).As for the second study, it will avoid (SQL injection, Path Traversal, Cross-Site Scripting, Local File Inclusion, Information Leakage, Brute force ) that reach 82% of avoiding these attacks. Figure (4.10) the illustration of the percentage of each type of attack on websites.

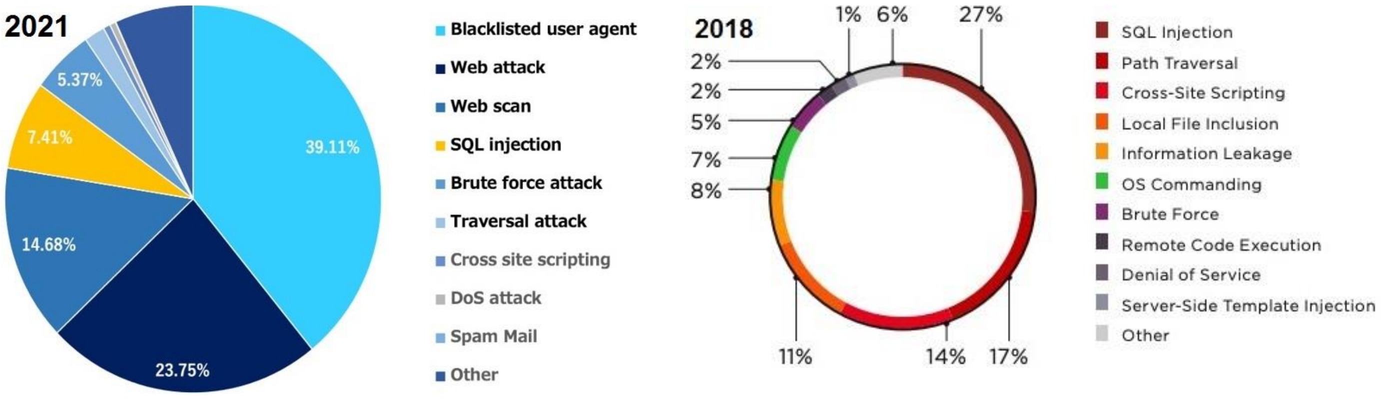


Figure: 4.10 Percentage per attack on websites for the years 2018 and 2021

This work's key contribution is to show how a permissioned blockchain framework such as the stapes of the proposed to secure website using blockchain techniques which are represented by (Preparing website, Extract data, Build blockchain, Embedded the blockchain and Verify the system) as it works to build a website from scratch to the end of the website within the blockchain. Then check the strength of the system, as it was noted that the website built inside the blockchain is less vulnerable to penetration and intrusion than the same website if it was built using traditional methods.

Where it has become possible to avoid many of the attacks of the regular and common websites, which represent more than 80% of the attacks against websites in the past few years, which were mentioned previously because the website has become built inside the Blockchain and not by traditional methods where a database type was not used SQL to save, read and modify data inside it. Also, not use PHP to design the interfaces of the page, and thus avoided many of the attacks that websites are exposed to at present.

Likewise, would did not use a central server and network, as by having hacked the main account, the system would have been hacked. A decentralized system was used, where penetration of any node in the system will not affect the system, but the different node will be isolated, and removed from the system. Also, our system does not only protect websites in a new way, but it has grown as a science seeker's guide to websites (scientific journals) to avoid fraud.

## 4.5.2 Security Analysis:

### A- SQL Injection

In the system that was implemented, no type of database was used, especially SQL where the website (frontend , backend) was built inside the blockchain network, as well as storing all the information and site data inside the network, where it was used as a storage method, thus avoiding this type of attack permanently.

### B- **Cross-Site Scripting (XSS)**

In the system was used blockchain and to solve this problem, the blockchain is used, which has security features through the concept of decentralization and through consensus algorithms, which can eliminate data changes made by hackers and make improvements to them. Where when hackers make changes and steal data, they will be successful first. But it is actually not so because blockchain uses a decentralized concept that utilizes a consensus algorithm where all transactions will be equalized on every blockchain network data manipulation efforts are useless. It only succeeds in this except for attacking all nodes of the network .

### C- Man-In-The-Middle

In the system was used blockchain and the blockchain has block hashing that can be used to close the weaknesses in the authentication process. The hashing mechanism converts data during the authentication process from a plain text form to encrypted data by converting the data into an encrypted block where the prohibited data cannot be read in order to ensure the security and confidentiality of the transferred data.Where previous experiments have proven that the blockchain will end this vulnerability and the result will be zero.

### D- Phishing and Spear Phishing

In the system was used blockchain and blockchain solve this attack because the nodes within the blockchain network are for people and this person can announce his real name or all personal information can be hidden, so the process of accessing him or guessing his geographical location or their full names and personal files is very difficult, so the process of accessing People within the blockchain network are a complex process.

