MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE NATIONAL AVIATION UNIVERSITY

FACULTY OF AERONAVIGATIONS, ELECTRONICS AND TELECOMMUNICATIONS

DEPARTMENT OF TELECOMMUNICATION AND RADIO ENGINEERING SYSTEMS

ADMIT TO DEFENCE
Head of the Department

_______________V. HNATYUK
“_____”__________ _____2023 p.

QUALIFICATION WORK

(EXPLANATORY NOTE)

MASTER'S DEGREE GRADUATE

Topic: «USING BLOCKCHAIN TECHNOLOGY IN IOT SYSTEMS TO PROTECT INFORMATION»____.

Performer:____Mykyta ROMANOV
(Signature)

Supervisor:____Georgy KONAKHOVYCH
(Signature)

Consultants from individual sections of the explanatory:

Consultant in the «Occupational Safety» Section:__________ Batyr KHALMURADOV
(Signature)

Consultant of the «Environmental Protection» section:_________ Andrian IAVNIUK
(Signature)

N-controller:____ Denys BAKHTIIAROV
(Signature)

Kyiv 2023

NATIONAL AVIATION UNIVERSITY

Faculty of aeronavigations, electronics and telecommunications

Department of telecommunication and radio engineering systems

Speciality: 172 "Telecommunications and radio engineering"

ADMIT TO DEFENCE
Head of the Department

__________ V. HNATYUK
“_____”___________2023

TASK

for execution of qualification work

Mykyta ROMANOV
(Full name)

1. Topic of diploma work: «Using blockchain technology in IoT systems to protect information» approved by the order of the rector from «28» September 2023 №1965/ст.

2. The term of the work: from 02 October 2023 to 31 December 2023.

3. Initial work data: Blockchain integration into IoT systems for safeguarding information; Analysis of security protocols in IP Telephony and development of an operational vulnerability scheme to assess system security levels.

4. Explanatory note content: INTRODUCTION; CHAPTER 1 OVERVIEW OF BLOCKCHAIN TECHNOLOGY AND INTERNET OF THINGS; CHAPTER; 2 ANALYSIS OF PRINCIPLES OF CONSTRUCTION AND ENHANCEMENT OF OPERATIONAL QUALITY; 3 THEORETICAL ASPECTS OF PROBABILITY AND ATTACK STRATEGIES IN BLOCKCHAIN FOR IOT; CHAPTER; 4: DEVELOPMENT OF PROPOSALS FOR PRACTICAL IMPLEMENTATION; APPENDICES

5. List of required illustrative material: figures, tables.

6. Work schedule

No cf.	Task	Term implementation	Performance note
1	Develop a detailed content of the sections of the qualification work	22.05.2023-24.05.2023	done
2	Introduction	25.05.2023	done
3	CHAPTER 1: OVERVIEW OF BLOCKCHAIN TECHNOLOGY AND INTERNET OF THINGS	26.05.2023-29.05.2023	done
4	CHAPTER 2: ANALYSIS OF PRINCIPLES OF CONSTRUCTION AND ENHANCEMENT OF OPERATIONAL QUALITY	30.05.2023-07.06.2023	done
5	CHAPTER 3: THEORETICAL ASPECTS OF PROBABILITY AND ATTACK STRATEGIES IN BLOCKCHAIN FOR IOT	08.06.2023-14.06.2023	done
6	CHAPTER 4: DEVELOPMENT OF PROPOSALS FOR PRACTICAL IMPLEMENTATION	15.06.2023-27.06.2023	done
7	CHAPTER 5: LABOR PROTECTION	28.06.2023-14.07.2023	done
8	CHAPTER 6: ENVIRONMENTAL PROTECTION	15.07.2023-24.08.2023	done
9	ELIMINATION OF DEFICIENCIES AND PROTECTION OF QUALIFYING WORK	11.11.2023-31.12.2023	done

7. Consultants from separate sections

Chapter	Consultant (position, Full Name)	Date, signature	
		Issued the task	Task accepted
Occupational Safety	Ph.D. in Med., Professor Batyr KHALMURADOV		
Environmental Protection	Ph.D. in Biol., Associate Professor Andrian IAVNIUK		

8. Release date of the task: September "29", 2023

Supervisor of Qualification Work_____________________ Georgy KONAKHOVYCH
(Signature of the supervisor) (Full name)

The task has been taken on for execution ____________________ Mykyta ROMANOV
(Graduate signature) (Full name)

ABSTRACT

Qualification work «Using Blockchain technology in IoT systems to protect information» contains _150_ pages, _56_ figures, _11_ tables, _43_ used sources.

BLOCKCHAIN TECHNOLOGY, DECENTRALIZATION, INTERNET OF THINGS (IOT), PROTOCOLS, AUTHENTICATION, AUTHORIZATION.

The object of the research – Internet of Things (IoT) systems and their potential for the implementation of Blockchain technology to ensure security and information protection.

The subject of the research – the interaction between Blockchain technology and Internet of Things (IoT) systems to elevate the level of security and information protection.

The goal of the work – to investigate and implement Blockchain technology into the IoT system to enhance the level of security and information protection.

To achieve the set goal, the following scientific tasks are addressed:

1) Investigate the structure and classification of Blockchain technology.

2) Explore the features of the IoT system.

3) Develop a model of an IoT system with the integration of Blockchain technology.

4) Develop a classification and determine methods for testing the quality of IoT systems, particularly with the integration of Blockchain technology.

5) Investigate security aspects and attacks in PoS consensus protocols.

6) Determine the probability of success of an attack based on the number of confirmation blocks.

7) Describe the architecture of the program and define operational algorithms.

8) Describe the results of program execution, including the process of token creation and web application development.

The materials of the qualification work are recommended for use in the development and enhancement of Internet of Things (IoT) systems with the integration of Blockchain technology.

CONTENT

LIST OF CONDITIONAL DESIGNATIONS

1. IoT	- Internet of Things
2. JSON	- JavaScript Object Notation
3. PoS	- Proof of Stake
4. JWT	- JSON Web Token
5. DB	- Database
6. AI	- Artificial Intelligence
7. API	- Application Programming Interface
8. UI	- User Interface
9. UX	- User Experience
10. URL	- Uniform Resource Locator
11. HTTPS	- Hypertext Transfer Protocol Secure
12. FAQ	- Frequently Asked Questions
13. SDK	- Software Development Kit
14. QR Code	- Quick Response Code
15. LAN	- Local Area Network
16. WAN	- Wide Area Network
17. RFID	- Radio-Frequency Identification
18. HTTP	- Hypertext Transfer Protocol
19. VPN	- Virtual Private Network
20. DNS	- Domain Name System.
21. DDoS	- Distributed denial of servise
22. DoS	- Denial of servise
23. IDS	- Intrusion detection system

INTRODUCTION

Relevance of the topic. The Internet of Things (IoT) serves as a catalyst for changes in the manner in which devices communicate and interact in the current digital age, in which every facet of our existence is becoming more and more reliant on technology. But as a result of this increased connectedness, a serious information security issue also emerges, one that, given the dynamics of the digital age, is not only urgent but also strategically crucial.

We have a problem in ensuring effective information protection given the proliferation of connected devices, the diversity of cybersecurity threats, and the processing power of massive volumes of data. The theme "Utilizing Blockchain Technology in IoT Systems for Information Security" is recognized in this context as a tactical move in the direction of guaranteeing security in the Internet of Things.

The integration of Blockchain technology with Internet of Things systems creates new opportunities to establish a trustworthy, decentralized, and safe environment for data sharing. This lowers the danger of cyberattacks and illegal access in addition to guaranteeing the security and integrity of data.

The necessity for innovative IoT security tactics as well as the quick adoption of Blockchain technology in various sectors of the economy determine the topic's relevance. This study makes a substantial contribution to the field by pointing out novel applications of blockchain technology that improve the dependability and security of Internet of Things systems. The outcomes hold great significance for the advancement and effective assimilation of these technologies into our digital future.

The purpose and objectives of the research.

The goal of the work is to investigate and implement Blockchain technology into the IoT system to enhance the level of security and information protection.

To achieve the set goal, the following scientific tasks are addressed:

1) Investigate the structure and classification of Blockchain technology.

2) Explore the features of the IoT system.

3) Develop a model of an IoT system with the integration of Blockchain technology.

4) Develop a classification and determine methods for testing the quality of IoT systems, particularly with the integration of Blockchain technology.

5) Investigate security aspects and attacks in PoS consensus protocols.

6) Determine the probability of success of an attack based on the number of confirmation blocks.

7) Describe the architecture of the program and define operational algorithms.

8) Develop an authorization and authentication mechanism for users using JSON Web Tokens.

9) Describe the results of program execution, including the process of token creation and web application development.

The object of the research is Internet of Things systems and their potential for the implementation of Blockchain technology to ensure security and information protection.

The subject of the research is the interaction between Blockchain technology and Internet of Things systems to elevate the level of security and information protection.

The scientific novelty lies in the deep and comprehensive analysis of the interaction between Blockchain technology and the Internet of Things with the aim of enhancing the security and efficiency of information systems.

CHAPTER 1
OVERVIEW OF BLOCKCHAIN TECHNOLOGY AND INTERNET OF THINGS

1.1 Overview of Blockchain Technology

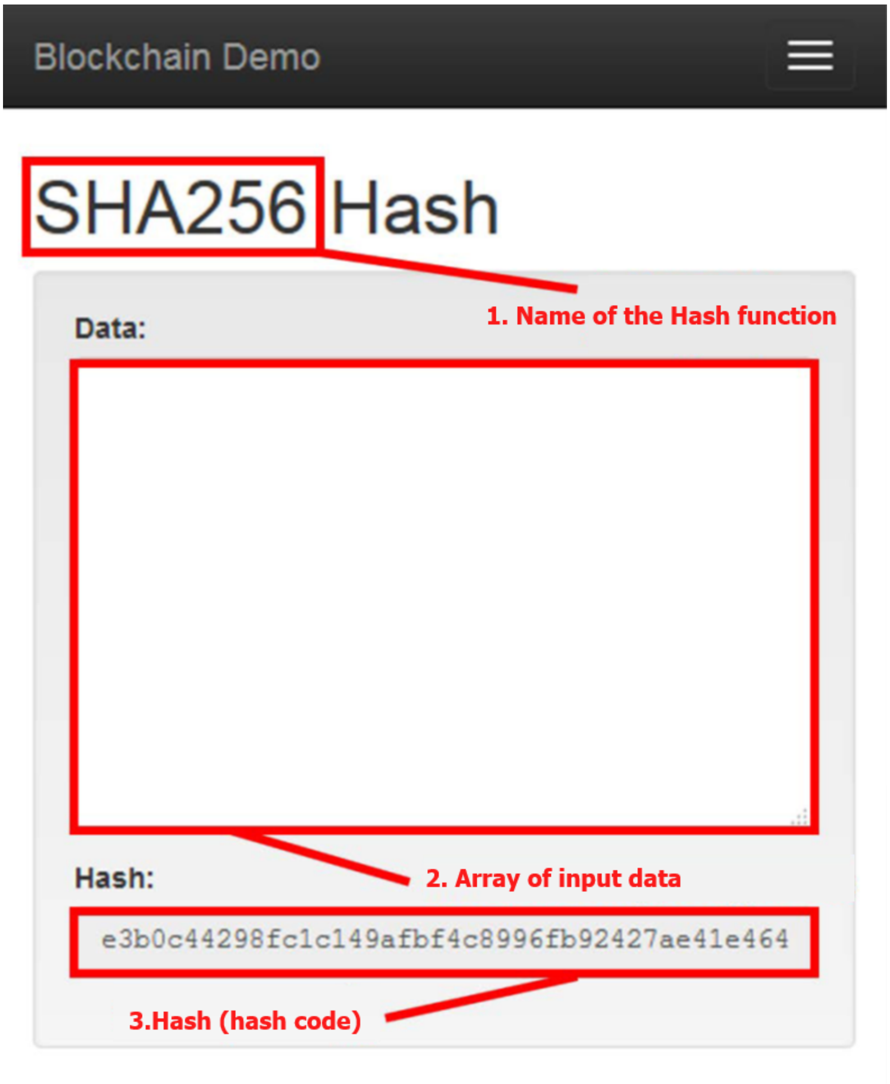
Blockchain is an information-containing, continuously linked chain of blocks that are organized in accordance with predetermined guidelines. This technique allows for the safe and dispersed archiving of all past transactions. A blockchain is made up of a series of data blocks, each of which has a growing volume as fresh blocks containing the most recent transaction records are added. It functions as a chronological database, which means that records are non-commutative because the time they are produced is intrinsically related to the data.

The information is shown as an expandable series of records. Blocks that are arranged as a linked list are used to store records and additional data. Every participant is represented by a node that communicates with other nodes and stores the complete array of data that is currently in use. Nodes can communicate with one another about changes to the list and add new entries to the end of the list.

Let us now investigate the methods by which this activity occurs as well as the features these mechanisms offer. Users can have a hands-on experience and learn how this technology works by visiting Anders Brownworth's website, where he has developed a demo version of a blockchain. He breaks down its structure in his video, beginning with the idea of hashing with the SHA256 hash function.

Let's concentrate on the primary elements of this function, as shown in Figure 1, rather than becoming too technical. Hashing is the process of using a particular algorithm to convert an array of input data of any length into a fixed-length bit string for the output. We refer to the function that carries out the transformation and embodies the algorithm as a "digest function" or "hash function."

The input data is referred to as the input array, "key," or "message." The result of the transformation (output data) is called the "hash," "hash code," "hash sum," or "message digest".



Hash: e3b0c44298fc1c149afbf4c8996fb92427ae41e464

1. Name of the Hash function

2. Array of input data

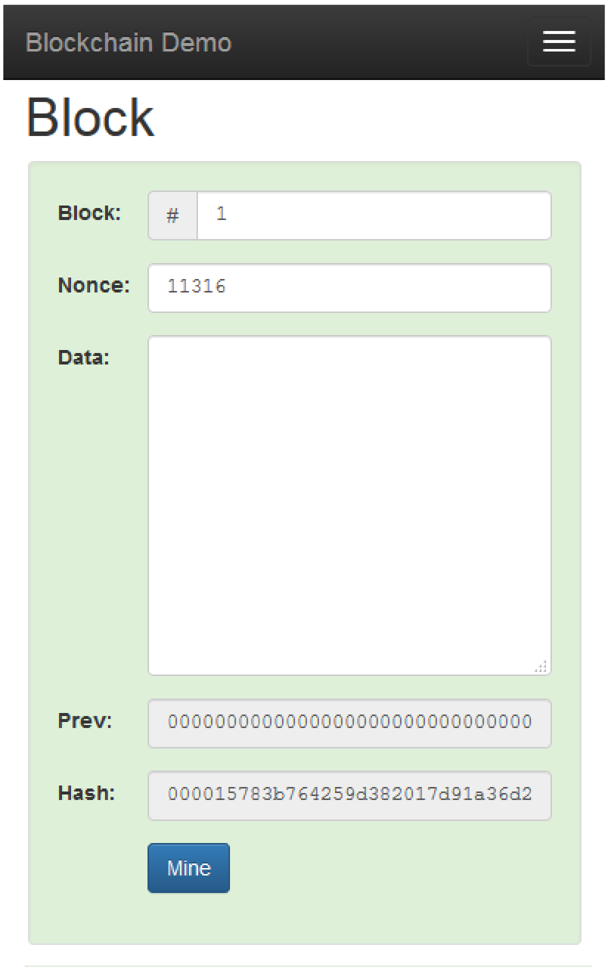
3.Hash (hash code)

Figure 1.1. Components of Hashing

The input data set that is supplied in the "Data" field is exclusive to the character set that is displayed in the "Hash" field below. Any other input data set can also generate it. Nevertheless, use the provided hash code to reverse extract the input data is a computationally demanding process.

The input data is split into four portions and the same hashing procedure is applied in the block (Figure 1.2):

- "Block" — block number in the chain;
- "Nonce" — a random number generated to achieve a hash that satisfies the conditions imposed by the developers;
- "Data" — data set;
- "Prev" — hash of the previous block in the chain.



Block

Block: # 1

Nonce: 11316

Data:

Prev: 0000000000000000000000000000000

Hash: 000015783b764259d382017d91a36d2

Figure 1.2. Chain Block Diagram

The fundamental data distribution model in a blockchain-based system can be conceptualized as the following sequence of actions:

1. A new transaction is broadcasted to all nodes in the network. The network is structured as a peer-to-peer network, and the transaction enters the pool of unprocessed data on these nodes (Figure 1.3).

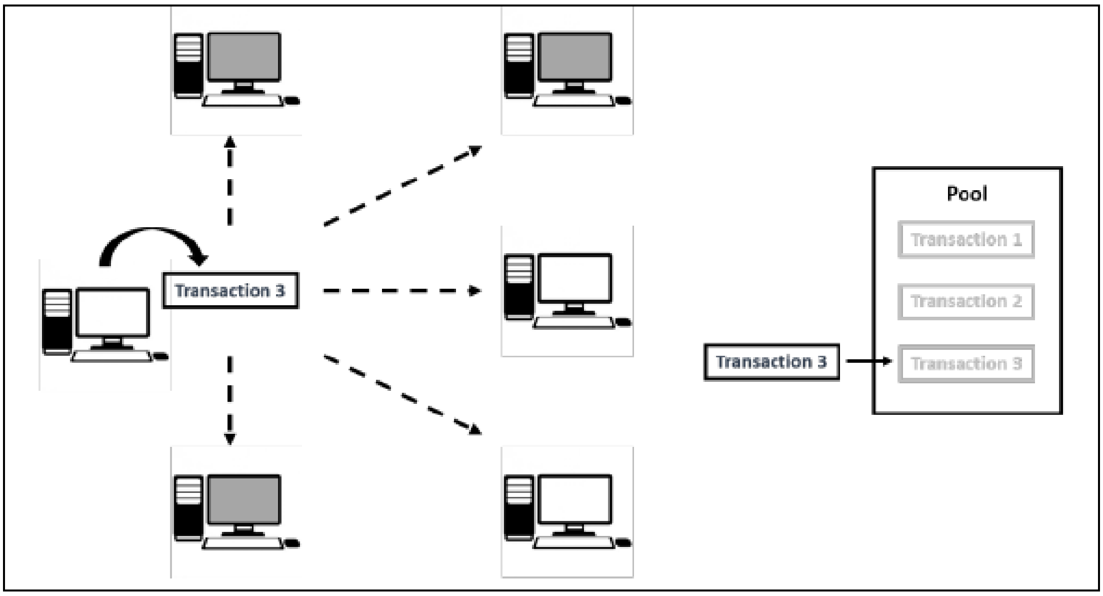
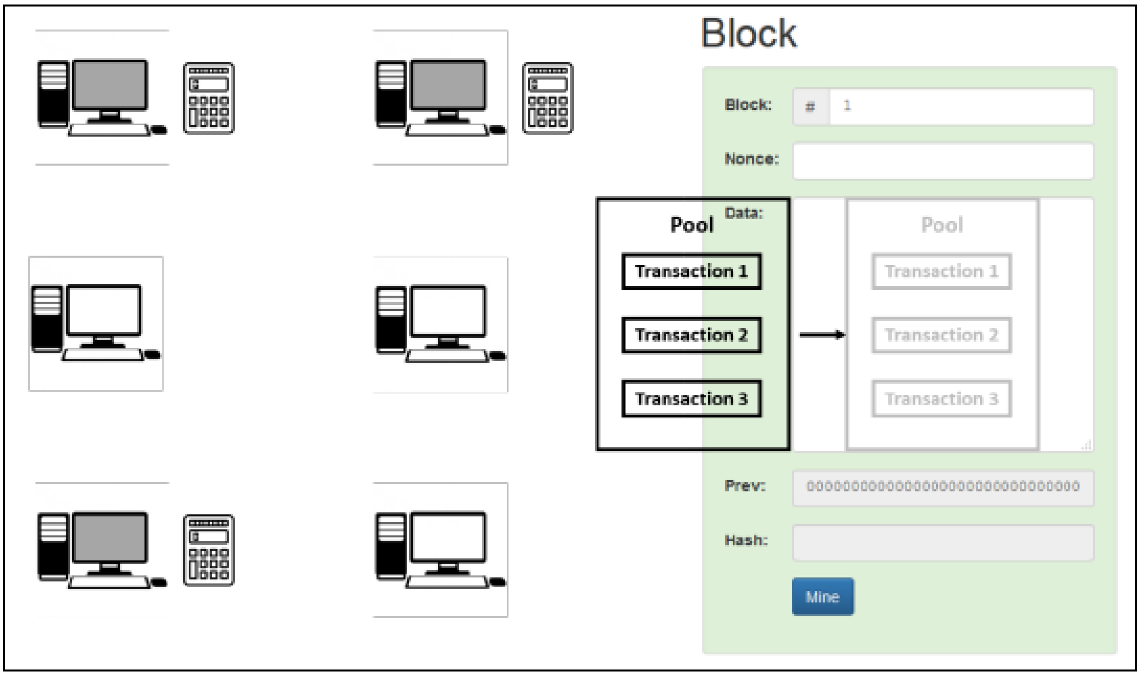


Figure 1.3. Adding a transaction to the pool of unprocessed transactions2.

2. Some nodes (highlighted in gray in Figure 1.3) add transactions from the pool of raw data to a block (Figure 1.4) by mining, which is the process of producing new structures, usually referring to new blocks in the blockchain, to ensure the operation of cryptocurrency platforms.

3. In the "Nonce" field, each miner looks for a value that would match the developers' requirements for the block hash (in the case of the Bitcoin blockchain, this meant that the condition was the existence of a specific number of leading zeros). We refer to this process as proof-of-work. At this point, a second technique for verifying authorization to carry out a block addition operation has surfaced: the proof-of-stake technique. We'll talk about both approaches later.

4. The block data is sent to all network users by the first miner to achieve a block hash that satisfies the requirements; in exchange, the miner is rewarded for adding the block (Figure 1.5). If a node misses a block, it won't be a big deal because it will ask for the information it needs to close the clear gap once it receives the subsequent block.



Block: # 1

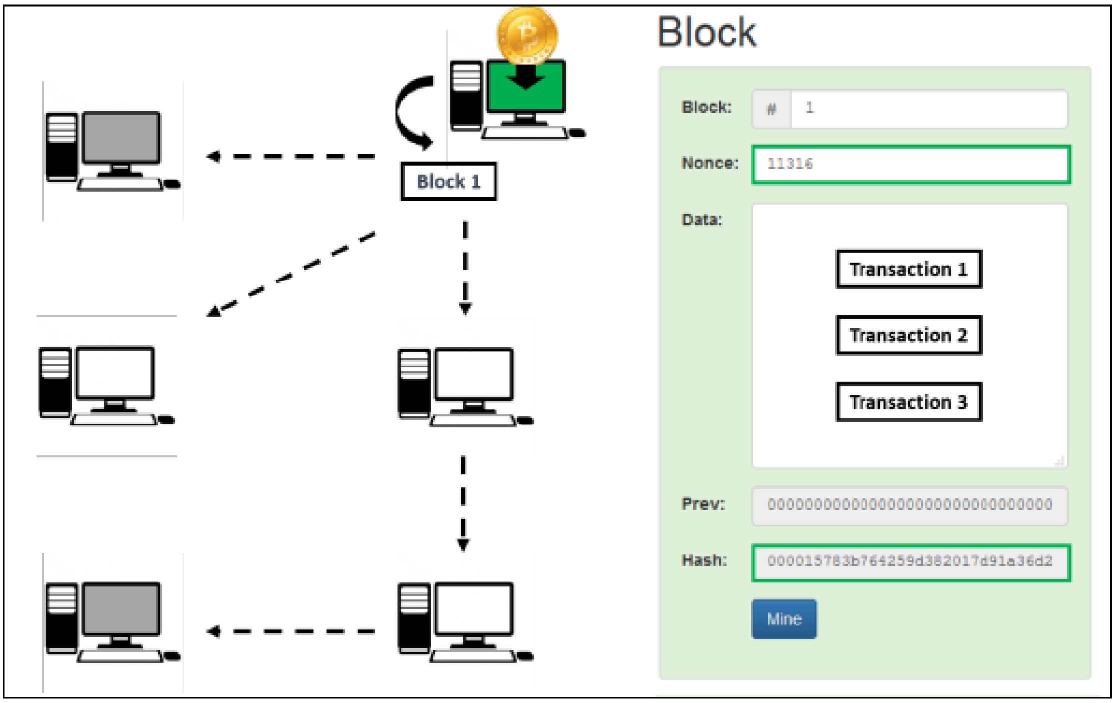
Nonce:

Data:

Prev: 00000000000000000000000000000000

Hash:

Figure 1.4. Adding the pool of unprocessed transactions to a block



Block: # 1

Nonce: 11316

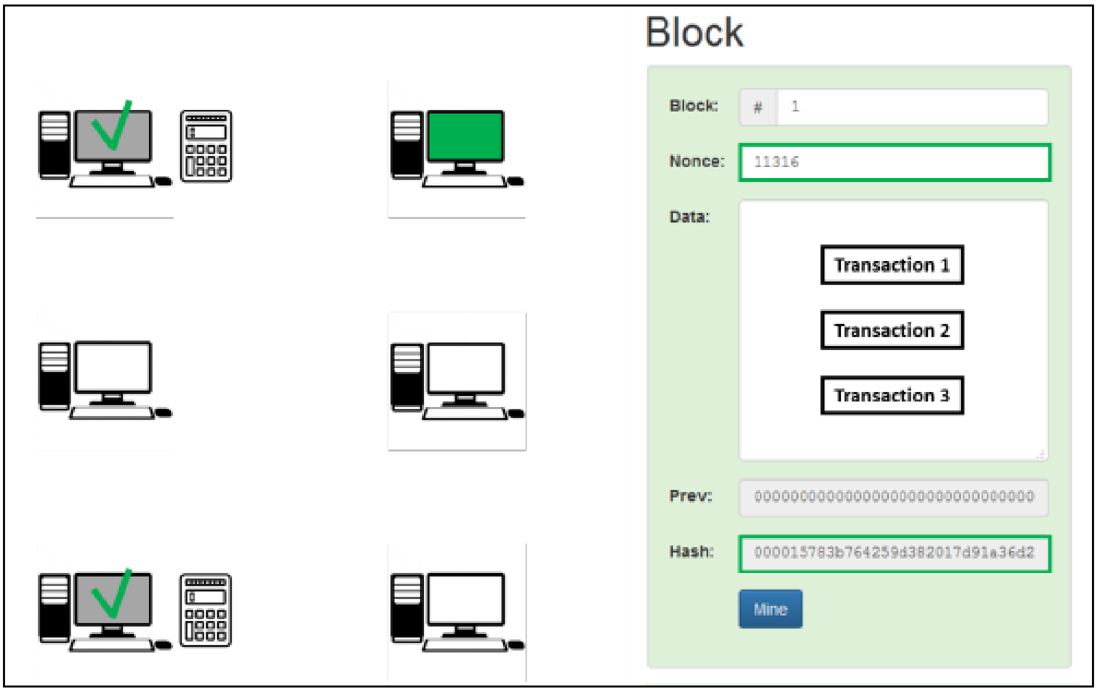
Data:

Prev: 00000000000000000000000000000000

Hash: 000015783b764259d382017d91a36d2

Figure 1.5. Computation of the hash and its transmission to other nodes for verification

Nodes that get this block verify that the transactions are accurate and that there isn't any "double spending" (Figure 1.6). The block is discarded if the verification is unsuccessful.



Block

Block: # 1

Nonce: 11316

Data:

Transaction 1

Transaction 2

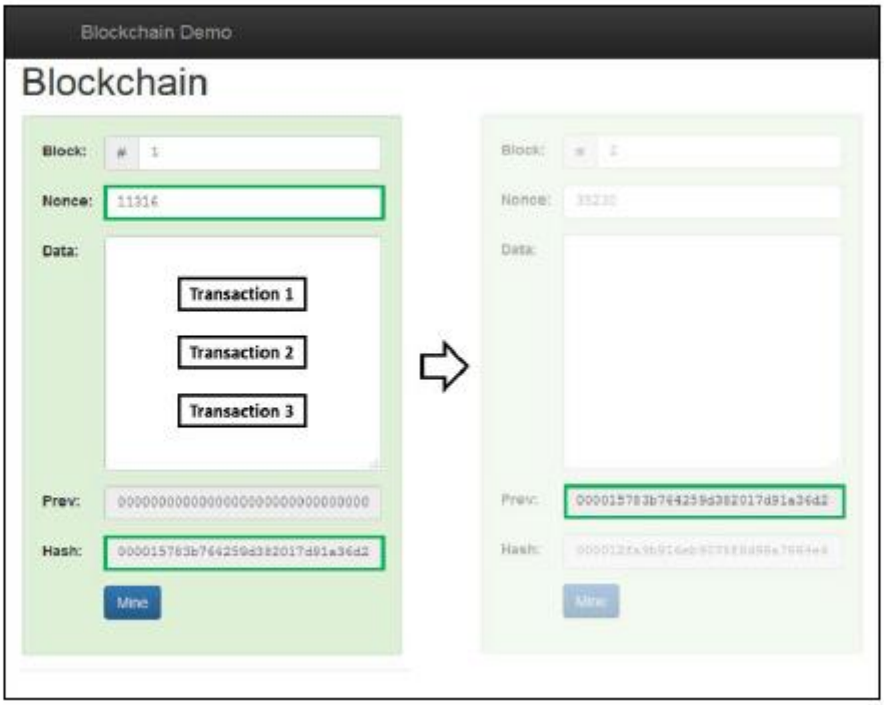
Transaction 3

Prev: 0000000000000000000000000000000

Hash: 000015783b764259d382017d91a36d2

Figure 1.6. Block Verification

6. If a consensus is reached on the correctness of the block, miners add it to the chain and begin working on a new block of data based on the hash of the recently added block (Figure 1.7).



Blockchain

Block: # 1

Nonce: 11316

Data:

Transaction 1

Transaction 2

Transaction 3

Prev: 0000000000000000000000000000000

Hash: 000015783b764259d382017d91a36d2

Block: # 2

Nonce: 35230

Data:

Prev: 000015783b764259d382017d91a36d2

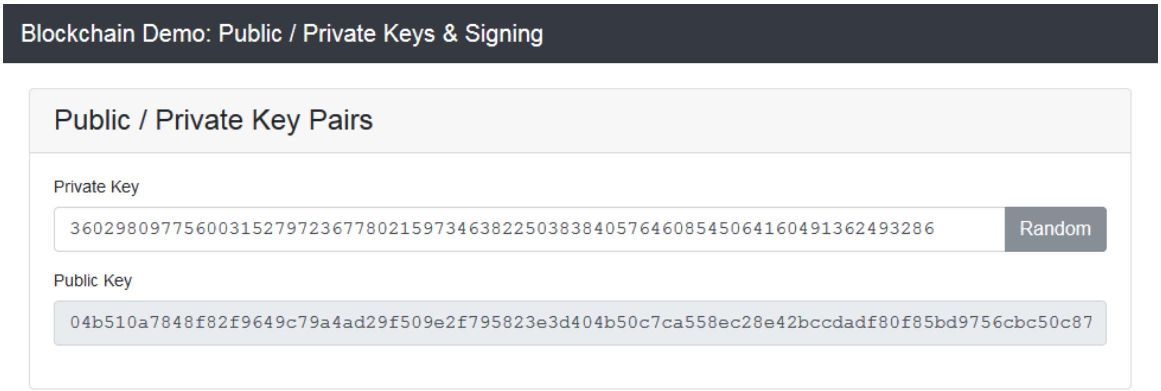
Hash: 000012fa9b916eb[illegible]

Figure 1.7. Adding a Block to the Chain

Since the hash of the previous block is one of the input data used to create the hash of the current block, any modification to any of the previous block's input data will affect the hash of the previous block as well as the hash of the block that comes after. As a result, the latter will no longer satisfy the given condition, making the entire chain that follows false. Moreover, it becomes harder to change a block in a chain the older it is.

Since anyone may fake a transaction by pretending to be someone else in the system and send all the funds to themselves, transaction information is not shared publicly. Sender and recipient details are converted into an unintelligible string of characters. This is how it takes place:

Every network user creates a random set of numbers (private key) after logging in and installing the required software on their computer. The public key, which is a more complicated set of characters, is subsequently created using this private key (Figure 1.8). The length of the public key makes it impossible to extract the private key without a large amount of processing power.


Blockchain Demo: Public / Private Keys & Signing

Public / Private Key Pairs

Private Key

3602980977560031527972367780215973463822503838405764608545064160491362493286

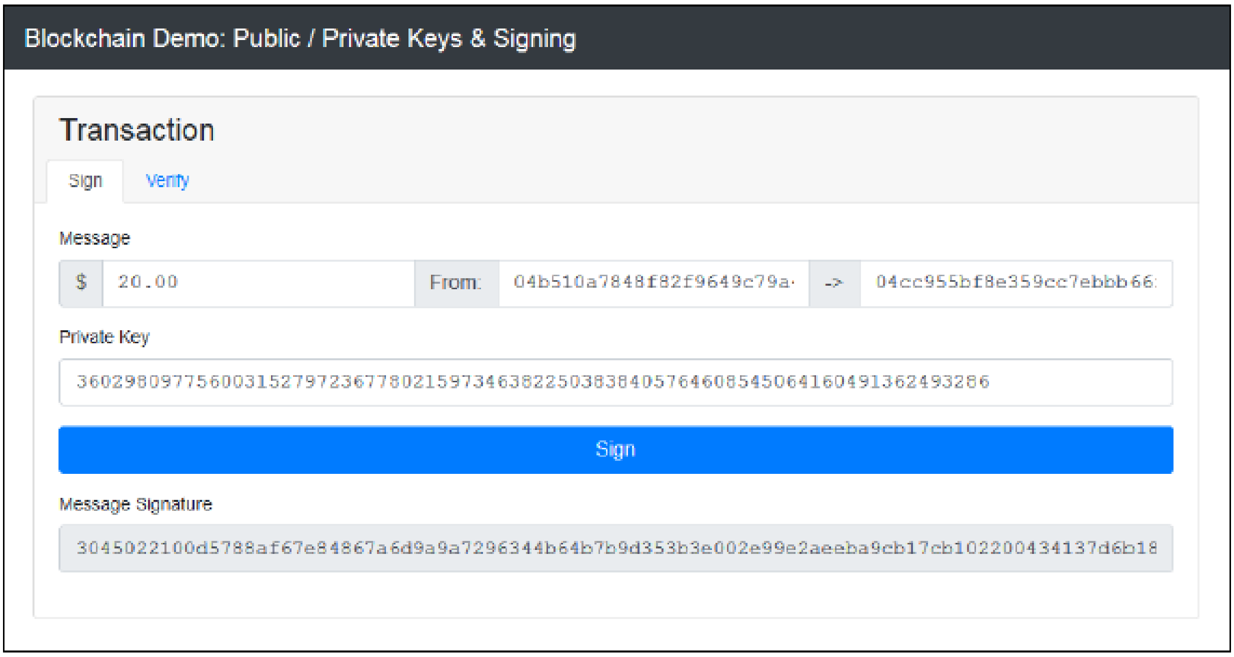
Public Key

04b510a7848f82f9649c79a4ad29f509e2f795823e3d404b50c7ca558ec28e42bccdadf80f85bd9756cbc50c87

Figure 1.8. Private and Public Keys

The person who generated the private key is the only one who owns it. It shouldn't be disclosed to anyone and doesn't take part in transactions. Although it is not communicated openly, it is used to sign transactions.

Every user sign in order to start a transaction. The public key of the wallet to which the funds to be transferred, together with the intended amount, should be entered in the recipient's data, and the sender's details should contain their public key representing their wallet (Figure 1.9).



Blockchain Demo: Public / Private Keys & Signing

Transaction

Message

$ 20.00 From: 04b510a7848f82f9649c79a -> 04cc955bf8e359cc7ebbb66

Private Key

3602980977560031527972367780215973463822503838405764608545064160491362493286

Message Signature

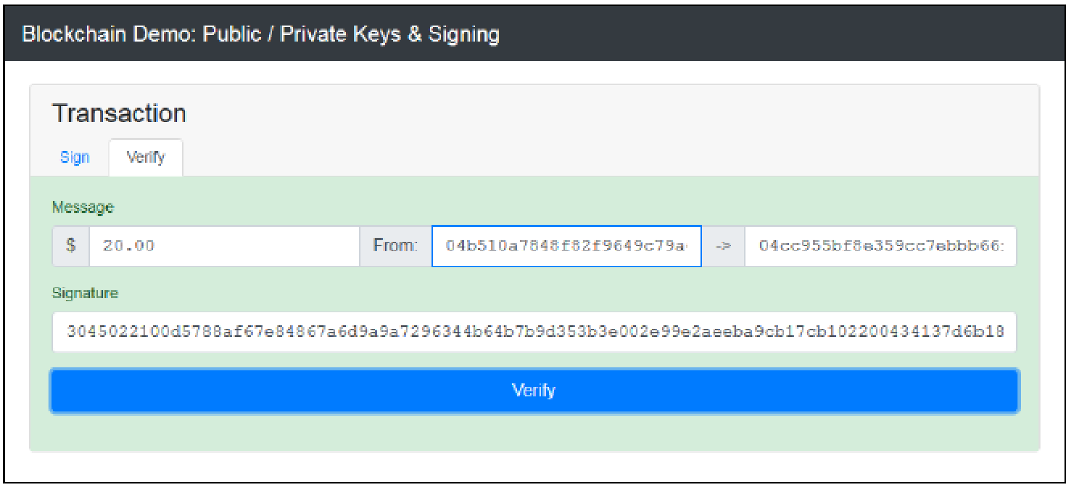
3045022100d5788af67e84867a6d9a9a7296344b64b7b9d353b3e002e99e2aeeba9cb17cb102200434137d6b18

Figure 1.9. Transaction Signature

A signature is created using this data and the private key, and it is subsequently distributed to other participants for confirmation before the transaction is included in a block.

Each user in the system can confirm that the transaction being attempted to be added to the block is signed by a user who has access to the actual private key when they have the signature and all the input data (Figure 1.10).

As a result, the blockchain only contains specific keys that represent wallets, which are hidden behind a variety of identities, and signatures for each transaction rather than personal information about people sending money to one another (Figure 1.11).



Blockchain Demo: Public / Private Keys & Signing

Transaction

Sign | Verify

Message

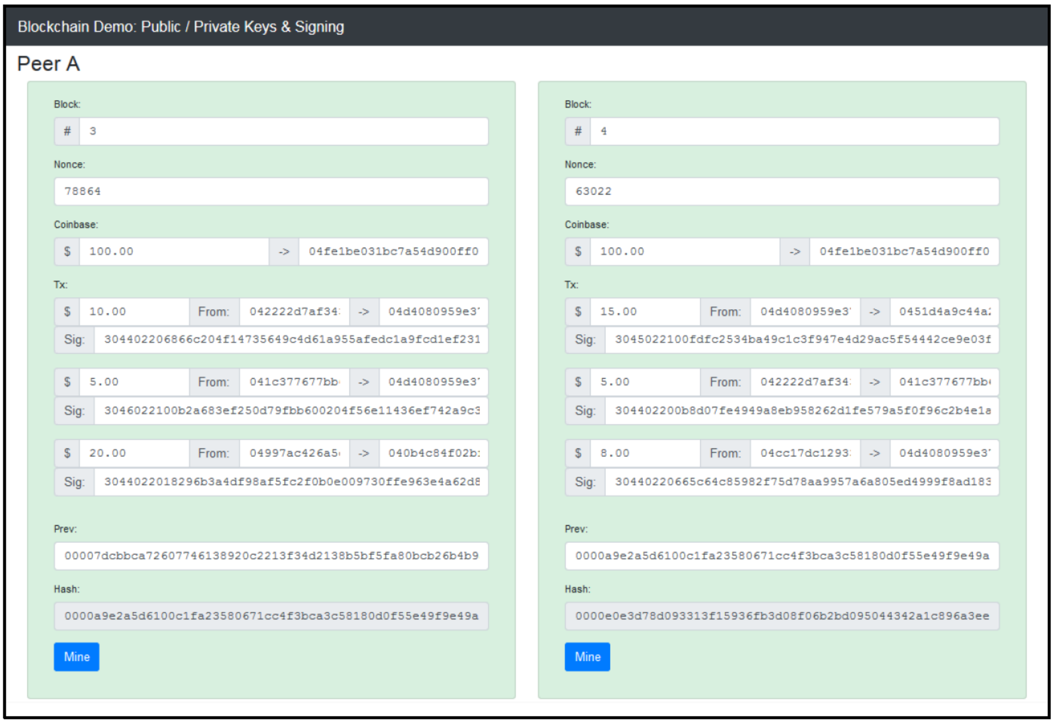
$ 20.00 From: 04b510a7848f82f9649c79a -> 04cc955bf8e359cc7ebbb66

Signature

3045022100d5788af67e84867a6d9a9a7296344b64b7b9d353b3e002e99e2aeeba9cb17cb102200434137d6b18

Verify

Figure 1.10. Transaction Signature Verification



Blockchain Demo: Public / Private Keys & Signing

Peer A

Block: # 3

Nonce: 78864

Coinbase: $ 100.00 -> 04fe1be031bc7a54d900ff0

Tx:

$ 10.00 From: 042222d7af34 -> 04d4080959e3
Sig: 304402206866c204f14735649c4d61a955afedc1a9fcd1ef231

$ 5.00 From: 041c377677bb -> 04d4080959e3
Sig: 3046022100b2a683ef250d79fbb600204f56e11436ef742a9c3

$ 20.00 From: 04997ac426a5 -> 040b4c84f02b
Sig: 304402201829６b3a4df98af5fc2f0b0e009730ffe963e4a62d8

Prev: 00007dcbbca72607746138920c2213f34d2138b5bf5fa80bcb26b4b9

Hash: 0000a9e2a5d6100c1fa23580671cc4f3bca3c58180d0f55e49f9e49a

Mine

Block: # 4

Nonce: 63022

Coinbase: $ 100.00 -> 04fe1be031bc7a54d900ff0

Tx:

$ 15.00 From: 04d4080959e3 -> 0451d4a9c44a
Sig: 3045022100fdfc2534ba49c1c3f947e4d29ac5f54442ce9e03f

$ 5.00 From: 042222d7af34 -> 041c377677bb
Sig: 304402200b8d07fe4949a8eb958262d1fe579a5f0f96c2b4e1a

$ 8.00 From: 04cc17dc1293 -> 04d4080959e3
Sig: 30440220665c64c85982f75d78aa9957a6a805ed4999f8ad183

Prev: 0000a9e2a5d6100c1fa23580671cc4f3bca3c58180d0f55e49f9e49a

Hash: 0000e0e3d78d093313f15936fb3d08f06b2bd095044342a1c896a3ee

Mine

Figure 1.11. Blockchain Scheme with Public Keys and Transaction Signatures

As previously stated, even the smallest alteration to the input data—be it the wallet number of the sender or receiver, the amount of money transferred, or the signature—will immediately cause the final hash to change, resulting in the chain being erroneous.

A hash function is used in this scheme to transform an array of data into a hash. For cryptocurrencies, it's transaction data; for more intricate systems, it contains details on smart contracts and the state at which code has been added to the blockchain. With the exception of hashing collisions, the transformation yields an almost unique alphanumeric string that describes the original element and is irreversible. The blockchain technology offers a high degree of data storage security since it combines hashing with the use of public and private keys.

Other users on the blockchain network will immediately reject any block that a miner tries to add that violates this regulation. The "genesis block" is the first block in the system, typically chosen by the system developers. A miner would have to alter the hash of every block before it in order to add an invalid block. One of the core characteristics of distributed ledger technology is the immutability of data contributed to the blockchain.

Rewriting a newly added block is possible because throughout the mining process, users gather together to form pools. But because it has to compete with the entire network's processing capacity, this is also a difficult challenge.

It is important to remember that miners add new blocks in accordance with certain guidelines. In order to maintain the decentralization of the blockchain and improve its security, these concepts were incorporated into the system. To add a new block to the blockchain, consensus is currently reached using two primary principles: Proof of Work (PoW) and Proof of Stake (PoS).

While there are more algorithms available for adding a new block, the ones mentioned above are the main and most widely applied ones. Each node in this system is unaware of which version of the database is valid at all times since blockchain security does not depend on a single certifying body, like a bank with its own security infrastructure. It's crucial to remember that the ledger is updated concurrently at predetermined intervals on every machine connected to the network.

During block mining on the Bitcoin blockchain, network security is dependent on the Proof of Work (PoW) algorithm. To ensure the legitimacy of the block, any node hoping to take part in the mining process needs to find a solution to a computationally challenging puzzle. New bitcoins are automatically credited to the miner as payment for solving it.

In the event of a blockchain database hack, the perpetrator would have to find a solution that works for the entire network. Stated differently, the success of the assault depends on the attacker's ability to gather a sizable amount of processing power.

The following resources are necessary for the Bitcoin protocol to function and keep network security:

- Hardware specifically designed for computational activities; - The electricity needed to run the apparatus.

Because of this, Bitcoin uses resources inefficiently. Bitcoin miners are forced to participate in a "arms race," utilizing ever-increasing amounts of resources for mining in order to increase their portion of rewards. This, on the one hand, makes it extremely expensive to attack Bitcoin. Conversely, due to Bitcoin's negative environmental impact, plans have been made to create comparable systems that use a lot less energy.

This issue was resolved via a technique built on the Proof-of-Stake (PoS) algorithm. The idea behind Proof-of-Stake is that a user's stake in the system determines the probability of them creating a new block and earning the associated reward, rather than processing capacity.

The Proof-of-Stake algorithm's consistency makes sense for the following reasons: Since they would lose the most if attacks caused the cryptocurrency's value and reputation to plummet, people with the biggest stakes in the system have the most incentive to keep the network secure. A hostile actor would have to purchase a sizable amount of the currency in order to carry out a successful attack, which would be unaffordable if the system is extensively used.

Because the database is distributed, it is nearly impossible for bad actors to hack it because they would need to simultaneously access copies of the database on a large number of networked computers. Since no single center is vulnerable to service denial, denial-of-service (DoS) attacks also lose their significance.

Additionally, the blockchain allows for the implementation of algorithmic improvements and modifications, so long as they are approved by the majority of system users.

Thus, distributed ledger technology possesses the following characteristics:

- Decentralization;
- Openness of entered data;
- Mathematical-cryptographic protection of information;
- Immutability of data once entered into the system.

Various sources often emphasize the following features:

- Transparency – access to the entire history of events, including monetary transfers, agreements, and other records, is always open to all participants in the system;
- Decentralization – the transaction history is stored on the hard drive of each participant, not on a central server;
- Anonymity – there is no need to disclose one's identity to operate in the blockchain;
- Equality – there are no administrators or information custodians in the blockchain, and all participants have equal status and capabilities;
- Security – the information recorded in the blockchain cannot be forged or substituted, ensuring its authenticity.

The amount of cyber fraud and external political, economic, and other issues, together with the activities of monetary regulatory bodies, emission constraints, brand distinctiveness and recognition, popularity, and the proliferation of use cases, are all major aspects that influence consumer trust in cryptocurrencies.

The advantages of cryptocurrencies, according to O. A. Nikolaychuk, also include transparency, dependability, and the difficulty of counterfeiting. Crucially, reliability is attained by giving each client the opportunity to confirm the accuracy of a transaction rather than by limiting access and keeping information hidden from other market players.

In addition, the merits of cryptocurrencies can be attributed to the advantages inherent in the development of non-cash payments in general, such as:

- Absence of accumulations outside the banking sector and attraction of investments into the economy;
- Reduction of society's costs for processing and storing banknotes, coins, and cash collection;
- Increased transparency and security of payments for all stakeholders in this market;
- Achievement of a certain tax collectability.

In reference to the anonymity that is frequently questioned in cryptocurrency, the following remark from the Organization for Economic Cooperation and Development (OECD) assessment is relevant: "The system's clear anonymity is a reason why bitcoin is defined as a tool for fraudulent transactions. Actually, when it comes to payment methods, cash is even more anonymous than virtual currencies. Law enforcement has a strong tool that allows them to track every chain of value transfer once the name and address (owner) are determined, something that currency would never permit. The case against cryptocurrencies' anonymity is far weaker than the one against cash."

The OECD also points out that, in contrast to national currency, cryptocurrency is not supported by the national government's complete recognition and trust and is not subject to its laws that limit certain acts (such as the abrupt hyperemission of that currency). