ISTANBUL TECHNICAL UNIVERSITY ★ INFORMATICS INSTITUTE

APPLYING BLOCKCHAIN IN EXCHANGING DATA

M.Sc. THESIS

Raneem SEIRAWAN

Department of Applied Informatics
Cybersecurity Engineering and Cryptography Programme

JUNE 2019

ISTANBUL TECHNICAL UNIVERSITY ★ INFORMATICS INSTITUTE

APPLYING BLOCKCHAIN IN EXCHANGING DATA

M.Sc. THESIS

Raneem SEIRAWAN
(707151028)

Department of Applied Informatics

Cybersecurity Engineering and Cryptography Programme

Thesis Advisor: Assoc.Prof. Enver ÖZDEMIR

JUNE 2019

İSTANBUL TEKNİK ÜNİVERSİTESİ★ BİLİŞİM ENSTİTÜSÜ

VERİ TRANSFERINDE BLOK ZİNCİRI UYGULAMASI

YÜKSEK LİSANS TEZİ

Raneem SEIRAWAN
(707151028)

Bilişim Uygulamları Anabilim Dalı

Bilgi Güvenliği Mühendisliği ve Krıptografı Programı

Tez Danışmanı: Doç. Enver OZDEMIR

HAZİRAN 2019

Raneem SEIRAWAN, a M.Sc./a Ph.D. student of ITU Informatics Institute student ID 707151028, successfully defended the thesis/dissertation entitled "APPLYING BLOCKCHAIN IN EXCHANGING DATA", which he/she prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor :	**Doc. Dr. Enver OZDEMIR** İstanbul Technical University	……..
Jury Members :	**Prof. Dr. Oguzhan KULEKCI** İstanbul Technical University	……..
	Dr. Deniz SARIER TUBITAK BILGEM	……..

Date of Submission : 3 May 2019
Date of Defense : 12 June 2019

FOREWORD

Above all, I would like to express my deepest gratitude to my advisor, Associate Professor Dr. Enver Özdemir for his guidance, encouragement, insight and extraordinary support throughout my academic journey. I offer sincere thanks to my examining committee members, Professor Dr. Oğuzhan Külekci and Dr. Deniz Sarier for their valuable suggestions and positive contributions. I want to thank all colleagues for their support, time and knowledge. In Istanbul, a city that was once foreign to me, I owe a huge thank you to my friends who gave me the chance to be part of their community. I want to thank my husband Ahmad who has always been my biggest supporter. And my greatest gratitude goes to my daughter Juliana who always gives me the hope and drive to continue. I would like to express my deepest gratitude and thanks to my family; father, sisters, and brothers. I hope that my mother's spirit is somewhere watching me and I hope that she will be proud of me as she always wanted.

June 2019 Raneem SEIRAWAN

TABLE OF CONTENTS

Page

ABBREVIATIONS

ID : Identity
H :Hospital
$\mathbf{k_A^+}$: Public key
$\mathbf{k_A^-}$: Private key
$\mathbf{s_A}$: Symmetric key
R : Healthcare record
SE : Symmetric key encryption function
PE : Public-private key encryption function
D : Decryption function
$\mathbf{R'}$: Health record encrypted by the symmetric key s_A
$\mathbf{s_A'}$: Symmetric key encrypted by the private key k_A^-
$\mathbf{M_j}$: Message constructed form transaction details
$\mathbf{L_j}$: Public ledger
h : Cryptographic hash function

LIST OF TABLES

Page

LIST OF FIGURES

Page

APPLYING BLOCKCHAIN IN EXCHANGING DATA

SUMMARY

The misuse of critical medical data is preventing medical organizations from providing the proper healthcare service for the patients. In other words, these organizations may not be able to fulfill the patient's needs. There is a statistic says that “Up to 40% of healthcare provider data records are filled up with errors or misleading information”.

A lot of healthcare organizations nowadays depend on outdated systems for storing patients’ healthcare data. These systems have old ways of storing and reviewing the data which is time and efforts consuming. Therefore, the process of examining a patient’s earlier data and diagnose it accordingly became a difficult and tedious task. The most important problem which is also time-consuming and tedious is exchanging health information with a third party. This problem increases the costs in the healthcare industry. As the patients have no control over their information, this information can be stolen easily and hence identity and sensitive data of individuals can be used for unauthorized purposes. In spite of having computers/servers/IoT at all of the healthcare organization, we are still not able to gather, test, analyze and exchange the medical information in a secure manner. The healthcare systems now need a flexible transparent easily operable and economically efficient systems, and that was our aim is to construct a trusted protocol which provides confidentiality to the healthcare system in various situations.

This proposed protocol in this thesis will allow only the authorized users to access the health record of the patient for a certain amount of time under different specified conditions depending on blockchain technology. Preserving privacy is crucial and required in this type of process and the blockchain technology provides additional high levels of integrity/security and privacy.

VERİ TRANSFERİNDE BLOK ZİNCİRİ UYGULAMASI

ÖZET

Kritik tıbbi verilerin kötüye kullanılması, sağlık kuruluşlarının hasta için uygun sağlık hizmeti sunmasını engellenmektedir. Başka bir deyişle, bu kuruluşlar hastanın ihtiyaçlarını karşılayamayabilmktedir. Bir istatistiğe göre: "Sağlık hizmeti sağlayıcısı veri kayıtlarının% 40'ına kadarı hata veya yanıltıcı bilgi ile dolu". Günümüzde pek çok sağlık kuruluşu, hastaların sağlık verilerinin depolanması için eski sistemlere dayanmaktadır. Bu sistemler verileri depolamak ve gözden geçirmek için eski yöntemlere sahiptir. Bu nedenle, hastanın önceki verilerini incelemek ve buna göre teşhis koymak zor ve sıkıcı bir iş haline gelmektedir. Ayrıca zaman alıcı ve sıkıcı olan en önemli sorun üçüncü tarafla sağlık bilgisi alışverişinde bulunmaktır. Bu sorun sağlık sektöründe maliyetleri arttırmaktadır. Hastalar bilgileri üzerinde kontrol sahibi olmadıklarından, bu bilgiler kolayca çalınabilir ve böylece kişilerin kimlikleri ve hassas verileri yetkisiz amaçlar için kullanılabilir. Tüm sağlık kuruluşlarında bilgisayar / sunucu / IoT olmasına rağmen, tıbbi bilgileri güvenli bir şekilde toplayamıyor, test edemiyor, analiz edemiyor ve değiş tokuş edemiyoruz. Sağlık sistemlerinde artık esnek, kolay işlenebilir ve ekonomik açıdan verimli bir sisteme ihtiyaç duyulmaktadır ve amacımız çeşitli durumlarda sağlık sistemine gizlilik sağlayan güvenilir bir protokol oluşturmaktı.
Bu protokol, yalnızca yetkili kullanıcıların, blok zinciri teknolojisine bağlı olarak belirtilen farklı koşullar altında belirli bir süre boyunca hastanın sağlık kaydına erişmesini sağlar. Taklit edilebilirlik bu tür bir süreçte çok önemlidir ve gereklidir. Blockchain teknolojisi ek yüksek seviyede bütünlük güvenlik ve gizlilik sağlar.
Blockchain teknolojisi, bugünlerde dünyayı fırtınaya sokan en yıkıcı teknolojilerden biri olarak. Blokzincirin'in özü, ağda gerçekleşen işlemleri ve etkinlikleri izleyen dağıtılmış bir defter olmasıdır. Bir blok zincirin en benzersiz özeli dağıtılmış deftere bir parça bilgi eklendiğinde, hiç kimsenin değiştiremeyeceğidir. Bir blok zinciride saklanan bilgiler bütünüyle güvendedir. Herhangi birinin bir blokta değişiklik yapması için, bundan sonraki tüm bloklarda değişiklik yapması gerekmektedir.