On the other hand, the process of hacking the blockchain network in this way is impossible because one node will be hacked and not more than half of the network will be hacked. When matching, this hacked node will be excluded and then deleted from the network. Machine learning and artificial intelligence can also be used to detect and respond to phishing and blocked.

### E- Brute Force

In our system, the blockchain was used, and since the blockchain does not use the user name and password, but rather the public key and the private key, the algorithms used for the private key, are more complex as the length of the private key (256 bit) is longer than any password and takes a very long time, up to (437,406,288,614,505,779,110,880,159,598,765,432,098,765,432,098,765,432,098,765,432 ) years If quantitative computers are used.

If calculate the time, then will need to hack one private key and our performance on our private machine (see 4-2) it is said that your performance is 9 million BTC-addresses per second, i.e. approximately 2^23 BTC-addresses per second. Thus, brute forcing will take 2^160-23 = 2^137seconds! I guess it is more than a septillion (10^24) years.

If adjust the formula considering a private key is a 256-bit number, it would take around 2^256–23 = 2^233 seconds.

### 4.5.3 Time Complexities

When looking at the code that was written in page(index.html) and page(login.html) to build a web site, the time complexity when calculating it is Θ (1) which is the same in the normal case; so, they are equal.

By calculating the time complexity of the (main.js) program, which contains functions, loop, and direct directives, its complexity is (x+Ω(n)+6n).x is constant.

Time complexity of the (Site.sol) program is (x+3n).

When add all that Θ (1) + (x+Ω(n)+6n) + (x+3n) well be equal Ω(n)+xn. That time complexity for the system is very good it about Θ (n), figure (4.11) diagram showing the time complexities of each function.

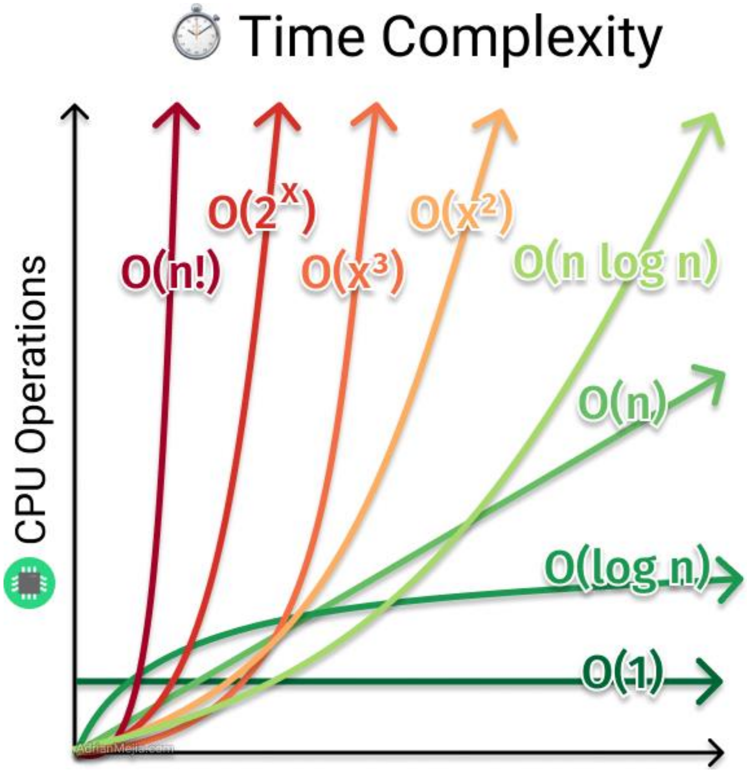


Figure: 4.11-time complexities for function

The time complexities of building a website using the traditional methods are equal to the time complexities of the proposed system because the steps of writing the code to build a web page are the same. but the difference will be in time for the proposed system because if the length of the chain within the network increases, the time will increase for the process of creating a new node, whether adding New site or update the current page.

### 4.5.4 The Cost of Ethereum

To calculate the cost of Ethereum in relation to the dollar, must know the following things:

**GAS** It's the amount of money needed to complete a transaction or run a node on the Ethereum blockchain technology.

**Gwei** is a portmanteau (a blend of words) of giga and wei. Gwei is a denomination of the cryptocurrency ether Ethereum. One Gwei is equal to 0.000000001 ETH or 10^-9 Ether.

In Ganache the GAS Price =20000000000 = Wei.

Going to website (https://eth-converter.com/) to calculate the Ethereum where Gwei = 20, then the Eth = 0.00000002. Figure (4.12) show how to calculate Eth.

