aurum

AURUM MÜHENDİSLİK SİSTEMLERİ VE MİMARLIK DERGİSİ
AURUM JOURNAL OF ENGINEERING SYSTEMS AND ARCHITECTURE

Cilt 6, Sayı 2 | Kış 2022
Volume 6, No 2 | Winter 2022, 157-173

ARAŞTIRMA MAKALESİ / RESEARCH ARTICLE

DIPLOMA VERICIFATION USING BLOCKCHAIN TECHNOLOGY

Ramazan KAZAN
Computer Engineering, Graduate School of Science and Engineering
Electrical And Computer Engineering, Altınbaş University, İstanbul, Türkiye
rkazan@gmail.com, ORCID: 0000-0002-7166-247X

GELİŞ TARİHİ/RECEIVED DATE: 31.01.2022 KABUL TARİHİ/ACCEPTED DATE: 03.11.2022

Abstract

Blockchain technology is attracting attention from academies, industries, governments all over the world. Expectations of increased potential have led to extensive exploration of the use of this technology in various application platforms. Today, blockchain is considered to be a technological breakthrough that touches all areas of social life, and is expected to lead to very significant changes, especially in a few application areas. In the study; A certification diploma verification system has been developed using the decentralized, open-source blockchain platform. Thanks to the integration of blockchain technology with the document verification system, the centrality in the control mechanism can be eliminated and user initiative can be eliminated. In addition, the task of verifying documents in existing systems is a time-consuming process. Treatment can take up to several months, depending on the provider's response. Thanks to the blockchain, employers or institutions that want to verify documents will be able to perform their transactions without spending time and money.

Keywords: Blockchain, Diploma Verification, Certification.

BLOCKCHAIN TEKNOLOJİSİ KULLANARAK DİPLOMA DOĞRULAMA

Özet

Blok zinciri teknolojisi, dünyanın her yerinden akademiler, endüstriler, hükümetler tarafından ilgi görmektedir. Potansiyelinin artacağı yönündeki beklentiler, değişik uygulama plâtformlarında bu teknolojinin kullanımının geniş çapta araştırılmasına yol açmıştır. Bugün blok zinciri sosyal hayatın tüm alanlarına dokunan, özellikle birkaç uygulama alanında çok önemli ölçüde değişimlere yol açması beklenen teknolojik bir atılım olarak kabul edilmektedir. Çalışmada; merkezi olmayan, açık kaynaklı blok zinciri plâtformu kullanılarak, bir sertifikasyon diploma doğrulama sistemi geliştirilmiştir. Blok zinciri teknolojisinin, belge doğrulama sistemi ile bütünleştirilmesi sayesinde kontrol mekanizmasındaki merkeziyetçilik ortadan kaldırılarak, kullanıcı inisiyatifi ortadan kaldırılabilir. Ayrıca, mevcut sistemlerde belgeleri doğrulama görevi uzun zaman alan bir işlemdir. Muamele, sağlayıcının verdiği yanıta bağlı olarak birkaç aya kadar sürebilir. Blok zinciri sayesinde belge doğrulaması yapmak isteyen işverenler ya da kurumlar, maliyet ve zaman harcamak durumunda kalmadan işlemlerini gerçekleştirebileceklerdir.

Anahtar Kelimeler: Blok Zinciri, Diploma Doğrulama, Sertifikasyon.

1. INTRODUCTION

The phenomenon of globalization that surrounds the world has brought some developments with it. This wind, which made itself felt in many areas, showed its weight over time with the industrial revolutions one by one. When the developments in technology are added to this, the world began to be described as a small village. The use of computers and the development of the information sector have brought economic and social life to a completely different dimension. Blockchain technology was first described in the article "Bitcoin: Peer-to-Peer Electronic Payment System" published by Satoshi Nakamoto. This new technology has aroused great interest in the world, studies have been made on it, it has been the subject of articles, albeit in a small number, and it has started to be used in many sectors in the business world with its qualifications.

Blockchain technology is receiving unparalleled attention from academies, industries, and governments all over the world. Expectations that its potential will increase has led to extensive research into the use of this technology in various application platforms. Numerous studies for various purposes have resulted in the implementation of various blockchain systems. Today, blockchain has considered a technological breakthrough that touches all areas of social life, and it is expected to lead to very significant changes in a few application areas. Blockchain technology; It has the potential to increase efficiency from the financial sector to energy markets, procurement processes, intellectual property management, the public sector and many other platforms. It attracts the attention of many sectors and governments with its fully automatic, transparent, safe and minimal intermediary infrastructure.

Finally, blockchain; uses asymmetric keys for encryption and authorization operations. Smart contracts; automatically executes logic and conditions as business rules. Today, besides students who apply for scholarships by issuing fake transcripts, it is seen that there are people whose diplomas are not real even though they have been practicing professions such as "teaching and medicine" for years. This is not due to the lack of a mechanism to check the diplomas that individuals certify their qualifications, but to the fact that it is unknown whether there is a malicious intervention in this mechanism later on. It reveals the need for a decentralized system with high traceability and monopolization of data.

Blockchain-based certification diploma verification system offers individuals securely encrypted digital freedom. This technique can help users identify the data they want to share in divergent environments and protect them from transactions such as fraud. In the study; a certification diploma verification system will be developed using the decentralized, open-source blockchain platform.