Bir blok zincirin çalışması uzun sürmektedir ve üç ana prensibe dayamaktadır. Bu ilkelerin derlenmesi, blockchain'in güvenli ve güvenli dijital ilişkiler, özel anahtar şifreleme, dağıtılmış defterler ve kimlik doğrulama sağlamalarını sağlar.
Blockchain'in önümüzdeki yıllarda sağlık sektörünü kötü etkilermesi konusundaki kapsamlı vizyon, mevcut sistemi etkileyen sorunları çözmek olacaktır. Herhangi bir zamanda doktorlar, hastalar ve eczacılar tarafından tüm bilgilere kolayca erişilebilen bir sağlık sistemi hayal edelim. Blokzincir, tek bir ortak sağlık bilgisi veritabanının oluşturulmasına ve paylaşılmasına izin vermektedir.

Bu sistem, kullandıkları elektronik tıbbi sistem ne olursa olsun, sürece dahil olan tüm kuruluşlar tarafından erişilebilir olacaktır. Bu, doktorların hasta bakımı ve tedavileri için daha fazla zamana şahislemesi izin verirken daha yüksek güvenlik ve şeffaflık

sunmaktadır. Ayrıca sırayla nadir görülen herhangi bir hastalık için klinik denemeleri ve tedavi terapilerini kolaylaştıracak araştırma istatistiklerinin daha iyi paylaşılmasını da sağlayacaktır.

Bir sağlık sisteminde, sağlık hizmeti çözüm sağlayıcıları arasında sorunsuz veri paylaşımı tanı, etkili tedaviler ve düşük maliyetli ekosistemde doğruluk sağlayabilmektedir. Hasta verilerinin günlük büyümesi, içinden geçen içgörüden en etkin şekilde yararlanabilmek için kaynakların uygun şekilde kullanılmasını gerektirmektedir.
Sağlık hizmeti için blok zincir, sağlık hizmeti ekosisteminin birden fazla biriminin senkronize kalmasını ve yaygın olarak dağıtılan bir defterde veri paylaşmasını sağlmaktadır. Böyle bir sistem kullandığında, katılımcılar bütünlük ve güvenlik için ek seçeneklere bakmak zorunda kalmadan sistemde gerçekleşen verilerini ve diğer etkinliklerini izleyebilir ve takip edebilirler. Ağ katılımcıları için gereksinimler ve erişim izinleri uyarınca, iki tip blok zinciri kullanılabilir:

İzin Verilen Blokajlar: Adından da anlaşılacağı gibi, bu tip blokajlar, ağın katılımcıları arasında gerçek zamanlı verilerin yalnızca izin verilen bir temelde paylaşılmasını sağlar. İzin verilen bir blok zinciri, sisteme katılan tüm katılımcıların ağa erişebildiği kapalı bir ağdır. Bilgi alışverişinde bulunmak ve güvenli işlem yapmak için kurum ve kuruluşlar içinde kurulur ve kullanılır. Bir işlem bir fikir birliği ile işlendikten sonra kalıcı bir kayıt olarak değerlendirilir ve mevcut blok zincirine yeni bir blok olarak eklenir.

İzinsiz blok zinciri: Blokajlar, daha azına izin verir. Herhangi birinin kendi adresini oluşturması ve etkileşime girmesi için herkese erişim sağlar.
Engelleme zincirleri izinsizdir ve bu da bir kimseye kendi adresini oluşturma ve ağ ile etkileşime girme erişimini sağlar. İzinsiz bir sistemin en popüler örneklerinden biri, herkesin kendi web sitesini oluşturmasını sağlayan internet. Benzer şekilde, daha az blok zinciri izninde, ağdaki herkes ağdaki adreslerini oluşturarak aynı ağdaki diğer katılımcılarla etkileşime girebilir.

Bunlardan ikisi arasında, özel veya izin verilen blokajlar, sağlık hizmetleri ekosistemi içinde doğru kararları almak için sağlık hizmetlerinde etkin bir şekilde kullanılabilir. Blokzinciri teknolojisinin sağlık hizmetlerinde kullanılması, daha fazla araştırıldığı için çok fazla potansiyel barındırmaktadır. Değişmezlik, güven azlığı ve ademi merkeziyetçilik gibi özelliklere sahip olan Blokzincirinin dağıtık teknolojisi, sağlık sektörüne sahtekarlığı tespit etme, işletme maliyetlerini düşürme, süreçleri yumuşatma, işlerin çoğaltılmasını kaldırma ve şeffaflığı sağlık ekosisteminde uygulama fırsatları sunar.
Nüfus sağlığı yönetiminde bugüne kadar karşılaşılan en büyük zorluklar veri güvenliği, paylaşılabilirlik ve birlikte çalışabilirliktir. Hasta bilgileri izole edildiğinde ve sorunsuz bilgi alışverişine izin vermeyen birden fazla sistemde saklanıldığında, çeşitli hasta kümelerindeki nüfus sağlığı veri setleri az olur. Blokzinciri bu özel zorluğa güvenilir bir çözüm sunar. Doğru uygulandığında, blockchain geliştirilmiş güvenlik, veri paylaşımı, birlikte çalışabilirlik, veri bütünlüğü ve gerçek zamanlı güncelleme ve erişim sağlar.

Blokzinciri teknolojisinin kullanılması, insanların nüfus sağlığı çalışmalarına katılmalarına ve verilerini jeton şeklinde para kazanmalarına olanak tanıyabilir.

Ayrıca, daha iyi veriler ve nüfus sağlığı verilerinin paylaşımı, farklı popülasyonlarda daha iyi iyileştirebilir. Daha fazla veri seti ile, yapay zeka ve makine öğrenme gibi yeni teknolojilerin kullanımı, nüfus sağlığının yaygın risklerini keşfetme ile sonuçlanacaktır.

Mevcut sağlık sistemi ve organizasyonlar tek bir merkezi veri tabanı üzerinden çalışmaktadır. Bu veritabanı kuruluştaki bir varlık tarafından yönetilir. Bu yaklaşımla başarısızlık noktası aynı zamanda tek bir noktaya gelir. Bu gibi durumlarda, bir hacker veya anti-sosyal unsur sisteme saldırırsa, genel veri tabanına erişebilir ve hastaları olduğu kadar organizasyonu da tehlikeye atabilir.

Bir organizasyonun iç altyapısını korumak için blokzincirin kullanılabilir. Birden fazla bağımsız aktöre sahip büyük bir organizasyon, bloklar içinde gömülü şifrelemeli bir blok zincir defterine farklı erişim seviyelerine sahiptir. Bir blok zinciri ağı bir sağlık kuruluşunda doğru bir şekilde uygulanırsa, bu tür fidye saldırılarının yanı sıra veri bozulması veya donanım arızası gibi diğer sorunları da önler.

Blokzincirinin sağlık hizmetlerinde göze çarpan bir diğer yararı, kripto para birimlerinin nakit para parası yerine ödemeler olarak kullanılmasıdır. Nakit tıbbi uygulamalar yaygındır, ancak sağlık hizmetleri maliyetleri böyle tanımlanmamıştır. Bugün bile davaların% 5–10'u para ve faturalandırılmamış hizmetler bakımından dolandırıcılıktan gelmektedir. Yalnızca ABD'de, 2016 yılında 30 milyon dolarlık dolandırıcılık tespit edilmektir.

Blokzincirinin sistemleri ve uygulanan uygulamalar sayesinde doğru çözümleri sağlama ve sahtekarlıkları ortadan kaldırma imkanı artmıştır. Fatura işleme otomasyonu üçüncü tarafları zincirden kaldıracak ve genel idari maliyetleri azaltacaktır. Dahası, daha büyük kurumlar kripto para birimleri aracılığıyla ödeme işlemlerini benimseyeceklerinde, büyük bir değişim meydana gelecektir. Sağlık sigortası ödenen her kuruş izlenir ve işlem sırasında herhangi bir dolandırıcılık yapılmamasını sağlar.

Diğer sağlık kuruluşlarında, ilaç şirketleri bugün şirketleri için belirli faydalar sağlayabilecek sonuçların kaydedilmesine ilgi göstermektedir. Bu gibi durumlarda, araştırmacılar sonucu değiştirmek için toplanan veri ve bilgileri sıklıkla gizmekte veya değiştirmektedir.

Klinik araştırmaları daha adil ve şeffaf hale getirmek için araştırmacılar güvenli, tarafsız ve şeffaf klinik çalışmaların kaydedilmesine yardımcı olabilecek blokzincirinin teknolojisini kullanabilirler.

Blokzincirinin teknolojisi, klinik denemelerin ve sonuçların güvenilirliğine katkıda bulunacaktır. Bu belgeler dijital parmak izi gibi davranan blok zincir üzerinde akıllı sözleşmeler olarak saklanabilir. Bu belge kataloğu, denetim maliyetlerini, dosyaların incelenmesini, kayıp belge sorunlarını ve sahtekarlıkları azaltacaktır. Blok zincir ayrıca ilaç tedarik zincirinin yönetimini ve uyuşturucu takibinin sorumluluğunu da koruyacaktır.

1. INTRODUCTION

The focus on providing a good medical service to the patient is the aim of all medical organizations nowadays. This can be done by ensuring the highest quality of management of sensitive medical information in a private and secure way. Therefore it is necessary to improve the old methods and procedures related to transfer health information between teams and medical staff to ensure the privacy of individuals.The main problem is the huge gap between service providers (doctors and nurses) and those who need these services (patients). The reliance on the third party in the providing information process may make the system more vulnerable. In the health care field, sensitive data of the patients are being kept across various department and systems. Therefore, the critical information of the patient may not be accessible or reachable when needed. Hence, the system cannot be considered a complete system as most of the entities in the system does not have the information at the right time.

In this thesis, we provide a protocol to ensure accessing data on time in a way that it respects user's privacy. Employing blockchain in our protocol ensures that these transactions will be done efficiently and could be verified by all authorized entities on the network.

1.1 Purpose of Thesis:

In this thesis, we aim to apply the blockchain technology in the healthcare field in order to ensure that healthcare data of patients will securely transfer between healthcare providers. The system allows patients to have full control of their data. This control will only be revoked by a central authority in case of a life-threatening emergency.

1.2 What is Blockchain:

Blockchain is a peer-to-peer system used to store transacting values between different nodes on the network with no need for any other intermediary. It is a

growing up list of “blocks" which are the storage units of the transactions. Each block in the chain is linked to the previous block in a manner prevents any altering or modifying in blocks order or blocks data.[3]

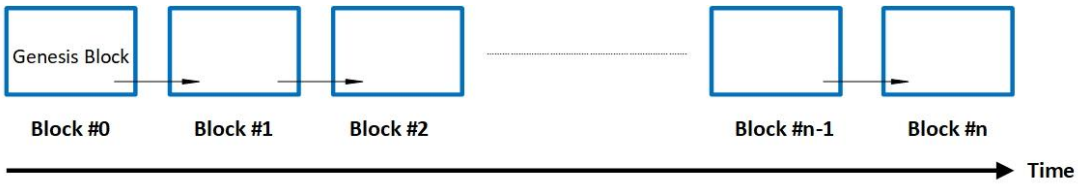

Figure 1.1 : Public format of blockchain.

1.3 History of Blockchain:

The first idea contributed to inventing Blockchain was written by David Lee Chaum in 1982 in his research **“Blind Signatures for Untraceable Payments”** which explained the concepts of digital cash and blind signatures. In this research, he shows the technical roots of the Cypherpunk movement in the 1980s in addition to propose a method for exchanging digital currency between users and bank which allows users to spend their digital currency untraceable by any other parties. In 1990 another invention had appeared depending on the same research and it is called Digicash which contributed to the achievement of the first electronic payment transaction in 1994. Digicash used different tools to hide its content in the same way current cryptocurrencies use like public and private keys cryptography and digital signature. At that time Digicash had different drawbacks which lead it to bankruptcy in 1998. One of the most important drawbacks was the double spend problem where an amount of money can be spent twice with only copy and paste with no confirmation. In 1998 in attempts to avoid the Digicash drawbacks the scientist Nick Szabo found another cryptocurrency Bitgold which is a decentralized digital currency depends on solving a cryptographic puzzle and it was accepted by the majority of the network. These puzzles were linked together like a chain and stamped by timestamp in order to solve double spending problem. Bitgold did not materialize to the reality and existed only in theory but it and its protocols were considered to be the real base for today's cryptocurrencies like Bitcoin. In the same year, Wei Dai had published a

paper entitled “B-Money, an anonymous distributed cash system”. In this research, the basis of digital coins was described.

In 2000 another research had been written by Stefan Konst that explained practical solutions to implement a system guarantee secured and depends on the concept of cryptography.[2]

This research was mentioned in Satoshi Nakamoto's paper **“Bitcoin -A peer to peer electronic cash system”** as reference and the last mentioned paper **"Bitcoin -A peer to peer electronic cash system"** included the explanation of all the concepts of blocks and transactions of Bitcoin. A year later of Satoshi’s paper, Bitcoin had been implemented with the first blockchain.[4]

1.4 Types of Blockchain:

we can classified Blockchaın into three main types according to the privilegeds of the nodes.

1.4.1 Public blockchain:

Here the blockchain is open and transparent, anyone can be a part of reading, writing, and auditing. The decision-making process can be performed by different decentralized consensus algorithms (proof of work, proof of stake).

1.4.2 Private blockchain:

Here the blockchain is a property of an organization or an individual. The blockchain, in this case, is not available for everyone. There is an entity who is responsible for controlling important things read/write and gives access right to a special set of nodes on the network. Taking a decision is due by this central authority who gives mining rights to others.

1.4.3 Consortium or federated blockchain:

Instead of having one entity as the responsibility of decision-making authority, there is a group of organizations that are in charge. [5]

Table 1.1: Types of Blockchain.

Public Blockchain	Private Blockchain	Federated Blockchain
In the application of cryptocurrency Bitcoin/Litecoin anyone can be a part in recording transactions if he set up the software.	In a private organization not, everyone is allowed to run a full node, only the central node can record and control the transactions.	Selected nodes in the network of the consortium can record and control the transactions.
Transactions can be made by any node in the network.	Only the central node can make the transaction.	Only group of chosen nodes can make the transactions.
Any node in the network can work as a miner to verify the transactions and share in adding new block process.	Only the central node can verify transactions and it is the only one responsible for adding new blocks to the chain.	Only group of selected nodes can verify transactions and it is the only one responsible for adding new blocks to the chain.