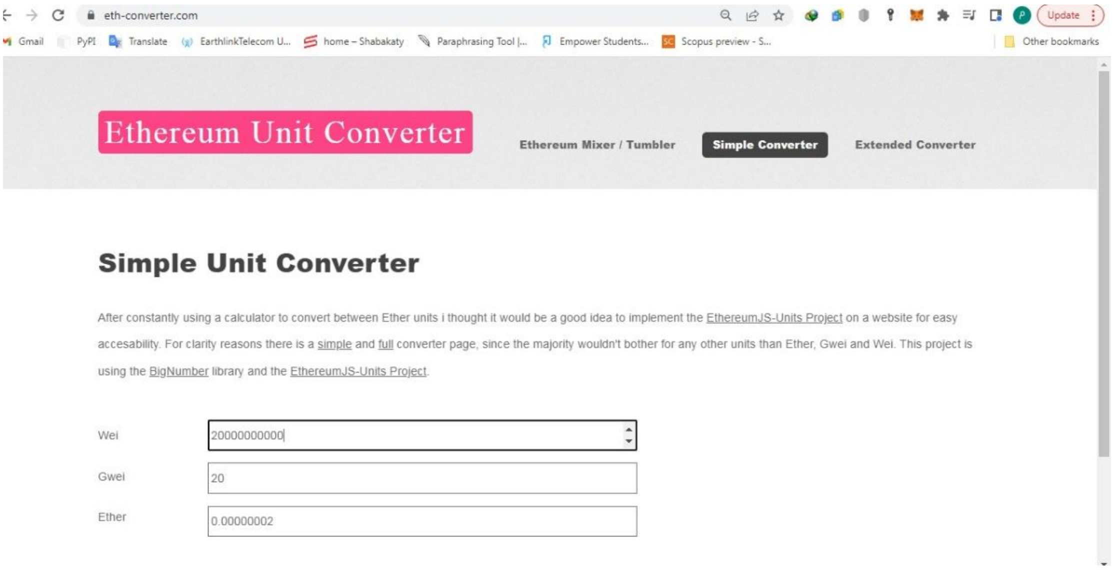
In Ganache in page Blocks will be add all GAS USED = 3068901.

Eth* Gas Used = 0.00000002*3068901= 0.06137802 Eth [63].

The cost in Dollar = Eth * 1954.68

= 0.06137802* 1954.68

= 119.9670227712 $



Simple Unit Converter

After constantly using a calculator to convert between Ether units i thought it would be a good idea to implement the EthereumJS-Units Project on a website for easy accesability. For clarity reasons there is a simple and full converter page, since the majority wouldn't bother for any other units than Ether, Gwei and Wei. This project is using the BigNumber library and the EthereumJS-Units Project.

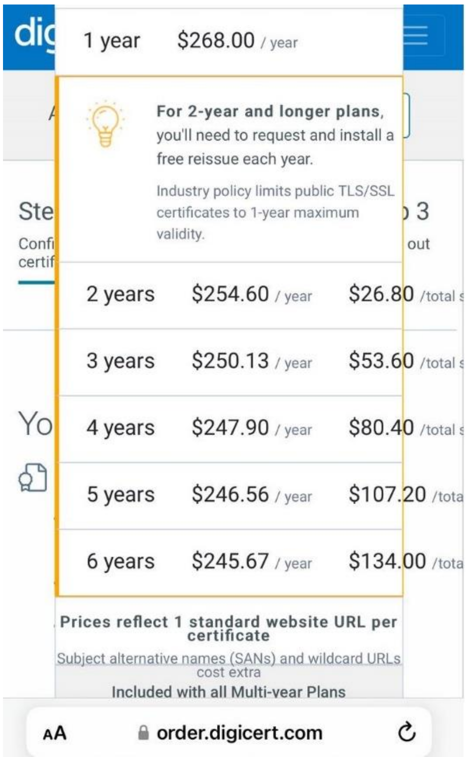
Wei: 20000000000

Gwei: 20

Ether: 0.00000002

Figure 4.12 The Cost Calculated Ethereum

And if it is compared with another usual method that is widely used today in most websites, which is the (Transport Layer Security) TLS method, the cost of protecting a website for a full year may amount to more than $268, which is a high cost compared to our new system. Figure (4.13) explain the cost of used TLS to secure website in one year.



| | | |
|---|---|---|
| 1 year | $268.00 / year | |
| 2 years | $254.60 / year | $26.80 /total s |
| 3 years | $250.13 / year | $53.60 /total s |
| 4 years | $247.90 / year | $80.40 /total s |
| 5 years | $246.56 / year | $107.20 /tota |
| 6 years | $245.67 / year | $134.00 /tota |

**For 2-year and longer plans,** you'll need to request and install a free reissue each year.

Industry policy limits public TLS/SSL certificates to 1-year maximum validity.

**Prices reflect 1 standard website URL per certificate**

Subject alternative names (SANs) and wildcard URLs cost extra

Included with all Multi-year Plans

Figure 4.13 The Cost of TLS

### 4.5.5The Most Important Criteria between the Implemented System and the Second Research in the Related Works

Table 4.1: Criterion between proposed system and save ideas

| NO | Criterion | Proposed System | Save Ideas |
|---|---|---|---|
| 1 | Blockchain properties | decentralization<br>Authentication of transaction validation | Time Stamps |
| 2 | Blockchain | To secure website | To secure ideas |
| 3 | Interest | Scientific properties | socioeconomic characteristics |
| 4 | Test | Take mor than 10 attack | Take only one website |
| 5 | On line | No | yes |

Table 4.2: Criterion between proposed system and SXX

| NO | Criterion | Proposed System | XSS |
|---|---|---|---|
| 1 | Blockchain properties | decentralization<br>Authentication of transaction validation | decentralization<br>consensus algorithm |
| 2 | Blockchain | To secure website | To secure IOT |
| 3 | Interest | Scientific properties | scientific and economic |
| 4 | Test | Take mor than 10 attack | Take only two |
| 5 | On line | No | yes |

## 4.6 The Obstacles Faced the System and How to Solve Them

**A-The first problem:** that was encountered in the project at the preparing and extract stage is when looking at a website, will all the data on the website be taken? And what is the important data (hue data) in the website that can distinguish the website from others? Will the real website owner be satisfied with the services of the new system?

The main idea of the project is to protect the website, so take had all the information on the website, and to do this, the website must be re-designed with the same previous (real) design within the blockchain network if the real website owner is convinced of the new system. If the website owner is hesitant or not convinced of the new system, will take all the components of the website using a program (code) prepared for this purpose that pulls everything that appears on the screen from the website (frontend) and as in Algorithm (4.1), pseudocode to scrape data from website that has been completed Executing it, it pulls all the information on the website and puts it into the database of each type separately, so that the website can then be created again within the blockchain network.

Algorithm (4.1): Python scrape data from a website:

**INPUT:** Website that want to scrape it

**Output:** Sort data from website each type separately

```
        // This program calculates data from the website and puts them in a database, each according to its type.

Function create database (Argument one)
    Calculate the data from the web and puts it in a database.
    Return an error creating the database.
Function Scrap website (Argument one, Argument two)
    Insert into products (title, description, price, review)
        Values ($, $, $, $)
        Insert the URL of website.  // Like https://www.msn.com
        Returns the values of the four variables, each according to its type and location on the website.
In the main function
```

```
Open control panel of website (username, Password, IP) and put them in CX.
          Loop
              If CX name = true
                  Print database
                  Call Create database
                  Print database successfully
                  CX.database = CX
            Else
                  Print ERRER
                  CX is closed
                  Exit
          If table name = true
            Table Description
            loop
                Print Table
                Call Scrap website
                Print already exists
          Else
            Print Error message
            CX is closed
     Else
      Print ok
Stop
```

This work requires effort and a long time, and to avoid that, and in order to facilitate the work and speed up the completion of the project, have begun to take what is the important information on the website (hue data) that distinguishes this website from other website, provided that this information taken from the owner’s website is not convinced so far of the project. Taking the first information is the URL that distinguishes each website since no two websites share the same URL. Then taken the website address and it is very important information so that the browser on the website can know the websites (journals) that have been added. And taken (user name and password) where login to the real website with a specific account (user name and password) and thus became part of the login registration for the website to be protected, and thus ensure that the website that was registered with is the real website and not another website, Another website came to the system and claimed that it was the desired website. Algorithm 4.2 shows how to add (Title, URL, Username, Password) to the inside of the blockchain network.

Algorithm (4.2): add new website:

**INPUT:** Build Website

**Output:** Add New Website to Blockchain Network

**// This program it takes the (username, password, URL and Name) order to be added to the blockchain network.**

```
Function handle-reg (username, password, URL, Name)
            Take the data to be stored within the blockchain network.
             Return ID how do save.
int ←—— name                              //title
int ←—— link                              //URL
int←—— username                           //username
int ←—— password                          //password
int ←—— siteinst                          //variable

Call function getaccount (error, account)      //Return error or account.
If the result error
```

```
      Return error.
      Account = 0
      Siteinst = instance.
      Return siteinst and create (username, password, URL and Name) ,
ID.
     Load window on the host.
Else
    Return Error.
Stop.
```

In the event that the owner of the website is convinced of the idea of the project, will build all the website (Front end & Backend) within the blockchain network, which is a complete security source for the electronic currency and has proven its worth, and on the one hand, the process of penetrating it is almost impossible, as it requires hacking half of the network nodes to control the network, and on the other hand that most of the attacks on websites focus on the database and login, and did not use the usual database SQL or Access to build backend, but it was stored inside the blockchain nodes and the login were used for the private key (wallet) and not the username and password. Algorithm (4.3) shows the construction of a website inside the blockchain.

Algorithm (4.3): construction of a website inside the blockchain:

**INPUT:** code in java script ***** .js

**Output:** code can deal with smart contract *.json

**// This program converting code from a language that smart contracts can't handle to one that it can handle.**

```
Call experimental ABIEncoderV2       // That can write in blockchain.
Call function Site
          Take the data to be stored within the blockchain network.
           Return ID how do save.
           int ←—— name                     //title
           int ←—— link                     //URL
           int ←—— username                 //username
           int ←—— password                 //password
           int ←—— ID                       //variable
 Array SiteInformation [] = site
Call function Create   // write in blockchain
       taken username and password of wallet.
       give URL of website.
SiteInformation [ ID, name ,link, username ,password]
Set ID=ID++
Call function read (ID, name ,link, username ,password)
Call function update (ID, name ,link, username ,password)
Call function destroy (ID, name ,link, username ,password)
Call function find (ID, name ,link, username ,password)
      For every item in sites.length
         if site[ x ] = ID
            return ID
        Else
           return site does not exist.
     Return Site.
Stop.
```

**B-The second problems:** that were encountered in the phase of building the blockchain, smart contracts are built in language solidity and web 3 is built in language JavaScript in another language. How can called function built in other a language?

To solve this problem, it is necessary to use a protocol (a language that talks between two different things) that goes to the smart contracts and then analyzes them and converts the smart contracts files from (site.sol) to (site.json) and thus it will give me a file with the same name but with a different extension. The website is built in the JavaScript language that works on the client, i.e. on the personal computer. When registering a new website, the fields (Title, URL, Username, Password) will be filled in to be sent to the smart contracts, which are shown in language solidity. It is not possible, so will send it to the web 3. Web 3 is also built in the JavaScript language, so it must understand the creation function in language solidity, what its inputs and outputs are in order to deal with it. Therefore, this protocol must be implemented (which is instruct truffle-migrate-build where it goes to a folder called contracts and extracts the first contract that analyzes it and makes it (*.json) and so on for all contracts) to convert site.sol to site.json and thus get the output of json code that can be dealt with by web 3 and gave it a clear picture of the create function. If only the address is given as input, an error will be returned in the input.

Therefore, on page main.js at line 34, when loading site.json was loaded, not site.sol. And the library truffle contract in line 37 passed the data that was fetched from json that Web 3 was able to recognize, and so it can now understand from the language solidity. Algorithm (4.4) Call site.json.

Algorithm (4.4):  Call site.json:

```
INPUT: code in java script * .js
Output: call code write in .json
            // This program will be call the code in .json not .js.
Call initContract function   // convert code from *.js to *. json.
```

```
This function will convert the code write in java script that not know smart contract to code can know smart contract it and will be .json.
Call site.json
Return website.
Stop.
```

# Chapter Five
# Conclusions and Future Works

## 5.1 Conclusions

After the process of designing and building websites within the blockchain network for the purpose of protecting it from current website attacks, it is concluded that a set of important points:

1- A website is built within the Block blockchain network for the purpose of protecting it from attacks. This process is not done in the traditional way, as it was previously, where the language Java Script had dialog with the language PHP through a group of links, and the latter was connected with the database. Since PHP has a Driver it gives the IP of MySQL, and if MySQL exists with the language PHP and put Localhost IP=172.0.0.1. After that the username and password have put, and then the name of the database.

   In our method, only IP and Port were used, and Web3 was used to access the blockchain network.

2- In the current system, the website is protected from the attacks it is currently exposed to, which largely target the database and login records, where different types of attacks have been addressed, for example (SQL Injection, Cross-Site Scripting, Man-In-The-Middle, Phishing and Spear Phishing) and thus it became possible to store data in places that are safer and more stable in terms of attacks.

3- If this system is worked on and developed in the future, will get rid of these types of attacks that are currently recognized, as more than 85% of these attacks have been avoided, and will witness the emergence of a different type of attacks due to the lack of effectiveness of these attacks on the new system.

4- The cost of creating a site and uploading it on the blockchain network may not be high if compared to the usual traditional methods currently used in our present time in terms of cost and performance where traditional methods protect data and work on encrypting it and leave the external structure unprotected and its cost is high, it may reach $250 for one site for a year One, while the cost of building and raising one site within the blockchain network reaches $120.

5- The time complexities of building a website are the same because they are the same steps and codes for building a web page, either in the traditional way or in a way according to the proposed system. but the difference will be in time for the proposed system because if the length of the chain within the network increases, the time for the process of creating a new node will increase, whether adding New site or update the current page.

6- The use of blockchain platforms on websites will speed up the use of funds faster within the website. Because a connection to the blockchain platforms requires creating a wallet with digital currencies and the process of referring to them is faster, while accessing the regular pages does not require an account that contains funds for that when using an account Bank or credit card, the normal page will crash to match the card account, and is there money in it or not? This time difference is very important in the future.

