Blockchain Security

Berk Adalı
Computer Engineering
Dokuz Eylul University
Izmir, Turkey
berk.adali@ceng.deu.edu.tr

Elif Karataş
Computer Engineering
Dokuz Eylul University
Izmir, Turkey
elif.karatas@ceng.deu.edu.tr

***Abstract*—Research on blockchain structure, security and usage areas. Project on creating basic blockchain and analyzing.**

Keywords—blockchain, bitcoin, block, hashing, consensus, proof of work, mining, transaction

I. INTRODUCTION

Nowadays, with the common use of network systems, we have reached an unimaginable amount of data. These data can be about many things.

One of the most common things people trade in daily life is money. They do this mostly through banks. Therefore, there is a lot of sensitive data in banks. Many people who want to access this sensitive data organize cyber attacks. Due to the excess of sensitive data in the banking sector, it is very important to safely store their data.

Today, the storage and security of these data is manage from a center. However, in 2008, the first blockchain was conceptualized by Satoshi Nakamoto. Subsequently, Nakamoto implemented the first core component and cryptocurrency, bitcoin. This component served as a public ledger keeping track of all transactions on the network. In this way, it became the first virtual currency that did not need a center or a reliable authority. In this way, the double spending problem is solved. This problem is that an identical digital token can be spent more than once.

The fame of the blockchain was realized in this way with the bitcoin system.

Generally, the structure of blockchain consists of blocks. Blockchain is an ever-growing list of registers. Each block stores the cryptographic hash function of the previous block. These blocks are managed as protocol-dependent communication between nodes and peer-to-peer networks. Each change requires consensus. Therefore, records in a block cannot be changed later. If a data is desired to be changed, all subsequent blocks must be changed. In addition, since it is clear who is responsible for the change in each block. In this way, reliability increases.

Blockchain's most important advantage is that it is reliable. Storing data on each node, not being managed from a center, and having everyone's approval increases its reliability. This verification is carried out using the Proof of Work algorithm. This is also called mining.

In most classical database systems, all records are based on a few servers. Therefore, any cyber attack or technical malfunction eliminates the reliability of the system.

Also, not needing any extra third party tools for security in blockchain reduces its cost.

One of its disadvantages is the 51% attack. The acquisition of more than 50% of the network hashing power can result in malicious control of transactions with sufficient mining power. But this possibility becomes less and less because the more the chain gets, the more difficult it is to replace previously certified data. As a related disadvantage, if the chain increases, the space needs more data storage.

Another disadvantage is that data exchange is very difficult. Data exchange requires a hard fork where a chain was abandoned or a new one started.

Another disadvantage is that it has asymmetric cryptography. If users lose their private key, they also lose access to their data (for example bitcoin).

Although blockchain is not used in many sectors today, it is a data recording system that can change depending on its advantages in the future. We are likely to see much more of its use in the future in areas such as the voting system, insurance system, supply chain and even social media. Many countries and sectors continue their initiatives in this field.

II. RELATED WORKS

A. How Does Blockchain Work

Blockchain consists of three basic things. These; The first is cryptographic key pairs. It provides us with a secure digital identity reference. Second, the blockchain structure is a P2P network. Instead of a central authority, the community controls you and decides whether to add to the chain. The third is network servicing protocol. Processing lament data, signatures, and timestamp are published to network participants. Public blockchains encourage service to the network by offering cryptocurrencies as rewards for their efforts. (Bitcoin, ether exc.)

Business stuff on blockchains now mostly happens on platforms like Ethereum. Unlike Bitcoin, Ethereum is versatile and can be used in different areas. These are document processing, voting systems, etc. Turing-Complete Virtual Machines specially introduced for Ethereum use. EVMs can be programmed. Solidity, the programming language of EVM, enables developers to code all kinds of smart contracts. Also, these smart contracts led to the creation of another platform like Ethereum, Dapps, which allows smart contracts to be coded. Because contracts are open to everyone, according to the blockchain operation, sometimes businesses may choose to keep part of the contract in a centralized

environment or create a custom blockchain fork. These blockchain networks types are:

Public Blockchain: It is a chain that is open to everyone. It is allowed to suggest new transactions and add them to the chain as long as they are valid. There is no central authority. The best known examples are Ethereum and Bitcoin.