1.1. Basic Concepts and Blockchain Terminology

"Data"; it is defined as the Turkish equivalent of the word "data", which appears in English and Latin languages, and the name given to the unprocessed piece of raw information. It would not be an erroneous approach to define data as "raw information that does not make sense on its own, but makes sense if it is processed and transformed into information". The concept of "data" is of great importance within the scope of blockchain technology. A database is a collection of data organized in a certain way and the structure that holds the data together. Based on the aforementioned definition, a database can be defined as "the mechanism that creates the data collection that is stored within certain standards". (Usta, 2017)

"Block" is an encrypted data set in which confirmation records of transactions performed within a certain time are kept. By a different definition, a block is a list of transactions recorded in a ledger for a certain period of time. The block records the time of transactions performed within the network managed by the rules agreed and accepted by the network participants. Each block from the starting block in the blockchain system to the last generated block contains the hash of the block just before it. As a result of the quoted information about the block, it is understood that each of the blocks in the blockchain system records the list of transactions performed in the network and the time of transactions. It would not be an inaccurate approach to claim that each of the blocks in the aforementioned system has the "done base" feature. At this point, as a result of the transition from the classical centralized database mechanism to the distributed database system, as mentioned in the previous title, with the concept of "block".

Peer-to-peer refers to the distributed network structure that occurs with direct data sharing between the participants within the scope of the "blockchain network", without the need for a central server. In blockchain technology, each participant in the network has its own synchronized copy, and as a result, participants can view and approve transactions that take place on the network. The concept of "peer-to-peer network" is referred to as a peer-to-peer network in some sources, and is expressed as "peer to peer (P2P)" in English-sourced scientific texts. Considering the definitions related to the concept of "peer-to-peer network", it was understood that there is no central server in the mechanism and that each participant is directly connected to each other. At this point, we can state that the concept of "peer-to-peer network" is different from the network structures used today, and this difference is due to the absence of a centralized structure.

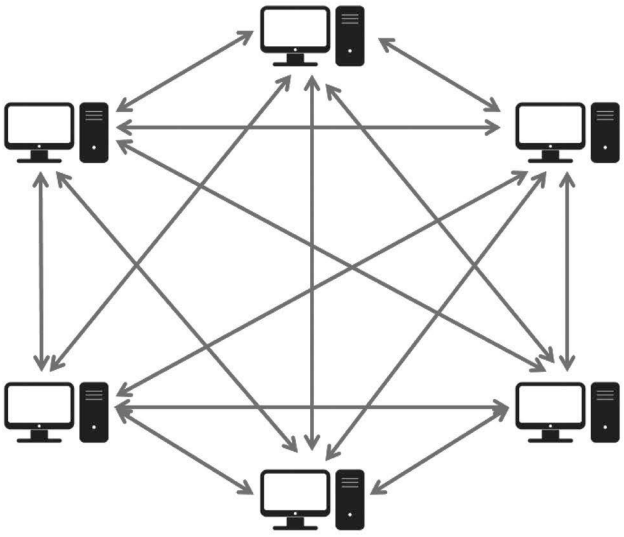

Figure 1: Peer-to-Peer Network Simulation.

Cryptography; It is closely related to the disciplines of "cryptology" and "crypto analysis". Microdots include methods such as "merging words with photos" and other ways to hide information during storage or transmission. Cryptography or encryption; it refers to the examination of secure information

and communication methods that allow the sender and receiver of a message to view the content of the message, using various software and mathematical methods. Cryptography ensures secure communication in the presence of malicious third parties known as enemies. Cryptography converts a plain text into output using an algorithm and key. An algorithm is considered secure if it cannot determine any property of the key when fuzzy text is given to a malicious third party.

Encryption: Encryption is the process of converting the data into an unreadable format in order to protect the confidentiality of the data during transactions such as "transport, reception, storage". Encrypted data is decrypted by a process called "decryption". Encryption and decryption require the use of some kind of key. Likewise, the data can be read and understood by the desired recipients, even if they seem confused.

Verification: Authentication is the process of ensuring that the alleged sender in a data string is actually the real sender.

Integrity: Proper encryption also ensures message integrity. This means that messages are transmitted correctly and are not intercepted or altered in the communication path. It is usually done by "hashing" the data.

Blockchain technology; by its very nature, it is a decentralized technology. One of the main features that make it so attractive to the broad public is that it is based on the standards of the P2P network. Most networks do not have a single influence, but there is a consensus among users. Being a member of a particular crypto currency community is not only exciting but also a responsibility. A node is the name given to each computer in a blockchain network. Nodes are one of the most important parts of the blockchain, as they are responsible for protecting the data of the blockchain. That is, the survival of the node is very important in the operation of the blockchain. A node can be any device with storage capacity and an internet connection. The role of a node in the blockchain; to support the network by maintaining the block copy and, in some cases, processing transactions.

"Distributed ledger" refers to the technology in which activities such as executing, validating or authorizing transactions in the blockchain system are kept in nodes, with the approval of all participants in an independent network, without the need for a central authority. The distributed registry is separated from the centralized network registry by a colon. (Desphande, 2017) These points are that a change in the information in one of the ledgers causes a change in each ledger at the same time, and the said information is verified with a "cryptographic signature". In the light of the information explained and in a simpler way, "messy registry"; it is a decentralized ledger where transactions performed on the blockchain network are recorded. In the distributed ledger, trust comes from the process itself, not from the status of any participant or from a central server. (Williams, 2016) The trust in the aforementioned system arises from the operating process of the system. Information available in the system; it is kept in more than one ledger, and a change in one of the ledgers is reflected in all ledgers.

Smart contract; a set of agreements and rules that govern a business. (Kırbaş, 2018) In other words, a "smart contract" is a contract whose implementation is automated. More broadly, a "smart contract" can

be defined as digital programs based on the blockchain consensus architecture, whose structures are self-executing and tamper-proof, which will automatically execute when the terms of the agreement are met. Smart contract; it is prepared after the agreement of the contracting parties on the scope of the contract, signed cryptographically and uploaded to the blockchain network.

"Hash" is an algorithmic treatment to convert data into a string of numbers and letters. With a different definition, "hash" is the information obtained as a result of recording and summarizing every transaction performed within the blockchain system by the system. Each block in the blockchain system contains the hash of the previous block. (Seirawan, 2019) If we combine the aforementioned information with the hash definition, we can state that each block actually contains the summary of the block before it. It is a natural consequence of the feature of the system to claim that the order of the blocks cannot be changed because each block contains the summary of the block immediately preceding it.

SHA 256 is a cryptographic data encryption method based on "secure cryptographic hash algorithm". SHA 256 algorithm; it is a cryptographic digest function and is used in digital certificate and data integrity. While hash is one of the most critical issues for blockchain protocols, the blockchain protocol uses the SHA 256 hash algorithm as its main hash function. Within the scope of the information explained, it is understood that the SHA 256 algorithm encrypts the data and actually extracts an encrypted summary of the data. When we consider the explanations for Hash and SHA 256, we see that SHA 256 is a type of Hash function. (Çetin, 2018)

1.2. Definition of "Blockchain" and Types of Blockchain Networks

Blockchain; it is an open, distributed ledger that can record transactions between two parties in an efficient, verifiable and permanent manner. In other words, "blockchain" refers to a digital global ledger, flat data file, or simple database containing public, transparent, sequential and time stamped Bitcoin transfer transactions. (Iansiti, 2018) As can be seen, within the scope of the last definition, the transparent and open registration system of blockchain technology has been emphasized.However, what should be noted and criticized in this definition is that blockchain technology is defined as a method that includes Bitcoin transfer transactions.

However, it is worth noting that Bitcoin is the first application of blockchain technology and that blockchain technology can be applied in many areas. In other words, blockchain technology is not only an application based on Bitcoin, but also a technology that can be used in many different applications. Blockchain is a decentralized encrypted ledger of variable data records that is replicated and distributed to each member of a peer-to-peer network. At this point, we see that each of the concepts of data, database, peer-to-peer network, distributed registry, block and hash explained under the previous headings of the study are included in the definitions made about blockchain. So, we can state that each of the conceptual explanations made up to this point is actually a part of the definition of blockchain technology. (Avunduk, 2018)

The main idea of the blockchain system is to create a database containing records of transactions shared with network participants. Integrity is based on strong cryptography that validates and chains blocks

in transactions, making the system so secure that it cannot be tampered with by a third party. Even if a malfunction occurs in one of the participants in the network, the system continues to work with other participants; security can be ensured because the transactions carried out in the system can be seen by everyone; it is very difficult for anyone to modify the device; in the event that such a change occurs, it will be noticeable to other participants; it will reduce the transaction cost; This is the "advantages of blockchain technology". (Fanning, 2016)

Blockchain technology is divided into different types of networks in different sources. The first distinction; it has been made as "completely permissionless blockchain networks" and "completely permissioned blockchain networks". Another distinction is expressed as *wholly permissionless blockchain networks*, *partially permissionless blockchain networks* and *wholly permissionless blockchain networks*. Another distinction related to the blockchain network structure is that it comes in the form of fully permissionless blockchain networks, partially permissioned blockchain networks, and fully permissioned blockchain networks. The final distinction is *completely permissionless blockchain networks*, *partially permissionless blockchain networks*, *partially permissioned blockchain networks*, *completely permissioned blockchain networks*. (Lai, 2018)

1.3. Application Areas of Blockchain Technology

The foundation of blockchain technology goes back to the period of 1990-2000, but the value of the blockchain was not realized until the emergence of Bitcoin. Although the concept of blockchain has been directly evaluated in the field of financial technologies due to the application of Bitcoin, which is a crypto money solution, the blockchain is currently being applied and has many applications in which it can be applied in the future. Today, it is conceptually accepted that blockchain stands out as a technology with the potential to transform the foundations of social and economic systems. Although blockchain technology is still in its infancy, it has worked flawlessly since its inception and has been successfully applied in both financial and non-financial fields. (Crosby, 2016) Blockchain applications are often designed with a specific purpose or function. With new platforms that are constantly announced, there is a continuous development in the field of blockchain technology and the use of blockchain technology is expanding.

In many ways, blockchain and crypto currencies are thought to fundamentally change the way many traditional businesses study and profit. It is claimed that the transition is as important as the differentiation that occurred with the emergence of the internet and is almost revolutionary. Most of the blockchain applications today; it is focused on increasing the efficiency of business processes and reducing the time and cost spent. These managerial processes will form the basis of new commercial and strategic opportunities for the customer. Ultimately, it will have a profound impact on how people relate to each other, their employers, organizations and governments. (Fuchs, 2019)

Blockchain is a suitable solution for emerging applications including "Internet of Things, Big Data, Cloud, Edge Computing, Identity Management". Accordingly, important studies continue in the industry to evaluate the effectiveness of blockchain for various business applications, and efforts are increasing to realize potential future needs. Blockchain; can solve problems such as security and privacy

violations that may occur in learning environments, and can use training records to collect respect awards. A blockchain-based distributed system can be used for training records, exam credentials, learning records, and reputation rewards.In Devine, a similar reputation system in 2015, teachers added blocks to the blockchain that house students' educational achievements. Blockchain-based programs; can improve the digital aspects of individual and academic education. Blockchain-enabled school information centers can also be built to collect data on school systems. (Sharples, 2016)