## 5.2 Suggestions for Future Works

Throughout this thesis, several topics have been identified that might further provide significant support in the field of network security systems, such as:

1- One of the most important future work that must be worked on is building our own Blockchain network, which is appropriate in terms of material cost by launching a local digital process for this purpose and suitable for work in terms of management, because it is an excellent method for protecting, preserving and transmitting data. While maintaining the features and characteristics of the blockchain network. It can also be a platform for students to benefit from for scientific and research purposes instead of the existing foreign platforms.

2- It is possible to exploit the properties of the blockchain for the purpose of protecting the servers and infrastructure of the state or its institutions to protect them from attacks or intrusion and tampering with them because the blockchain is characterized by a highly efficient protection method.

3- After building a special platform for the blockchain and launching a local digital currency to manage it and protect the internal servers of the country or institutions using the blockchain, it has become possible to protect all the sites of the country and institutions and build these sites within our blockchain network. Will reduce the time and effort spent between state departments.

4- The proposed system can be used after its development as a basic system for a university or any scientific institution, where each teacher or person will have an official account and when a person saves his information or scientific ideas in his personal account, the date of preservation will be recorded with it, and it will be hash and preserved and recorded in his name, thus preserving it from intellectual theft.

5- The proposed system can be modified to suit the work of the Ministry of Education in saving exam questions from dropping out, or saving the results of the completed stages and preserving them from loss or manipulation.

## References

[1] "Web site", www.britannica.com,11-9-2017 ‹Retrieved 21-4-2021. Edited.

[2] S. Nakamoto and A. Bitcoin, “A peer-to-peer electronic cash system,” Bitcoin.–URL https//bitcoin. org/bitcoin. pdf, 2008.

[3] D. Vujičić, D. Jagodić, and S. Randić, “Blockchain technology, bitcoin, and Ethereum: A brief overview,” 2018 17th Int. Symp. INFOTEH-JAHORINA, INFOTEH 2018 - Proc., vol. 2018–Janua, no. March, pp. 1–6, 2018.

[4]V. Morabito, Business Innovation Through Blockchain. 2017.

[5] Z. Chen and Y. Zhu, Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging. 2017.

[6] Safiani A. Faaroek, Aropria Saulina Panjaitan, Zaleha Fauziah, Nanda Septiani.(2022) . Design and Build Academic Website with Digital Certificate Storage Using Blockchain Technology.IAIC Transactions on Sustainable Digital Innovation (ITSDI).2 April 2022.

[7] Simona Ramos, Lela Melon and Joshua Ellul.Exploring Blockchains Cyber Security Techno- Regulatory Gap. An Application to Crypto-Asset Regulation in the EU.10th Graduate Conference in Law and Technology, Sciences Po.18 June 2022.

[8] Imam Riadi, Rusydi Umar and Tri Lestari, (2020). Smart Payment Application Security Optimization from Cross-Site Scripting (XSS) Attacks Based on Blockchain Technology, 2 August 2021.

[9] Dirsehan, T. (2020). Analysis of a Blockchain-based website using the technology acceptance model: the case of Save Ideas. International Journal of Diplomacy and Economy, 6(1), 17.

[10] Carl J. Case, Darwin L. King and Julie A. Case .(2020). BLOCKCHAIN: AN EMPIRICAL REVIEW OF FORTUNE 500

WEBSITE POSTINGS AND USAGE.Journal of Business and Behavioral Sciences,Volume 32, Number 2; Fall 2020.

[11] Singh, R., Tanwar, S., & Sharma, T. P. (2019). Utilization of blockchain for mitigating the distributed denial of service attacks. Security and Privacy.

[12] Shorman, S., & Allaymoun, M. (2019). Authentication and Verification of Social Networking Accounts Using Blockchain Technology. International Journal of Computer Science and Information Technology, 11(6), 1–11.

[13] Dadkhah, M., Seno, S. A. H., & Borchardt, G. (2017). Current and potential cyber attacks on medical journals; guidelines for improving security. European Journal of Internal Medicine, 38, 25–29.

[14] Alyson Shontell (29-6-2011), "This Is What The First-Ever Website Looked Like", "www.businessinsider.com" ,Retrieved 21-4-2021. Edited.

[15] ELIZABETH NIX (30-8-2018), "The World’s First Web Site" ، www.history.com, Retrieved 21-4-2021. Edited.

[16] How Many Websites Are There?", websitesetup.org,28-5-2020 ، Retrieved 21-4-2021. Edited.

[17] "Static vs Dynamic Website", www.geeksforgeeks.org,22-12-2020 ، Retrieved 21-4-2021. Edited.

[18] "Websites URL Registration", www.tutorialspoint.com, Retrieved 21-4-2021. Edited.

[19] "Websites URL Registration", "https://en.wikipedia.org/wiki/Website",21-4-2021. Edited.

[20] "flux-academy" ," https://www.flux-academy.com/blog/ 12-popular-

website-types-and-how-to-design-them", Retrieved 21-4-2021. Edited.

[21]"hostgator", " https://www.hostgator.com/blog/popular -types-websites-create/" , Retrieved 21-4-2021. Edited.

[22] ACIRS."How to choose a solid scientific journal to publish research content?".URL:www.acjrs.com.(visited on 07/03/2022).

[23] Bitcoinwiki, “Proof of Stake”, [online] Available: https://en.bitcoin.it/wiki/Proof_of_Stake, (accessed February 28, 2021).

[24] "Malwarebytes"," https://www.malwarebytes.com/data-breach", Retrieved 21-4-2021. Edited.

[25] "entrepreneur", " https://www.entrepreneur.com/article/241620", Retrieved 21-4-2021. Edited.

[26] "IPA IT SECURITY CENTER (ISEC) - INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN"," How to Secure Your Website 5th Edition", April 2011.

[27] "Cookies Destroy Bitcoin Anonymity During Transactions ",Ray Walsh,"https://proprivacy.com/privacy-news/cookies-bitcoin-anonymity", Retrieved 10-12-2019. Edited.

[28] Narayanan, Arvind, et al. “Bitcoin and cryptocurrency technologies: a comprehensive introduction”. Princeton University Press, 2016.

[29] Nakamoto, Satoshi, and A. Bitcoin. "A peer-to-peer electronic cash system." Bitcoin.–URL: https://bitcoin. Org/bitcoin. Pdf (2008).

[30] Swan, Melanie. "Blockchain for business: next-generation enterprise artificial intelligence systems." Advances in computers. Vol. 111. Elsevier, 2018. 121-162.

[31] Underwood, Sarah. "Blockchain beyond bitcoin”. Communications of the ACM 59.11 (2016): 15-17.

[32] Thakur, Mukesh. "Authentication, Authorization and Accounting with

Ethereum Blockchain." URL: https://helda. Helsinki. Fi/handle/10138/228842 (visited on 07/03/2020) (2017).

[33] Jutila, Laura. "The blockchain technology and its applications in the financial sector." (2017).

[34] Yaga, Dylan, et al. "Blockchain technology overview." Draft NISTIR 8202 (2018).

[35] Lin, Iuon-Chang, and Tzu-Chun Liao. "A Survey of Blockchain Security Issues and Challenges." IJ Network Security 19.5 (2017): 653-659.

[36] Bashir, Imran. “Mastering Blockchain”. Packt Publishing Ltd,2017.

[37] Zheng, Zibin, et al. "An overview of blockchain technology: Architecture, consensus, and future trends." 2017 IEEE international congress on big data (BigData congress). IEEE, 2017.

[38] Es-Samaali, Hamza, Aissam Outchakoucht, and Jean Philippe Leroy. "A blockchain-based access control for big data." International Journal of Computer Networks and Communications Security 5.7 (2017): 137.

[39] Costa, Pier Francesco.” Ethereum blockchain as a decentralized and autonomous key server: storing and extracting public keys through smart contracts”. Diss.

[40] Chen, Zhixong, and Yixuan Zhu. "Personal archive service system using blockchain technology: case study, promising and challenging." 2017 IEEE International Conference on AI & Mobile Services (AIMS). IEEE, 2017.

[41] Berryhill, Jamie, Théo Bourgery, and Angela Hanson. "Blockchains unchained." (2018).

[42] Meunier, Sebastien. "Blockchain 101: What is blockchain and how does this revolutionary technology work?" Transforming climate finance and green investment with Blockchains. Academic Press,

2018.23-34.

[43] Triantafyllidis, Nikolaos Petros, and T. N. O. Oskar van Deventer. “Developing an Ethereum blockchain application”. Diss. Ph. D. Thesis, University of Amsterdam, Amsterdam, the Netherlands, 2016.

[44] "Packt","Hands-On Blockchain with Hyperledger" Edition",Dr. Salman A. Baset , April 2018.

[45] Wikipedia, “NEM (cryptocurrency)”, [online] Available: https://en.wikipedia.org/wiki/NEM_(cryptocurrency)#Proof-ofimportance,(accessed February 28, 2021).

[46] Grech, Alexander, and Anthony F. Camilleri. "Blockchain in education." (2017).

[47] Haffke, Florian. "Technical Analysis of Established Blockchain Systems." Master's thesis. Technical University of Munich, SW Engineering for Business Informatics (2017).

[48] Type of blockchain, "101 Blockchains"[online] Available: https://101blockchains.com/types-of-blockchain/,(accessed February 28, 2021).

[49] Type of blockchain, "Data Flair"[online] Available: https://data-flair.training/blogs/types-of-blockchain/,(accessed February 28, 2021).

[50] Bitcoinwiki, “Proof of work”, [online] Available: https://en.bitcoin.it/wiki/Proof_of_work, (accessed February 28, 2021).

[51] Wikipedia, “Proof of Space”, [online] Available: https://en.wikipedia.org/wiki/Proof-of-space, (accessed February 28,2021).

[52] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," in 3rd OSDI USENIX, Feb 1999, pp. 173-186.

[53] "Coin Academy" , https://thecoinacademy.co/blockchain/how-to-calculate-the-cost-of-an-ethereum-erc20-transaction-in-dollars/ , Retrieved Edited.15-6-2022.

[54] " yellow paper", "ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER", DR. GAVIN WOOD, BERLIN VERSION b2d0dbf - 2022-05-06.

# الخلاصة:

يومًا بعد يوم، يتم استخدام المواقع الإلكترونية على نطاق واسع من حيث إيداع البيانات واسترجاعها، لذا فهي تتطلب تطويرًا وتوسعًا مستمرين. من ناحية أخرى، يتم أيضًا تطوير العديد من الطرق لمهاجمتها. لذلك، هناك حاجة لاقتراح طريقة (مصقولة) كإجراء مضاد يحتفظ بمسارات الهجمات الحالية. تم اقتراح إطار عمل لاستخدام البلوك جين كتقنية لتأمين مواقع الويب. تعتبر شبكة البلوك جين بشكل عام شبكة قوية وثبتت قدرتها من حيث الأمان، وبالتالي فهي تستخدم بشكل طبيعي لحماية البيانات الثمينة لمواقع الويب.

تتكون منهجية البحث في الأطروحة من عدة مراحل. وقد اشتملت على خطة أولية للبحث، ودراسة الأعمال ذات الصلة، ومن ثم نقدها، وتصميم النموذج وتنفيذها، والتحقق من صحتها وتقييمها، وأخيراً تقرير العمل.

تقدم هذه الأطروحة نظامًا مقترحًا يقوم ببناء موقع ويب كامل ضمن شبكة البلوك جين، حيث تتم حماية المواقع عن طريق إضافتها إلى النظام باستخدام عناصر يمكن من خلالها يمكن تمييز الموقع الحقيقي من المواقع الوهمية او المفترسة، وهي (العنوان، URL لموقع الويب، اسم المستخدم وكلمة المرور (بعد التسجيل معهم على الموقع الحقيقي)) وكذلك تم إنشاء موقع ويب كامل داخل شبكة بلوك جين يحتوي على جميع تفاصيل المواقع الموجودة. وبالتالي، تم استغلال خصائص البلوك جين من اللامركزية والاستقرار والخصوصية لحماية المواقع.

يتم تقييم النظام المقترح وفقًا لمجموعة من المعايير، بما في ذلك نسبة نتائج التكلفة حوالي 119 دولارًا، وهو أقل مما لو تم استخدام طريقة Transport Layer Security) TLS)، حيث تصل إلى 268 دولارًا، فضلًا عن نتائج الوقت النسبة المئوية Θ (N)، وهو نفس الوقت المستخدم في إنشاء موقع ويب بالطرق التقليدية، ولكن يزداد الوقت إذا ما زاد طول السلسلة. تم تقييم العمل بمقارنته بالأعمال السابقة وثبت أنه أفضل منهم في النتائج. بناءً على الدراسة التي أجرتها شركة (Cyber Security Cloud، Inc.) في النصف الأول من عام 2021 ، وكذلك التقرير السنوي لـ (Positive Technologies Application Firewall) لعام 2018 ، حيث في الدراسة الأولى ، سيتجنب نظامنا الجديد أكثر من 90٪ من الهجمات الحالية سوف تتجنب ( Blacklisted user agents, Web attack, Web scan, SQL injection, Brute force attack) أما الدراسة الثانية ، فستتجنب ( SQL injection, Path Traversal, Cross-Site Scripting,

(Local File Inclusion, Information Leakage, Brute force التي تصل إلى 82٪ من تجنب هذه الهجمات.

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابل ـ كلية تكنولوجيا المعلومات
قسم البرمجيات

# تأمين المواقع الإلكترونية بالاعتماد على سلسلة الكتل

رسالة
مقدمة إلى مجلس كلية تكنولوجيا المعلومات في جامعة بابل كجزء من متطلبات الحصول على درجة الماجستير في تكنولوجيا المعلومات / البرمجيات

**من قبل**

**مصطفى سعدي حسين صالح**

**بإشراف**

**د. مهند محمد جاسم الياسري**

**1444هـ** **2022م**