1.5 Different fields applied blockchain:

Although the appearance of Blockchain technology was related to the finance in order to store the transactions and exchanges of the digital currencies, nowadays blockchain has been expanded and invaded different fields and no longer limited to the financial field, Now we can notice clearly the existance of Blockchain in different life scopes and we can surely wait for it to be applied in many others.

1.5.1 Financial and banking:

Blockchain is tightly bounded to digital and cryptocurrencies since it has been invented. It leads its role in speed up remittances and transactions and ends slow current transfers by reducing the duration of a bank transfer from one country to another from 5 business days to a few moments. That leads to increase operations and provides fast customer services also depending on blockchain reduce costs and commissions providing cheaper services while increasing the profit margin of these institutions and allow them to compete better.[6]

1.5.2 Import and export:

The blockchain solution can close the gap between exporters and importers by reducing the need for paperwork, communications, long periods bank transactions and onsite visits with real-time information exchange over a decentralized ledger. That includes encryption and safely secure all essential transport documentation like bills, booking, delivery, orders, etc. [7]

1.5.3 Oil and energy:

Some cryptocurrencies have emerged to target this field, such as NEM, which is trying to provide Blockchain services to oil and energy producers. Different energies as solar energy and associated manufacturing industries can benefit from this technology. Some of the currencies appeared to be made gain by mining solar energy instead of electricity consumption and encourages the developers of those currencies to use solar panels in the production of mining power. There is also a tendency from some companies working in this area to issue their own currencies for use in a fuel station and power supply. Utilizing the new technology would reduce costs and increase gains even if oil and energy production declined.[8]

1.5.4 Electronic stores:

While companies like Amazon and eBay usually act as intermediaries between traders and buyers, Blockchain technology paves the way for the emergence of decentralized e-shops and this new concept would if successful, be the reason for the disappearance of Amazon and major companies-controlled e-commerce for the benefit of these new stores. These new stores will be handled using cryptocurrencies, while customer data and purchase records will become fully encrypted, and in-store operations cannot be tracked or spied on from third parties, with easy shipping and easy business completion.[9]

1.5.5 Electronic media and websites:

Since the appearance of the Internet, advertising has been the best solution for websites to generate revenue and profit for their services. Blockchain technology can boost the gains in new and different ways, One way is to cryptocurrency mining on users' computers and devices without displaying ads and gets profit from it. The technology will also allow webmasters to recruit more content creators to produce

more news and articles on the day, accelerate competition and get optimal results.[10]

1.5.6 Real estate and real estate transfer:

Bitcoin and other cryptocurrencies have entered into this field to become a payment tool. Blockchain is expected to take advantage of the acceleration of real estate transfer and real estate preservation operations through accelerating contracting and establishing smart contracts and sequential financial transactions quickly. This opens the door for further sales and growth of this field significantly in the coming period, as well as facilitate the memorization and contracting processes and transfer of ownership from person to person.[11]

1.5.7 Property rights and exploitation of wealthy:

More than 170 trillion dollars of the property has not been registered as property rights, real estates, land and various things in addition to innovations and scientific achievements. The use of Blockchain technology can help individuals to register these properties, thus maintaining their good value and avoiding loss of wealth.

1.5.8 Healthcare field:

Critical health care data of patients remains scattered across different systems and departments which makes crucial data is inaccessible and handily available in need times. This problem has been expressed by Shaun Grannis, the Director of Center for Biomedical Informatics (CBMI), he said "Statistics show that up to one in five patient records are not accurately matched even within the same health care system. As many as half of the patient records are mismatched when data is transferred between healthcare systems.", so by applying Blockchain, patients' records can be easily sent with no worries about any tampering or corruption of the data since Blockchain is traceable and immutable.

In each one of these filed there are several practical applications of the blockchain like Bitcoin, Ethereum, Ripple, Smart Contracts, etc.[12][13]
The most popular application of Blockchain is Bitcoin.

1.6 Reasons for Choosing Blockchain Technology:

Blockchain has earned the trust of users according to the following attributes:

1. Distributed: The public distributed ledger is shared upon all the nodes and it is being updated with every new transaction among the blockchain nodes. This process is executed in real time because there is no central server control it.

2. Secure: Blockchain is secured towards any unauthorized access, the access is controlled and limited by permissions and cryptography.

3. Transparent: All transactions data can be accessible by any node or participant of the blockchain because these nodes are already having a copy of the blockchain data and they can verify the identities with no need for mediators.

4. Consensus-based: All participants on the network must agree on the validity of the transaction. This is can be achieved through consensus algorithms.

5. Immutability: Data modification or alteration cannot be done without being detected.

6. Scalability: More nodes can be added to the system leading to an increase in system features.

7. Interchangeability: We can change the nodes with other equivalent nodes or new nodes with exact features with improvements.

8. More stable and have the property of fault-tolerant due to lack of no central node. (In the case of a central node this node can be attacked and this leads to the breaking down the system).[14][15]

While current transactions systems have a lot of disadvantages :

- The entire system will be affected and break down if the core of it is compromised.
- Cash can only be used in low amount transaction locally.
- Third-party verification and authentication are needed.
- Transactions need a huge waiting time to be executed.
- Transactions fees are expensive due to the validation charge by the responsible organization.

Blockchain helps to remove all the disadvantages of current transactions systems in addition to various new benefits and differences :

- **Time-saving:** The system does not contain the central authority to verify transactions, so the process executed cheaper and faster.
- **Cost-saving:** There are different ways to reduces the expenses in blockchain, no need for third-party verification, all nodes can share the data directly to the number of intermediaries is reduced, every node has a copy of the ledger so transactions efforts are decreased.
- **Tighter security:** The blockchain network is tamper-free because it is shared among millions of nodes and, it is also secure against fraud and cybercrimes.[15]

1.7 Symmetric And Asymmetric Key Encryption :

1.7. 1 Public key cryptography (Asymmetric key):

In the public key encryption systems, we have a pair of keys for each entity:

Public key: This key is available for everyone to be used for encrypting the message.

Private key: This key is used only by the owner to decrypt the message. This key is kept secret

Because of the mathematical relation between public and private key, the data encrypted by the public key can only be decrypted by using the private key.

This pair of keys is generated depending on mathematical problems that produce one-way functions.[1]

1.7.2 Symmetric key cryptography:

In this method, there is only a single key used for both encryption and decryption. When this method is applied we must ensure that the communication channel is secure so this key cannot be stolen by any other party. The encrypted message has an unreadable format and when we want to retrieve it back we apply the symmetric key in a reserve procedure so we get the origin message.[1]

There are two types of algorithms depends on symmetric encryption:

1.Block algorithms: The data is divided into fixed-length blocks and each block is being encrypted by the encryption key. In this case, the system stored these blocks in its memory until all blocks arrive.

2.Stream algorithms: The system does not store the data in its memory but when each bit arrives, it is encrypted by the secret key.[16]

Sometimes we can't guarantee that the message has not been changed while the encryption process, therefore, we add authentication code to the cyphertext. This authentication code will make any change in the encrypted message notable by the receiver.

The symmetric key encryption method has appeared before the asymmetric encryption methods and it is faster than the asymmetric methods, so it is used typically when we have a large amount of data needed to be encrypted.[17]

1.8 Difference Between Symmetric and Asymmetric Encryption:

- In the symmetric key encryption algorithm, we have only one key used for both encryption and decryption, but in the asymmetric key encryption algorithm we have a pair of keys one is used for the encryption and the other one is used for decryption.
- Symmetric key encryption can be considered as the old way of encryption while the asymmetric key encryption is the modern way.
- Asymmetric key encryption needs more time to be done in comparison to the symmetric key encryption.
- Asymmetric key encryption is invented to be the solution of the sharing-key problem in the symmetric key encryption.[18]

Advantages of symmetric key encryption:

- The encrypted data can be sent via a communication channel even if there is a possibility of being intercepted.
- This type of encryption methods is a fast method of encryption.
- Password authentication is used to prove the identity of the receiver.
- Only the receiver owning the key will be able to decrypt the message.[19]

Advantages of asymmetric key encryption:

- In this method, there is no need to exchange the encryption key between the sender and receiver.

- Guarantee more security because the private key will never be transmitted over the channel.
- The ability to provide a digital signature.[20]

2. BITCOIN

2.1 What is Bitcoin:

It is one of the cryptocurrencies depending on peer to peer network that doesn't need intermediaries. Transactions in Bitcoin are confirmed by the network nodes depending on the cryptographic techniques, these transactions are recorded in a distributed public ledger.

As mentioned above it was invented by Satoshi Nakamoto and published as open-source software in 2009. Bitcoin offers a reward for the mining process and for now it can be exchanged for other currencies, services, products, etc.

University of Cambridge's research shows that in 2017 the number of cryptocurrency wallet user was up to 5.8 million and most of these users were using Bitcoin. The creation of Bitcoin's first block was on 3 January 2009, and it was known as genesis block and it contained the following text: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.". This note was considered as a time stamp for this genesis block. Hal Finney was the first receiver of Bitcoin transaction who also invented the proof-of-work system in 2004. The first transaction was on 12 January 2009. The transactions of Bitcoin had been expanded so in 2010 when Laszlo Hanyecz ordered two Papa John's pizzas for 10,000 Bitcoins. The Bitcoin blockchain implemented as a chain of blocks and these blocks have their own structure.[1]

2.2 Block Structure:

The blocks are considered to be data container and they depend on the technology of cryptography to encrypt data. In Bitcoin world, one block of the blockchain can contain up to 500 transactions, in this status the block size equals to 1 MB, in another different status it could reach 8 MB according to the used filed which increases the processed transactions per second. The block can be identified by referencing the block cryptographic hash, or by referencing the block height and each block consists basically of two main parts the header "metadata container" and the transaction list.

Block header size is 80 bytes and the average transaction is about 250 bytes. The complete block with all of its transaction 1000 times larger than its header.[22]

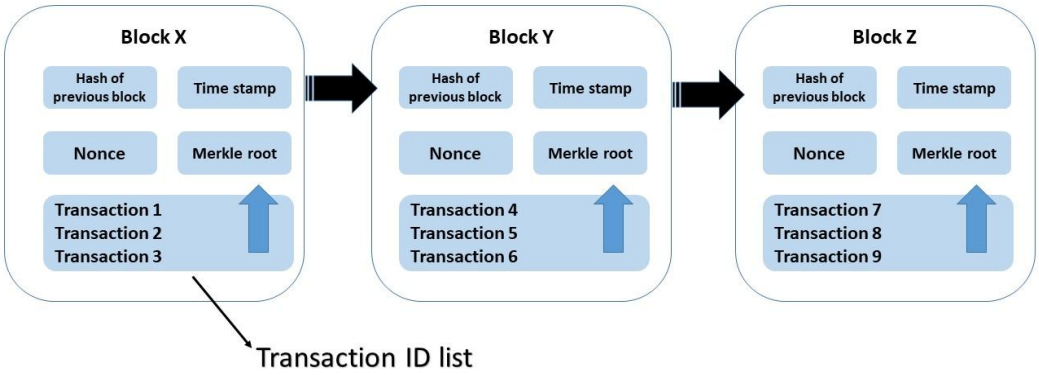

Figure 2.1 : Block structure.

Table 2.1 : Block components sizes and descriptions.

Size	Field	Description
4 bytes	Block Size	The size of the block in bytes.
80 bytes	Block Header	Several fields from the block header.
1-9 bytes (VarInt)	Transaction Counter	How many transactions follow.
Variable	Transactions	The transactions recorded in this block.

The Block header:

In the header we store the metadata (metadata is the data used to describe other types of data) which fall into three types:

- **The hash of the previous block:** Each block in the blockchain contains the hash of the data stored in the previous block. This hash is necessary for the process of creating a new block. If we have N blocks, the Nth block contains the hash of the N-1 st block. But about the first block which has no previous block so it has no previous block hash, we call this first block a Genesis block, we supply it with some arbitrary data that is needed to create its hash.[22]

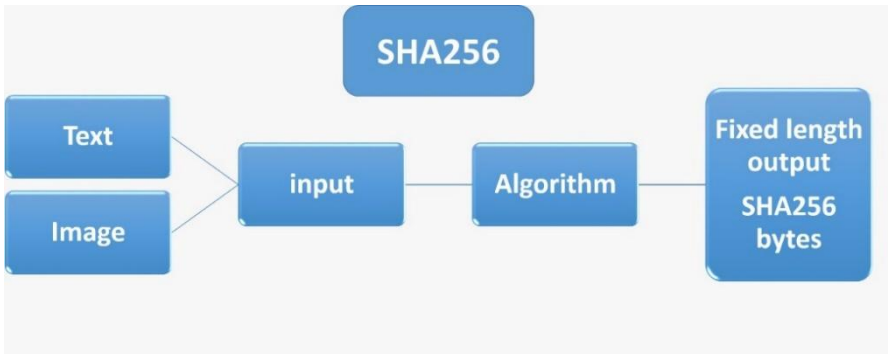

Figure 2.2 : Hash function.

- **Merkle tree root:**

It is a binary hash tree which used to summarize the amount of data related to transactions being stored in the block in an efficient manner.

If we have N pair of nodes so the Merkle tree hash levels will be equal to $\log_2(N)$.[22]

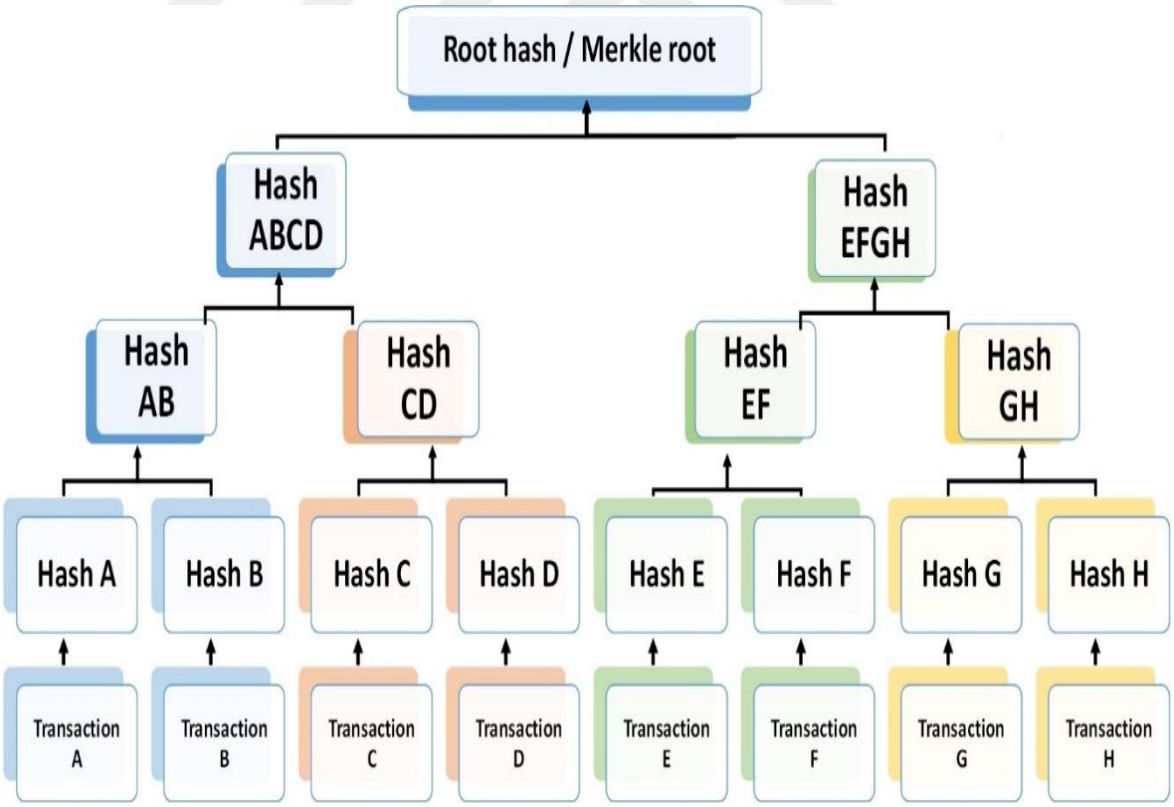

Figure 2.3 : Merkle root hash.

- **Mining competition:**

In the process of adding a new block to the blockchain, we should supply the new block with a hash and this hash should be valid (The validity of the block is considered according to the first four characters in the hash). It also includes a timestamp, version number (which used to follow the protocol upgrade and the software) and the nonce.[23]

Nonce:

In the case of the hash is invalid, so we must re-do the hashing process. While the data is still the same data with no change that is mean the result of the hash will still the same each time and it will never get a valid value of the hash so we use the nonce to solve this problem. A nonce is a number that concatenates to the data stored in the block "including previous hash value and other data " and we hash these data together. So when we get invalid hash we just increment the nonce and redo the hash process until we get a valid hash value.[1]

Target:

Target is the value that miners compare their result with and the result should be below it. It is set by the Bitcoin network to determine the difficulty of adding a new block to the blockchain.[1]

Difficulty explanation:

Blockchain network creates the target which determines whether the hash is valid or not comparing to the target value. If the hash value is higher than the target value so the hash is not valid.

If we have a block hash like:

000000000000000000020c60222099aaebc6e7795784f74628ec640b223d3d339

so here we have 18 leading zeros. So, each hash contains less the 18 leading zeros will be invalid.

At the beginning of the mining process, the nonce will initialize to "0". When we start mining the block that means we are trying to find the value of the nonce which leads to a hash lower than the target. We could end up with a billion or trillion probability of the nonce before getting the valid hash.

Version:

Describes the structure of the data inside the block. This is used so that computers can read the contents of each block correctly.[1][23]

Timestamp:

Timestamp defines all information related to date/time about the current created block. Timestamp considered valid if it is greater than the median timestamp of the previous 11 blocks and less than the network-adjusted time +2 hours. The network-adjusted time is the median of the timestamps returned by all nodes connected to you. According to that block, timestamps may not be accurate exactly and may not be in order too. The block timestamps are accurate only within one or two hours. When two nodes are connected together on the network, one of them gets UTC timestamp from the other one and stores its offset from node-local UTC and at this point, the network-adjusted time is then the node-local UTC plus the median offset from all nodes connected on the network. Time in the network is never adjusted more than 70 minutes from the local system time. Timestamp helps in overcome double spending problem.[1][23]

Table 2.2 : Block header components sizes and descriptions.

Size	Field	Description
4 bytes	Version	A version number to track software / protocol upgrades.
32 bytes	Previous block hash	A reference to the hash of the previous (parent) block in the chain.
32 bytes	Merkle Root	A hash of the root of the Merkle tree of this block's transactions.
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch).
4 bytes	Difficulty Target	The proof-of-work algorithm difficulty target for this block.
4 bytes	Nonce	A counter used for the proof-of-work algorithm.

Mining:

Mining is the method which guarantees that the blockchain is decentralized in a secure way. In other words, it is the process responsible for validating the new transactions and registering them on the public ledger. The requested time to create a new block is 10 minutes.

There is a competition between the miners to find the solution of a very complex mathematical problem build on a cryptographic hash algorithm and we call this solution "Proof of work". The "Proof of work" confirms that the miners consume enough resources and spend enough time to solve the problem. In this status when the block problem is solved the contained transactions consider as proved or confirmed. After solving this problem, the founder "Miner" gets a prize and this prize has two types: new currency created with each new block, and transaction fees from all included transactions in the block. These days, the transactions fees represent 0.5% or less of a bitcoin miner's income, while the majority coming from the newly minted Bitcoins. However, the number of transactions per block increases over time and the reward decreases, a greater amount of Bitcoin mining gain will come from transactions fees. So, by a few mathematical equations we discover that after 2140, all the Bitcoin mining gain will be the form of transaction fees.[1][23]

2.3 How Does it Work?

We know that blockchain has no central authority so every node on the blockchain network has the accessibility right to the public ledger of the transactions which is a reliable record. In some way, each node on the network work on this doubtful information and end up with the same results and conclusions.

While the block is waiting to be confirmed and added to the network it spends its waiting time in the transaction pool (memory pool) where the miner's task starts: gathering transactions from the transaction pool in a form of "candidate block" and try to add this candidate block to the blockchain. This candidate block can also have a block header. At this point, we apply the hash function to the block header, and we want the hash value to be less than the target value to be a valid hash.[1][23]

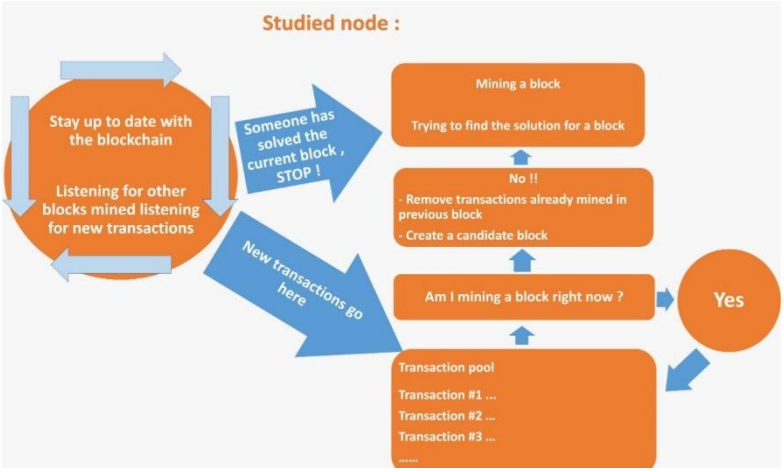

Figure 2.4: Mining.

2.4 Example of Adding a New Block To The Blockchain:

In the Bitcoin world, the process of creating a new block and adding it to the network including validating process takes around 10 minutes. Let us assume that one of the miners in the competition of solving the problem is trying to solve the block 502425 but unfortunately other miners precede him. When this block 502425 was mined that means a new block is being initialized and at this point our miner is updating his local copy of the blockchain and begins the process of creating the candidate block "in this status the block 502426 " so when our miner was trying to solve the problem of the previous block it was also monitoring the network and trying to catch any new transactions. These new transactions are gathered in the memory which is called memory pool or transaction pool. Hence, the transaction pool is logical where transactions stay until they are being added to the blockchain. When our miner ensures that current block was solved and get its validation, the node begins initializing the candidate block by adding the transactions in the memory pool removing all transactions included in the previous block if existed.[23]

3. OUR PROPOSED SYSTEM :

Our aim is to build a secure protocol grants the privacy of healthcare data in different cases. This protocol will allow only the authorized users to access the health record of the patient for a certain amount of time under different specified conditions. The work here is similar to the work in Bitcoin where the blockchain is responsible for the control and record all healthcare data transactions and permission including also all information about the identity of the patient and the health professional. The integrity of data is important and required in this type of process and the blockchain technology provides it. In our protocol not only the patient himself will be responsible to grant the permission to access his healthcare, but the central health authority will have an important role in some situations because we should include all cases like the urgent case where the patient does not have the ability to do that process. In urgent cases, the central health authority will be responsible for giving permission to access the healthcare record to the authorized user.

3.1 Components Of Our System:

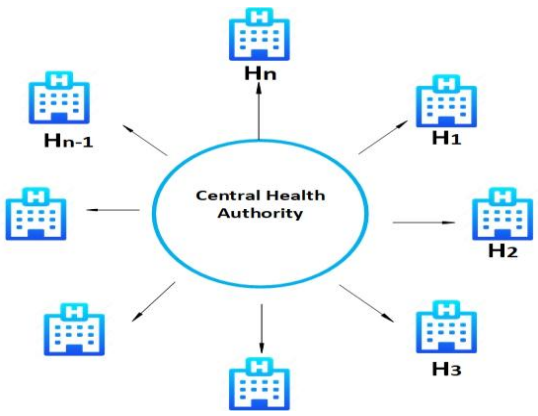

Figure 3.1 : Public figure of our system.

1. The central health authority which represents by the health ministry mostly. It will be responsible for grant the users their credentials and IDs and authenticate hospitals and health professionals.

2. The nodes which are represented by hospitals that contain an important part: The Emergency Room that is responsible for authenticating emergency case and a lot of clinics that contains another type of entities.

3. The users which fall into two categories:

1) **Health professionals:** They are given IDs by the central health authority and existed in the hospitals which are authorized by the central health authority or existed in their private clinics.

2) **The patients:** They are given IDs by the central health authority and they fully control their healthcare data records, giving access right to the trusted authorized health professionals.

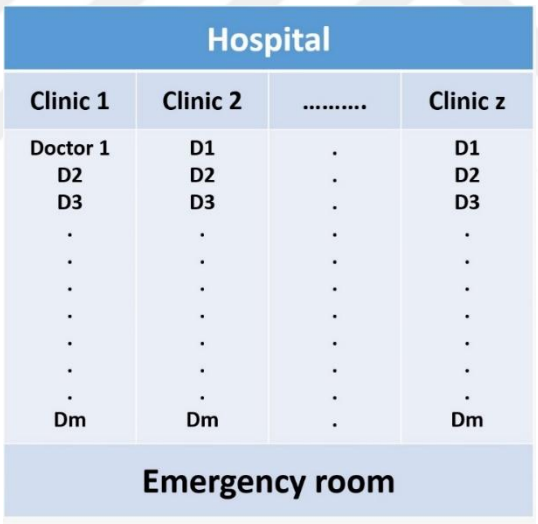

Figure 3.2 : The proposed figure of the hospital in the system.

3.2 Our Proposals:

Our work ensures a high level of privacy and security in the healthcare information as they will be available for a certain amount of time specified by the owner. By allowing to access the healthcare record with permission, this permission also has to be authorized by a set of nodes and then recorded in the chain in addition to record the specified given time. The storage system in our work is a distributed storage

system is responsible for storing all healthcare data records and the hospitals will be responsible for controlling and managing all the access right request and achieving process in addition to construct the needed data from the nodes in the system. The storage system is being constructed by the nodes (hospitals) that have their own storage systems. In the storage system, all healthcare records are stored allowing them to be available and accessed once authorized.

As the blockchain depends on cryptography, our system will surely depend on it too. The proposed work assumes that every patient in our system is given both public key and private key by the central health authority. These keys ensure that healthcare data are secure and confidential. In addition to these two keys, another additional key is provided by the central health authority and this key is a symmetric secret key. The main purpose of using the symmetric key here is achieving the requested efficiency when large data is being processed. This is not the only reason to use the symmetric key but the need to embed the central health authority as a permission provider in an emergency case.

In our system, we have the health record R and then we construct the cryptographic version that will be stored in the storage system.

First, the healthcare record itself will be encrypted by the symmetric key s_A :

$$R' = SE_{s_A}(R) \tag{3.1}$$

At the end of this process we need to encrypt the symmetric key itself with the private key of the patient who is the owner of R:

$$s'_A = PE_{K_A}^{+}(s_A) \tag{3.2}$$

Now we will construct the proper form of the healthcare record as two parts: one is R' and the other is s'_A.

It is worth mentioning that in our system, especially the confirmation of our basic knowledge when constructing it, we want to allow authorized users to access these healthcare records under certain conditions for the purpose of saving patients' lives as soon as possible that a full copy of s_A is stored in the central health authority order to be used in urgent cases.

At this point the proper form to storage the healthcare record in our storage system is ready.

3.3 The Method:

When an access right request is applied we should check whether the access right request is applied by an authorized entity not by an intruder. This can be made by employing a set of hospitals to check the ID of the health professional who requests the access right to the R and verify him or not. A multi-step method is running:

1. In the case of the health professional is authorized by this set of nodes his ID is recorded in the ledger in addition to the ID of the hospital he belongs to.
2. Patient ID and hospitals IDs which verify and authenticate the health professional will also be recorded in the ledger.
3. Time/date of the request and the given permission is recorded in the ledger.
4. If the health professional doesn't belong to one of our system hospitals (out of the system) he will be checked by a set of nodes to verify his identity. All information related to this process is recorded in the ledger. (IDs of hospitals contributed to the process of authenticating).
5. IDs of all hospitals involving in the authenticating process is also recorded in the ledger.
6. At this point the patient himself will be able to give the access right to his healthcare record as he owns and controls his k_A^-. By owning it he will be able to open the health record data for the concerned health professional for a certain time which will be recorded in the ledger.
7. In the case of an emergency, the emergency case must be authenticated and verified by the emergency room in the concerned hospital.
8. The emergency case is recorded in the ledger in addition to the ID of the entity contributed in the authentication process.
9. In this emergency case, the central health authority will be responsible for giving the requested access right to the healthcare record by providing s_A.
10. The s_A will be available for a certain amount of time and this certain time is recorded in the ledger.

11. The s_A will be used by a various number of hospitals in order to open the healthcare record and initialize it to be used by the health professional requesting access right.

According to the aforementioned steps we can see that every transaction indicated in the block contains the following details:

1. The patient ID.
2. The health professional ID.
3. The IDs of hospitals which authenticated the health professional.
4. Ids of hospitals responsible for initializing requested data.
5. A timestamp of the related process and the given data/time frame.
6. All nodes sharing the process of record authenticating.

All previous details are combined in one part inside the block and this part labeled as M_j.

These details are not enough fully understand what the ledger is. There are many other details to be included in the public ledger. We have to employ a cryptographic hash function in order to provide privacy and a set of hospitals needed to authenticate the constructed ledger.

3.4 Ledger Constructing Steps :

1. M_j: It is the message constructed from different details explained in the previous paragraph.

2. Encryption of the previous message hash by using the private key of each hospital included in the authentication $E_{H_i^-}(h(M_j))$ process.

3. The hash of previous ledger $h(L_{j-1})$.

4. IDs of all hospitals verify and record the ledger.

3.5 Goals We Achieved and Solved Problems :

1. Because of the blockchain immutability and traceability, patients can share their data with no worries about being tampered or altered.

2. All healthcare data transactions records which are generated under the Blockchain technology and being added to the chain are completely secure.

3. Patients will have (somehow) full management and control of their healthcare records in order to share the records fully or just parts of the record with some medical entities (organization and institutes). In this case, any medical entity will not be able to access the records without the patient permission.

4. The reward mechanism can be used to incentivize the patients for their good behavior. By staying healthy or following a care plan they can get tokens as rewards for sharing the healthcare data for research or clinical trials.

5. In the pharma companies, a lot of stolen accidents happened from the supplier in order to be sold illegally to different types of customers. In this case, these companies need a secure trust supply chain because of their work nature. Some statistics talked about that costs 200 billion $ of stolen drugs per year. By using the blockchain which has the feature of transparency these pharma companies will be able to trace all drugs deals from the starting point to the end helping in remove falsified drugs.

6. Over the world, various medical organizations and institutes are working on research and clinical trials whether on diseases or drugs. By using blockchain, these organizations and institutes will have a global database and it will be shared over all of them for easily data and results exchange.

7. The most important problem facing the healthcare industry is insurance fraud. When false information/claims are submitted by patients or dishonest providers in the aim of getting payable benefits. In the USA according to Boyd Insurance, the fraud in Medicare costs to 68 billion $ per year.[24]

4. CONCLUSION:

In this thesis, we have presented a new protocol in the healthcare field using Blockchain technology which revolutionized the world of privacy and security. Our aim is to build a new system that any healthcare provider or patient can rely on to achieve maximum results of healthcare security and privacy. In addition, we are also aspiring to give patients full control over their own healthcare data. Our methods control all data transactions between different types of entities starting from requesting healthcare records of the patient to updating patient healthcare record of examinations, pharmacotherapy and monitor vital developments and all new parameters related to the patient. These transactions are run in secure communication channels connected between different healthcare system entities and various parts of the storage system. They are executed under specific conditions ensuring that healthcare data records are inaccessible by non-trusted users and also resistant to any modification or alteration from an entity that is not authorized by the system.

REFERENCES:

[1] **Bashir, I**. (2018). Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2nd Edition.

[2] **Singh, V**. (2017). Understanding Blockchain Technology: Your quick guide to understand blockchain concepts.

[3]**Url-1** < *https://en.wikipedia.org/wiki/Blockchain*>, date retrived 19.01.2019.

[4]**Url-2** < *https://en.wikipedia.org/wiki/Bitcoin*>, date retrived 09.01.2019.

[5]**Url-3** <*https://coinsutra.com/different-types-blockchains*>, date retrived 01.01.2019.

[6]**Url-4** <*https://youteam.co.uk/blog/10-use-cases-of-blockchain-technology-in-banking*>, date retrived 10.12.2018.

[7]**Url-5** <*https://hackernoon.com/blockchain-in-healthcare-opportunities-challenges-and-applications-d6b286da6e1f*>, date retrived 22.12.2018.

[8]**Url-6** <*https://www.researchgate.net/publication/332048415_Blockchain_technology_in_the_oil_and_gas_industry_A_review_of_applications_opportunities_challenges_and_risks*>, date retrived 22.12.2018.

[9]**Url-7** <*https://www.forbes.com/sites/rogeraitken/2017/10/24/whats-the-future-of-online-marketplaces-blockchains-technology-impact/#398a985b63a0*>, date retrived 22.12.2018.

[10]**Url-8** <https://www.blockchaintechnologies.com/applications>, date retrived 11.01.2019.

[11]**Url-9** <https://espeoblockchain.com/blog/blockchain-real-estate-startups>, date retrived 15.01.2019.

[12]**Url-10** *https://www.mdpi.com/2410-387X/3/1/3*>, date retrived 17.01.2019.

[13]**Url-11** < *http://healthcareitsujeetkatiyar.blogspot.com/2019/06/blockchain-in-healthcare-ultimate-use.html*>, date retrived 17.01.2019.

[14]**Url-12** <*https://www.quora.com/What-is-the-benefit-of-blockchain-technology*>, date retrived 02.02.2019.

[15]**Url-13** <*https://www.geeksforgeeks.org/blockchain-technology-introduction*>, date retrived 02.02.2019.

[16]**Url-14** <*https://en.wikipedia.org/wiki/Symmetric-key_algorithm*>, date retrived 15.05.2019.

[17]**Url-15** *<https://itstillworks.com/advantages-disadvantages-symmetric-key-encryption-2609.html>*, date retrived 15.05.2019.

[18]**Url-16** *<http://www.enterprisenetworkingplanet.com/netsecur/article.php/623901/Understand-the-differences-between-public-key-and-symmetric-key-encryption.htm>*, date retrived 16.05.2019.

[19]**Url-17** *<https://itstillworks.com/advantages-disadvantages-symmetric-key-encryption-2609.html>*, date retrived 16.05.2019.

[20]**Url-18** *<http://techrejects.blogspot.com/2014/08/advantages-disadvantages-symmetric-asymmetric-key-encryption-methods.html>*, date retrived 16.05.2019.

[21]**Url-19** *<http://www.enterprisenetworkingplanet.com/netsecur/article.php/623901/Understand-the-differences-between-public-key-and-symmetric-key-encryption.htm>*, date retrived 16.05.2019.

[22]**Url-20** *<https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo>*, date retrived 12.03.2019.

[23]**Url-21** *<https://dev.to/damcosset/blockchain-what-is-mining-2eod>*, date retrived 15.03.2019.

[24]**Url-22** *< https://blockgeeks.com/guides/blockchain-in-healthcare>*, date retrived 15.04.2019.

CURRICULUM VITA

Name Surname : Raneem Seirawan

Place and Date of Birth : Syria 23.03.1988

E-Mail : raneemsierawan@gmail.com

EDUCATION :

- **B.Sc.** : 2013, Damascus University, Faculty of Mechanical and Electrical Engineering, Department of Computer Engineering and Automation.

PROFESSIONAL EXPERIENCE AND REWARDS:

- **2012-2013** Al Tanmyah Services, Damascus Syria, web developer.
- **2014-2015** Dleaf, Istanbul Turkey, web developer.

PUBLICATIONS, PRESENTATIONS AND PATENTS ON THE THESIS:

- **Seirawan, R.** 2019 **:** Application of BlockChain in Data Exchange Protocol. IMASES-2019: International Symposium on Multidisciplinary Academic Studies.

- Ozdemir, E., **Seirawan, R.** 2019. Applying Blockchain In Health System. (In preparation).