Consortium Blockchain: Limits the number of users that can participate in the consensus process. A company can be compared to a board of directors. Examples are Energy Web Foundation, Corda and Azure Multi-Member blockchain.

Private Blockchain: Centralized blockchains. A single node only needs permission. Examples are supply chain management, government management, healthcare and the financial sector [1].

B. Blockchain Oracle's

Sometimes it is necessary to learn the results of transactions made on blockchains. Blockchain Oracle's are used in such times. For example, consider two people who bet on which team a and b will win. By agreeing on the wagering terms, they lock the deposits into a smart contract that will release the deposits depending on who wins the match or competition. Since smart contracts cannot interact with external data, they have to get support from Oracle, a third-party service that provides external information. After the contest or match is over, Oracle queries a trusted API and passes it to the smart contract to find out which team won. It then sends the funds to the individuals according to the contract result [2].

C. Blockchain in Turkey

Turkey's first blockchain project by Borsa İstanbul's Information Technology team in 2018. There is no technical document regarding the work done, but the an announcement has been posted on Borsa Istanbul's website. Blockchain Research Laboratory established by Tübitak Bilgem with working as a powerful guiding behalf of Blockchain in Turkey. Held in Ankara by TUBITAK as research in the First Workshop Blockchain, has been announced that Takas Bank, Hazine Müsteşarlığı, TCMB supports this. Especially Takas Istanbul undertakes many projects. Takas Istanbul announced the products that it has completed its tests and used by itself as BIGA and Value Transfer System (Değer Transfer Sistemi). Other known blockchain projects are Crowdfunding (Kitle Fonlaması) and Private Pension System (Bireysel Emeklilik Sistemi). Also at Bahcesehir University in Istanbul, Turkey's first center of Blockchain was established. (Blockchain and Innovation Center - blockchainIST Center) [3].

D. Deloitte's Research

Deloitte did some research on Blockchain around the world in 2018. There are many questions in these studies. According to the responses of the companies, the most important reason for choosing Blockchain are:

- 32% speed
- 28% new business opportunities and revenue sources
- 21% high security and low risk

According to another question posed, companies with 43% rate their approach to blockchain as critical. Blockchain is thought to be important, but not critical, with a rate of 29%. It is stated that they are related with a rate of 21%. Another question was asked which departments of companies are more important for blockchain. Companies responded with 39% IT, 39% company, 15% Innovation. The most preferred Blockchain models by companies are as follows:

- 52% Permissioned blockchain
- 44% Private blockchain
- 44% Public blockchain
- 36% Consortium blockchain

Blockchain usage areas in the world are:

- 53% Supply chain
- 51% IoT
- 50% Digital ID
- 44% Digital records
- 40% Digital currency
- 30% Payments
- 12% Voting More information can be found in Deloitte's Breaking blockchain open [4].

E. Risks of Blockchain

The risks of using blockchain can be summarized as follows:

Standard risks: These are the risks that organizations may face with the business process in general. These can be strategic, regulatory, business continuity, operations, reputation, contract, information security, and supplier.

Value transfer risks: Unlike the old system, information is transferred in the new system without being connected to a center. Sensitive information transferred during transfer may be at new risks. These can be consensus protocol, key management, data privacy and liquidity.

Smart contract risks: Problems with coding smart contracts may occur. These can be business and regulatory, contract enforcement, legal obligation and information security. Detailed information on these risks can be found in Deloitte's Blockchain risk management report [5].

F. Blockchain Attacks

Sybil Attack: A Sybil attack is not an attack on one person, but an attack on the network as a whole. The attacker adds multiple nodes with unreal accounts to the system and run from a single part. In this way, the attacker targets attacks such as multiple spending or data capture.

Selfish Mining Attack: The high number of layers in a blockchain ensures that the data is not changed and is well protected against attackers, but this also has some disadvantages. Some miners can create a small gap for themselves when creating a client with 2 or more blocks at the top of the chain. Thanks to this interval, it can create a hidden block and spend double.

51% Attack: A 51% attack is a possible attack on Bitcoin or a blockchain network by controlling the majority of the hash rate of a single person or organization and causing disruption to the network. Thanks to this majority, they can reverse previous work or limit the powers of other miners and capture a large portion of their data.

Finney Attack: The Finney attack type is in a way an attack on the transaction verification mechanism. In order for this attack to be carried out, not only the attacker but also the miner must be involved. This attack can be found on systems that require a single approval. Since a single approval transaction is required in response to the mistake made by the user, the work done behind is copied and converted into a double payment system.

Race Attack: The race attack allows the attacker to accomplish the process he planned to spend twice without mining. The attacker sends it to the user with an unverified job and also takes another action on the network. In this way,

the transaction seen by the seller is actually just an illusion. In this way, he can do whatever he wants in the back [6].

G. Mining

Mining is the registration and approval of crypto money transfers as well as crypto money production. Each time a new unit is produced, the difficulty levels of unlocking the blocks formed also increase. Therefore, mining requires a computer with very powerful processors, and this is increasing.

For example, mining for Bitcoin is the process of verifying transaction information and storing it on the blockchain. Mining creates a consensus ecosystem. To make a Bitcoin transaction spendable, there must be at least six network confirmations. Miners generally approve new transactions and save them on the blockchain, which are then added to the blockchain, then approved. For Bitcoin, the Bitcoin buyer can only spend Bitcoin when the transaction is confirmed. However, all of this requires a significant amount of computing power. The reason miners do these calculations is because they are rewarded.

Each transaction typically includes a transaction fee. This is taken as a Bitcoin surplus between the input and output of the transaction. The winning Bitcoin miner gets the right to receive extra Bitcoins on transactions included in the winning block.

The maximum amount of Bitcoin the miner can buy from a block is programmed to be halved every 4 years.

The rewards were 50 Bitcoins per block in January 2009. It was later reduced to 25 Bitcoins per block in November 2012 and to 12.5 Bitcoins in July 2016. With the halving in May 2020, the reward fell from 12.5 BTC to 6.25 BTC. It will continue to decrease until 2140 [7].

H. Proof of Work Algorithm (Consensus Algorithm)

Blockchain is a large database and anyone can check whether funds have already been spent. To give an example where we write the transactions of our friends in the notebook; It can be written as Alice paid Bob five units, Bob paid five units to Carol. But there is another detail. In every transaction, you refer to the transaction from which the funds came. So: An entry appears that Bob paid Carol with five units from his transaction with Alice earlier. If Bob tries to do another transaction with the units he just sent to Carol, it will be noticed by everyone and the transaction is not allowed to be added. But this system is not very reliable on high participants, so the PoW algorithm must be applied.

The ledger mentioned above is the blockchain. Transactions are written into blocks instead of being added one by one. Transactions are reported to the network, and users who create blocks then include those transactions in a candidate block. Transactions are considered valid only after the candidate block has become an approved block. Block data is hashed. This hash value is unique for each block. It is impossible to obtain the data by turning the hash back. However, if the input is known, it can be checked whether the hash is correct or not. It is enough to put the data into the function and check whether the output is the same.

The hash value of the data provided in the Proof of Work algorithm must meet certain conditions. Therefore, the data must be hashed and checked whether the conditions are met. If the conditions are not met, a small change in the data is required to get a different hash.

When creating a block, usually all transactions we want to add are combined together. But since the dataset does not change, another piece of information must be added that can change, otherwise it will always have the same hash as the output. This added variable is called nonce. This number is changed on each trial, resulting in a different hash. This process is called mining.

Mining is a process that consists of collecting blockchain data and hashing data by adding nonce until the hash value is found. When a hash value that meets the protocol conditions is found, the block with that new hash value is reported to the network. Other participants of the network update their blockchains to add the new block.

The higher the hash rate in a network, the harder it is to find the hash value. This feature prevents blocks from being found too quickly because computers with high processing power are needed. This is an application that provides security [8].

İ. Blockchain Structure

In real world, Blockchain structure is different from Basic Blockchain project.

The framework (let's simply call it a library) should be programmed first. There must be protocols here. Then a must-have light VM - virtual machine - that is, a small-scale virtual machine virtual machine should be developed. The software you will program to the miners will use it and when the smart contracts arrive, it will run them in the VM and process the result. Your host-server software that should work over the network-internet, or even more than one. Its software should also be created with a pre-written framework. For miners - not required if PoS is present - wallet must be programmed. This software should also include the VM. The main framework has to be written first and then it is necessary to use it in all other software. Blockchain-based software such as Bitcoin, ethereum etc. started by doing these [9].

J. Security of Blockchains

Security in the blockchain is achieved by protecting the data in the block. Safety-related information:

Penetration defense: An approach that uses multiple corrective measures to protect data. It follows the principle that it is more efficient to protect data in multiple layers than a single layer of security.

Minimum privilege: Access to data is reduced to the lowest possible level to strengthen the level of security.

Manage vulnerabilities: Vulnerabilities are checked and identified. These vulnerabilities are managed by verifying, changing, and applying patches.

Manage risks: Risks are identified, evaluated and controlled.

Manage patches: Code, application, operating system, firmware, etc., by purchasing, testing, and installing patches. such defective parts are patched [10].

III. BASIC BLOCKCHAIN

The project is about understanding the general blockchain structure and security. By creating a simple blockchain structure, the structure and security of the blockchain will be examined step by step.

A. Design Schema

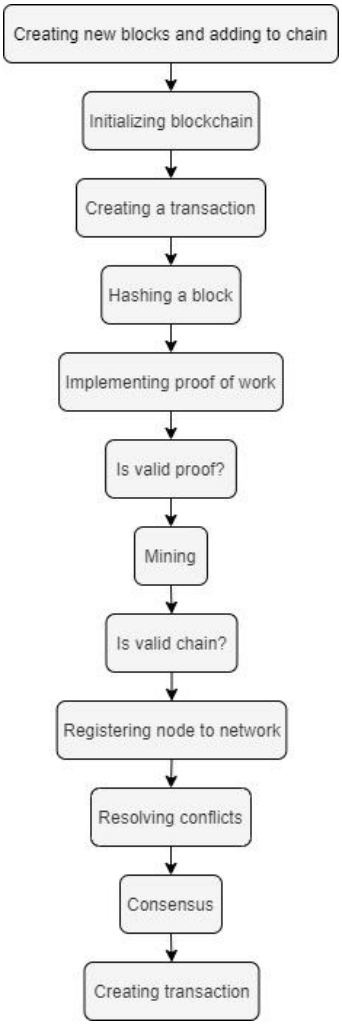

Fig. 1. Design schema of Basic Blockchain.

B. Steps

- Firstly, new blocks are created and added to the chain. The blocks contain the index, timestamp, list of transactions, proof and hash of the previous block.
- The transaction is added to the block.
- Proof of work is implemented. PoW is about mining. The purpose of PoW is to find a number that solves the mathematical problem.
- The number should be difficult to find, but easy to verify by others on the network.
- The validation of the chain is confirmed by checking the hash. Nodes to be added to the network are created.
- Resolving conflicts is a method that loops between our neighbor nodes and downloads their chains. If a valid chain of greater length is found, it will replace it. This part is very important.
- Consensus is applied for the acceptance of transactions.
- The transaction is created. Any data can be contained in the transaction.

IV. TEST RESULTS AND DISCUSSION

Our main goal in the Basic Blockchain project is to understand how to build a simple blockchain and how to create the Proof of Work algorithm, transactions and peer to peer structure.

In the program we run using DLL, we need to connect to a server first. We connect to our own server in two separate command lines.

Fig. 2. Options on ommand line .

After connecting, there are 4 options of the program. The first of these is to connect to the server. With the connect to the server option, we establish a connection between servers with port numbers 5001 and 5002.

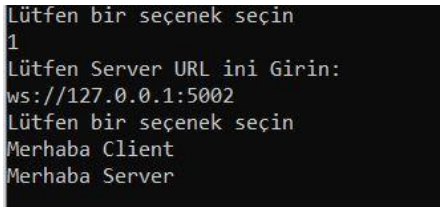

Fig. 3. Connecting to servers.

With the second option, add transaction, we can simulate a simple Bitcoin transfer process. Transaction includes sender, recipient and quantity information. With the third option, we can view the blockchain we created.

Fig. 4. Displaying the blockchain.

The displayed blocks contain the index value, the time indicator, the hash value of the previous block, the hash value of the block, the transaction transaction and the nonce value as well as the difficulty value. When we view the blockchain structure, the first block that appears is our genesis block. Therefore, there is no previous hash and transaction value.

Finally, you can exit the program.

Fig. 5. Trying mining.

Some experiments were made during the development phase of the project to understand mining logic. This trial was to change the information in the transaction so that the program provided the validation control for the block. First, it was seen that validation could not be achieved by changing the value in the transaction. Secondly, it was seen that validation could not be achieved by finding only the hash value of the block and synchronizing it according to the data we changed. This is because the *isValid* function cannot ensure that the block synchronizes the hash of the previous block. Thirdly, it was seen that validation was achieved by matching the hash of the block to the previous hash value of the block that came after it. In fact, the process of finding this hash value is referred to as mining.

With the *Mine* operations, the more 0 we add in front of the hash value, the more difficult the mining process. It returns the nonce value until it finds the hash value.

V. CONCLUSION

Blockchain, which became famous with the emergence of Bitcoin, is now used in many areas. Most of all, in today's digitalizing world, crypto coins replace physical money. Cryptocurrencies, whose value is increasing day by day, started to attract people's attention. Therefore, understanding the blockchain structure will not only help us professionally, but also in our daily routines.

One of its most important advantages is that there is no need for central authority. Although there are different blockchain structures in different areas, this is the most important feature of the blockchain logic. Its reliability is increasing. Due to its advantages, many companies and governments around the world turn to blockchain in order to manipulate their data. With the increasing popularity and use of blockchain, many studies and research are carried out on blockchain. But this can also be a disadvantage. Since there are not enough experts and responsible, things can get complicated in case of possible errors and malfunctions. Although it can be used in many areas in theory, it can create some new problems in practice.

At this time, when everything in our world is happening with data on the internet, data-related technologies are increasing rapidly. Without a doubt, blockchain is one of the very important technologies for our time.

REFERENCES

[1] How Does Blockchain Work: Guide for Businesses | web3devs developers. (2020). Retrieved 30 December 2020, from https://web3devs.com/how-does-blockchain-work-guide-forbusinesses/

[2] Blockchain Oracle'ları Nedir | Binance Academy. (2020). Retrieved 30 December 2020, from https://academy.binance.com/tr/articles/blockchain-oracles-explained

[3] YILMAZ TÜRKMEN, S., & ERÖZEL DURBİLMEZ, S. (2019). Blockchain Teknolojisi ve Türkiye Finans Sektöründeki Durumu. Finans Ekonomi Ve Sosyal Araştırmalar Dergisi. doi: 10.29106/fesa.509254

[4] Deloitte (2019). Breaking blockchain open: Deloitte's 2018 global blockchain survey.

[5] Deloitte. Blockchain risk management:: Risk functions need to play an active role in shaping blockchain strategy

[6] G. Liang, S. R. Weller, F. Luo, J. Zhao and Z. Y. Dong, "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks," in IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 3162-3173, May 2019, doi: 10.1109/TSG.2018.2819663.

[7] (2020). Retrieved 11 January 2021, from https://www.paribu.com/blog/sozluk/madencilik-mining-nedir/

[8] What Is Proof of Work (PoW)? | Binance Academy. (2021). Retrieved 11 January 2021, from https://academy.binance.com/en/articles/proof-of-work-explained

[9] Zincirleri Kırmak | Selçuk Çelik. (2021). Retrieved 11 January 2021, from https://selcukcelik.org/zincirleri-kirmak-blockchain/

[10] Prashanth Joshi, A., Han, M., & Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing*, *1*(2), 121-147. doi: 10.3934/mfc.2018007