Blockchain technology has a very important role in the healthcare industry. Thanks to the use of blockchain technology, there are records containing all kinds of data including patients' private information, medical history and treatment processes. Records; it is seen as a protocol where users can access and protect health data, guaranteeing security for a blockchain system. The technique used by healthcare providers is not qualified to cover aspects of care. This is partly due to the fact that providers with old systems are not able to keep the medical records of patients in a digital environment and transfer information. When hospitals want to eliminate this extra burden by using a technology infrastructure, substantial resources must be allocated to process medical requests and administrative records. (Casino, 2019)

Insurance companies provide health insurance to patients for a fee. Providers send payment requests directly to insurance companies rather than patients. In this context, insurance companies; It has become a central resource for patients to access personalized healthcare services. Blockchain, a digital ledger technique that can securely host ever-growing lists of data records, has the potential to facilitate the flow of information for medical records that change hands between multiple parties in healthcare programs. Blockchain; it aims to establish a link between health services and to ensure safe access to patient records. For example, a healthcare blockchain-enabled scenario is provided, in which an emergency medical technician receives the information that a patient is having an acute period through his interactive wristband. The message, along with the recorded encounter details, is forwarded to the patient's physician and hospital, which use the password security to access the blockchain healthcare account. Blockchain, with its technical structure, allows a transaction to be carried out by a node. This helps the claims settle properly. Blockchain claims adjudication process; it allows patients to make their payments in the form of remittance to their providers. While this process is taking place, the security in the blockchain is increased by limiting the data access of the blockchain through smart contracts.

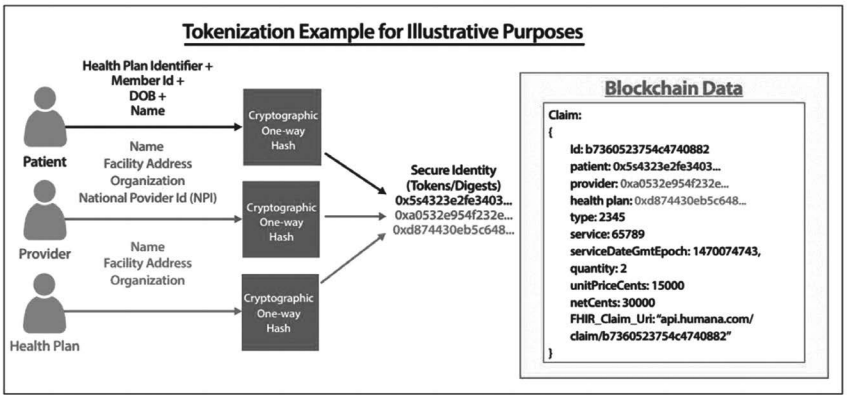

Figure 2: Blockchain Cryptography/Hash Security Concept.

Blockchain technology; it allows patients to provide secure and long-term connections to their health records. Broeder highlighted several problems that need to be solved for blockchain-related healthcare applications. One of them is the problem of online patient access. Blockchain must document that it will take action to resolve any difficulties that may arise from the need for unfinished legal variations. These solutions include regulations to update the blockchain.Another blockchain put forward by Eckblaw is presented on the concept of "MedRec". MedRec; using blockchain technology, it allows sharing medical records directly with a patient. MedRec, however, uses blockchain smart reconciliations to find "patient-provider" relationship authentication and relevant medical record information.

Blockchain technique; by providing real-time contract tracking and the ability for users to determine when reconciliations are complete, it can renew health care reconciliation management and reduce costs by improving the health care system. Technical; it provides real-time tracking, eliminates mistakes with smart reconciliation blockchain service, improves contract management. As a futuristic software in healthcare, it can create positive effects on supply chain activities and outcomes by increasing applied analytical productivity related to various digitized data about services. The result is increased productivity, reduced costs in healthcare supply chain management, and improvements in quality control positively impacting the quality of overall patient care. Blockchain technology; it is applied in a wide variety of financial areas, including commercial services, payment transactions, money transfers, exchange of financial assets, digital identity management, prediction markets. Since blockchain has an important mission in the development of the global economy, it is hoped that it will benefit banking services and society at large. Blockchain technology; it promises much more useful methodologies for performing transactions such as "securities, digital payments, credit management schemes, general banking services".

With the acceptance of this technique by the financial sector, cost savings will be achieved in areas such as "central financial reporting, central actions, business operations". Some of the world's most important banks have joined forces with blockchain company *R3CEV* to create a "blockchain" based system by going to the consortium. Examples of these collaborating banks are "Goldman Sachs, Santander, Bank of America". (Casino, 2016) Blockchain technology, in the public sector; it has many uses such as "voting, document management, digital identity-passport, social security system, tax system". States are trying to create opportunities for the adoption of blockchain technology in the public sector to "reduce cost" and "increase efficiency". In some countries such as *Switzerland*, *Cyprus* and *Singapore*, it is observed that there are official blockchain steps. NATO and the American Ministry of Defense have also started to become interested in "blockchain technology". NATO aims to use blockchain technology as the basis of classical applications such as "logistics". The US Department of Defense aims to use blockchain technology for a secure message program. Blockchain technology; it creates important expectations in the private and public sectors, as it provides an opportunity to create the infrastructure for the development of peer-to-peer areas required for digitized asset exchange without the need for an intermediary. Blockchain; it has the power to fundamentally differentiate many industries and to ensure that controls are applied regularly. (Ünsal, 2018)Another area affected by blockchain technology is the real estate industry. The real estate market is made up of parts that are quite complex and span many areas. There are many sales and rental models such as real estate rental, daily rental, real estate sales, contract sales, land sales,

timeshare. It is obvious that global real estate sales play an active role in the financial markets for the country's currency. Using blockchain technology on decentralized real estate platform; it reduces audit costs, registration and loan costs, minimizes the use of files, and provides many advantages by ensuring the payment of immovable property taxes. On the other hand, the system will not only eliminate cheating in sales, but will also be a solution to problems that span many areas. Issues encountered in *common housing* or *collaborative housing* structures implemented in different ways, especially in Europe, are on the agenda. These problems are; room rental, joint ownership, organization of residences, real estate crowd funding. With the blockchain technique, there is practical access to the residences. Likewise, with smart contracts, many benefits such as checking the legal and physical properties of the land before the transaction, paying the taxes of the parties, specifying the real rights, and deciding the situations that will occur in the debt conditions are offered. With the blockchain structure, the buyer will go to his new home; fast, safe, low cost, without the need for an intermediary. Benefits of using this technology; to increase financial confidentiality, reduce costs, prevent fraud, and accelerate real estate transactions in the international market. Blockchain technique has the potential to interfere with the basic operating conditions of existing real estate processes. Restructuring real estate management, this technology is revolutionizing many traditional business models. (Azmar, 2018)

1.4. Blockchain Applications In The World and Turkey

Various studies are carried out to develop the innovative infrastructure of blockchain technology. Established by 22 member countries by the European Union countries in 2018 to establish the European blockchain infrastructure and cooperation, EBSI has expanded to 30 member countries as of today. With this declaration, member countries are to create a knowledge network by making technical information and regulation studies about blockchain technology. Under the leadership of the European Commission, countries such as *Norway*, *England*, *Liechtenstein* have also joined the EBSI, apart from the European Union countries. Each member country creates its own blockchain node infrastructure system and works on scenarios to ensure reliable data integrity of systems such as "cross-border trading infrastructure, European identity studies, tax applications".

The international financial system and payment systems are constantly open to technological developments against digitalization. So much so that financial systems have gone through many changes, from the clearing system to the cashless system we use today. Some countries in the world, by adapting to the innovative interface of blockchain technology more quickly than other countries; they work for the integration of other sectors. At the beginning of these countries are "Austria, China, Japan, United Arab Emirates, Malta, Switzerland, United States of America, Estonia, England, Singapore". As in the world, blockchain applications are followed with interest by the public and private sectors. Within the framework of the 11th Development Plan, Turkey has decided to start working on a variety of instruments in the field of "finance" in order to implement a strong institutionally strong financial sector that will cover the period of 2019-2023.[1] With this in mind, it was decided to implement blockchain-based digital money with the support of the central bank. In this context, a Blockchain Research Laboratory was established in 2017 under the Mathematical and Computational Sciences Unit, the Information

1 https://bctr.org/avrupa-blokzininciri-altyapisi-ebsi-dereye-girdi, (December 29, 2021).

and Information Security Advanced Technologies Research Center, and the National Electronics and Cryptology Research Institute to manage the infrastructure of blockchain technologies.(Topçu, 2020)

With the studies, it is aimed to remove the difficulties in this field by creating a sustainable blockchain ecosystem. The Interbank Card Center (BKM) is among the main institutions that carry out such test studies. BKM is testing the virtual currency application called "Partridge", abbreviated as BBN and its abbreviation "Bye Bye Nakit". In 2018, under the leadership of the Turkish Informatics Foundation, the Blockchain Turkey Platform was established as an independent body in order to increase the interest in blockchain technology and to bring people who are considering working with the subject together on a common ground. Courses involving blockchain and distributed systems technology are added to the academic programs of many universities in the world, and laboratories are created for examinations. Turkey's first Blockchain center, *Istanbul Blockchain and Innovation Center*, was established at Bahcesehir University. Processing blockchain into scientific programs; it will be useful in issues such as "development of technology, transferring it, meeting the demand". (Tüfekçi, 2018)

1.5 Application in Use

Throughout history, there has been a constant effort to verify valuable documents. It is an important point that the content of the information is not changed. Encryption of data was done using simple equipment until the 20th century. In ancient Greece and Spartans, it was carried out by writing a message on a leather band wrapped around it with a wooden tool. Ribbon gained momentum with the increase of first mechanical and then electromechanical possibilities. The concept of *blockchain* first emerged in 2008 with an article written by Satoshi Nakamoto. Article; it envisaged that without being dependent on an intermediary, a trust-based transformation could be made between spouses and that these transactions could be kept in distributed ledgers. With the rapid developments in the field of internet and mobile technologies, devices capable of connecting to the internet have started to take place in every field. Smart environments aim to make life practical by controlling devices remotely and mechanically.

Devices use different technologies to communicate by acquiring meaningful data about the state of the environment or people; it creates informed models and shares data, and can even receive or send information from external sources via wired or wireless internet telecommunications infrastructure. In this context, smart environments include "smart offices, supply chain monitoring, industrial automation; applications for the elderly and disabled; autonomous patient monitoring and assistance; "smart cities" can be given as an example in the field of urban planning. The spread of the IoT[2] paradigm and the increase in physical IoT mechanisms play an important role in the development of smart environments. (Ryu, 2015)

Although basic technologies such as "different networks, innovative communication protocols, data analytics, machine learning algorithms" attract great attention by various research communities; The reliability and transparency of such environments and systems are key issues under discussion.

2 Internet of Things.

Considering the processes such as processing sensitive data produced by devices in smart environments, storing sensitive data, taking them instantly from the server, and transferring them over the network, it is predicted that a centralized system that can be used in these environments will create significant problems. Since devices in smart environments communicate with each other mainly through "wireless connections", the security requirements of these devices must be met. The need for security in intelligent environments is equivalent to the need for security in all other computer systems: "Not stealing information, not changing information, non-blocking of access to information".

The aim of the study is to design and develop a certification diploma based verification model that can be used in smart environments. Thanks to the model; records will be created between the actors through a distributed structure. In order for the model to be dynamic, a smart contract infrastructure will be developed, and access permissions will be defined for the actors, and it will be ensured that the actors can access and reach each other securely.

Certification Diploma Verification Process to be Applied During Registration to the System

(1) The end user declares to a certain provider that he wants to use a certain service by sending a request via mobile or web. The service provider asks the user for some personal information along with the phone number. The end user sends the requested information to the relevant service provider.

(2) The Provider sends a one-time password to the phone number information it receives in order to determine that the user is a real person and the person it claims.

(3) If the user provides the correct password, the provider records the provided information and signs it with its own private key. If the user provides incorrect information, a transaction failure notification is sent to the user.

(4) The service provider node sends the signed record to the government agency node as a "trusted third party" located in the network.

(5) government agency node; By decrypting the record with the public key of the service provider node, it checks the compatibility of the user certification diploma information provided in the record with the information on its server.

(6) The government agency servers send the result back to the government agency node, and the result is forwarded by the government agency node to the service provider node.

(7) If the end user's certification diploma verification result is correct, the service provider node performs a profile creation for the end user. It sends a pair of key information belonging to the user to the user's phone. The information will be used in subsequent uses to be able to access the apparatus. If the certification diploma verification result is incorrect, a "process failure notification" is sent to the user.

The primary step for the access control process is to define the required authorization information of the providers for each service registered and active in the mechanism. Information will be recorded in smart reconciliations. The user who has valid token information to use a service will be able to use the relevant service he/she requests.

Access control process; It starts with the user sending a request for the service that he/she wants to access to the relevant service provider node. The provider needs to generate the access token and add it to the smart contract. To create token information, three pieces of information are first combined. Then, using the SHA-3 function, the summary information is calculated.

```
createToken: function (serviceNo, randomVal, tokenPeriod) {
    var record = serviceNo + randomVal + tokenPeriod;
    var hashedRecord = web3.sha3(record);
    var signedRecordWithUserKey = web3.eth.sign(userKey,
hashedRecord).slice(2);
    App.contracts.Profiles.deployed().then(function (instance) {
      instance.addAccessToken(userKey, signedRecordWithUserKey, {
        from: App.allAccounts[0],
        gas: 500000
      }).then(function (token) {
          alert("Erisim Token basari ile olusturuldu: " + token)
      }).catch(function (err) {
        console.error(err);
      });
    });
```

Figure 3: Access Token Information Generating Function.

(1) A user, whose certification diploma verification has been completed and registered in the system, selects the service he wants to use through the application and sends the service usage request to the blockchain network. The user sends a request for information about a particular service to the service provider via the web application. In the content of the sent request; user's address, service number, service provider's address and token information.

(2) Smart consensus checks whether there is a valid token information with the information provided by the requesting user.

(3) The result of the token check operation is notified to the service provider node.

(4) If a positive result is obtained from the smart reconciliation, the user will be provided with access to the relevant service's information.


```
checkAccessControl: function () {
    var hashedToken = App.getToken(userKey, serviceNo, SP);
    var r = `0x${hashedToken.slice(0, 64)}`
    var s = `0x${sihashedTokeng.slice(64, 128)}`
    var v = web3.toDecimal(hashedToken.slice(128, 130)) + 27
    App.contracts.Authenticator.deployed().then(function (instance) {
      return instance.authenticateUser.call(hashedToken, v, r,
s).then(function (result) {
        if (result == userKey) {
          alert("Erişim token'i doğrudur. Kullanıcı istenilen bilgiye
erişebilir !")
        }
      }).catch(function (err) {
        console.error(err);
      });
    });
  }
```

Figure 4: Access Token Information Control Function.

Certification diploma verification is one of the most basic requirements for ensuring the security of a mechanism. In the examination, it is recommended to create a reliable profile of the user by the service provider. During the registration stage, a prerequisite for the user will be added to the agreement by the service provider in connection with the information requested from the user. The attached record contains the open information of the user. This record can then be used by other nodes. Sensitive and confidential information other than this information will be transmitted to the user over the phone.

With the proposed model, a two-stage process is designed for the certification diploma verification processes of the users who will join the system. The communication in the first stage takes place between the end user and the service provider. In the blockchain-based certification diploma verification model proposed within the scope of the audit, 2-factor verification method is used. In the first stage, certification diploma verification is designed via the mobile device owned by the user. In the second phase, it is proposed to verify the user certification diploma information by "cross-examination" through a government agency as a third trusted party.

Data centralization in classical systems leads to questioning of trust in data. Data held on a central server or a distributed database is always open to manipulation. With the emergence of third parties that provide "guarantee of trust", the expenses of the parties increase. As a solution to the shortcomings, with the development of blockchain technology, it is seen that decentralized applications and smart contracts are becoming increasingly important in terms of trust in data.

The model proposed within the scope of the study also makes a contribution in terms of access control mechanisms. It provides data sharing under a secure ecosystem on the blockchain. With the application made within the scope of the study, it was ensured that the model that will use smart contracts has a dynamic structure. As can be seen, the services offered by the providers are carried out through smart contracts. Information query-like requests are controlled by the smart contract. The defined rules are created by the service provider and recorded in the smart contract with token information. It saves some information about both the user and the service as a summary of the generated token information.

The blockchain-based certification diploma verification model proposed in the study is likely to be applied in various fields and business models.

Thanks to the certification and diploma verification that the model will provide together, a reliable communication environment and cooperation development are foreseen.

As a business model that we commonly encounter today, a user who is a customer of a particular service provider is provided with various campaigns, discounts or benefits in exchange for receiving another service. For example, a customer belonging to an airline company can receive service at more affordable prices if he stays in hotels with which the airline has a contract. Users who want to benefit from such advantages must prove that they are the customer of the relevant service provider.

Showing the membership card or email printout are the most common methods; however, when such methods are used, the service provider is required to verify the proof provided by the users. Checking

the accuracy of information shared among service providers in an ecosystem requires intensive telecommunication and time. This can be a challenging process.

With the model proposed in the thesis, any transaction made on the network will be instantly visible to all nodes.

Therefore, secure data telecommunication and data integrity will be ensured.

2. CONCLUSION

As a result of technological developments removing spatial boundaries and reducing temporal boundaries, the need for data to be unchangeable, verifiable and constantly accessible has emerged. Technology provides wide technical application areas along with the blockchain structure that rises as a value.

The method proposed in the study based on the blockchain structure. Blockchain technology has the potential to affect social, economic and public areas. Blockchain can be used in the field of education such as training documents and diplomas. The training data is added to the blockchain by the institution providing the document. Blockchain provides a continuous public record against the loss of private records against regulations in the institution.

As a result, it will have a strong structure against the situations where diplomas are stored in a distributed structure, the closure of the diploma issuing authority or the loss of accessibility. Since the data is stored with the blockchain structure, it is almost impossible to change it, and in this way the data is secured.

Storing diplomas on the blockchain brings the advantages of document forgery, accessibility, data verification, and data storage in a redundant way, and it is a viable method. On the other hand, considering the fact that it reduces the burden of data centers thanks to its distributed structure and eliminates the communication problem, and eliminates printing costs thanks to its digital data, it is seen that it will make a financial contribution. With this aspect, the thesis will also give an idea to the studies to be done to see the cost contribution of blockchain applications.

The aim of the thesis is to provide the architecture of a secure certification diploma verification model by taking advantage of the uniqueness of the blockchain. This is provided with the Smart Contract infrastructure so that it can be more dynamic.

In this context, in this study, a secure communication infrastructure has been established between actors in smart environments who do not trust each other.

Blockchain-based certification diploma verification model provides a secure communication model on a decentralized body between actors in smart environments. At the same time, it can follow the actions performed by the actors through a web application.

In this study, a comprehensive literature search was conducted on blockchain technology, which is developing and its usage areas are widespread. Information about smart contracts, blockchain platforms, programming languages, which started to become popular with blockchain technology, was given. A literature search was conducted on decentralized applications, whose reliability is indisputably at the forefront compared to classical application solutions. After all this literature research, "DAPP"[3] was developed, which includes a smart consensus developed with Solidity language, running on a local Ethereum private blockchain. With DAPP, universities will be able to store the diplomas of their graduates on the blockchain in an unchangeable, traceable and transparent manner. Employers will be able to inquire about the validity of the diplomas presented to them by graduate students applying for a job through DAPP. Diploma data does not allow any interference, as it is not kept in a centralized base and is recorded on the blockchain. Thanks to this application; Unlawful gains and diploma fraud will be prevented.

The proposed model is likely to be applied in different areas. Aiming to create a suitable infrastructure for actors who do not trust each other, this model provides a secure and systematic exchange of information between actors. Thanks to the "certification diploma verification" and "access control mechanism" features that the model will provide as a whole, it is foreseen that a reliable telecommunication environment will be created and cooperation will develop between service providers.

In the proposed model, another important issue is the need to increase the security in the system if the institution that approves the certification diploma verification is not in the system as a formal entity. It is not enough just to verify the end user's certification diploma; therefore, it is important to use other information together with a one-time password.

REFERENCES

Al-Fuqaha, A., M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash. (2015). "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", *IEEE Communications Surveys & Tutorials*, 17(4), p.2347–2376.

Topçu, A., and B. Sümerli Sarıgül, S. (2020). "Dünyada ve Türkiye'de Blok Zinciri Teknolojisi: Finans Sektörü, Dış Ticaret ve Vergisel Düzenlemeler Üzerine Genel Bir Değerlendirme", *Avrupa Bilim ve Teknoloji Dergisi*, p.37.

Topçu, A., and B. Sümerli Sarıgül, S. (2020). "Dünyada ve Türkiye'de Blok Zinciri Teknolojisi: Finans Sektörü, Dış Ticaret ve Vergisel Düzenlemeler Üzerine Genel Bir Değerlendirme", *Avrupa Bilim ve Teknoloji Dergisi*, p.37.

Atlam, H.F. and G.B. Wills. (2019). "Intersections Between IoT and Distributed Ledger", *Advances in Computers*, Elsevier, Vol. 115, p.73–113.

3 Decentralized Applications

Avunduk, H. and H. Aşan. (2018). "Blok Zinciri (Blockchain) Teknolojisi ve İşletme Uygulamaları: Genel Bir Değerlendirme", *Dokuz Eylül Üniversitesi İktisâdi ve İdarî Bilimler Fakültesi Dergisi*, 33, 1, p.371.

Bashir, I. (2017). *Mastering Blockchain*, Packt Publishing, Birmingham, p.26.

Blockchain Türkiye Plâtformu, *Blokzinciri Teknolojisi Terminoloji Çalışması*, p.16.

Blockchain Türkiye Plâtformu, *Blokzinciri Teknolojisi Terminoloji Çalışması*, p.16.

Brown, Phillip. (2013). Education, opportunity and the prospects for social mobility. British Journal of Sociology of Education 34, no. 5-6. p. 678-700.

Catarinucci, L., D. De Donno, L. Mainetti, L. Palano, L. Patrono, M.L. Stefanizzi, L, Tarricone. (2015). "An IoT-Aware Architecture for Smart Healthcare Systems", *IEEE Internet of Things Journal*, 2(6), p.515–526.

Çetin, S.C. (2018). Implementing A Blockchain Protocol and Creating A Digital Asset Transfer Environment, Thesis, Bahçeşehir Üniversitesi, İstanbul, p.40.

Deshpande, A. K., Stewart, L. Lepetit, S. Gunashekar. (2017). "Distributed Ledger Technologies/ Blockchain: Challenges, Opportunities and the Prospects for Standards", *Overview Report*, BSI Group, p.1.

Erözel Durbilmez, S., S.Yılmaz Türkmen. (2019). "Blockchain Teknolojisi ve Türkiye Finans Sektöründeki Durumu", *Finans Ekonomi ve Sosyal Araştırmalar Dergisi*, 4(1), p.32.

Haveman, R., and S. Timothy. (2006). The role of higher education in social mobility. The Future of children. p. 125-150.

https://bctr.org/avrupa-blokzininciri-altyapisi-ebsi-dereye-girdi, (December 29, 2021).

https://github.com/blockchain-certificates, (December 13, 2021).

https://webrazzi.com/2017/08/07/turkiyede-blockchain-userans, (December 15, 2021).

https://www.synopsys.com/glossary/what-is-cryptography, (November 30, 2021).

Kırbaş, İ. (2018). "Blokzinciri Teknolojisi ve Yakın Gelecekteki Uygulama Alanları", Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 9, 1, p.80.

Kim, H.M. and Laskowski, M. (2018). "Toward An Ontology-Driven Blockchain Design for Supply-Chain Provenance", *Intelligent Systems in Accounting, Finance and Management*, 25(1), p.18–27;

Li, S., Da Xu, L. and Zhao, S. (2015). "The Internet of Things: A Survey", *Information Systems Frontiers*, 17(2), p.243–259; Whitmore, A. Agarwal, A. Da Xu, L. 2015, "The Internet of Things-A Survey of Topics and Trends", *Information Systems Frontiers*, 17(2), p.261–274.

Mendi, A.F. and A. Çabuk. (2018). "Bitcoin'in Arkasındaki Güç: Blockchain", *GSI Journals Serie C: Advancements in Information Sciences and Technologies*, 1, (1), p.18.

Mohanty, S.P., U. Choppali, and E. Kougianos. (2016). "Everything You Wanted to Know About Smart Cities: The Internet of Things is The Backbone", *IEEE Consumer Electronics Magazine*, 5(3), p.60–70.

Ryu, M., J. Kim, and J. Yun (2015). "Integrated Semantics Service Platform for The Internet of Things: A Case Study of A Smart Office", *Sensors*, 15(1), p.2137–2160.

Seirawan, R. (2019). *Applying Blockchain in Exchanging Data*, Thesis, İstanbul Technical University, İstanbul, p.12.

Stefanov, D.H., Bien, Z. and Bang, W.C. (2004). "The Smart House for Older Persons and Persons With Physical Disabilities: Structure, Technology Arrangements, and Perspectives", *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, 12(2), p.228–250.

Tüfekçi, A., and Ç. Karahan. (2019). "Blokzincir Teknolojisi ve Kamu Kurumlarınca Verilen Hizmetlerde Blokzincirin Kullanım Durumu", *Verimlilik Dergisi*, 4, p.165–166.

Tüfekçi, K., "Blokzincir Teknolojisi ve Kamu Kurumlarınca Verilen Hizmetlerde Blokzincirin Kullanım Durumu", p.182.

Usta, A., S. Doğantekin. (2019). *Blockchain 101 v2*, Bankalararası Kart Merkezi, p.12.

Williams, G., D. Gunn, E. Roma, and B. Bansal. (2016). *Distributed Ledgers in Payments: Beyond the Bitcoin Hype*, Bain&Company, p.1.

Wollschlaeger, M., T. Sauter, and J. Jasperneite. (2017). "The Future of Industrial Communication: Automation Networks in The Era of The Internet of Things and Industry 4.0", *IEEE Industrial Electronics Magazine*, 11(1), p.17–27.

Zhao, J.L. Fanan, and J. S. Yan. (2016). "Overview of Business Innovations and Research Opportunities in Blockchain and Introduction to the Special Issue", *Financial Innovation*, p.2.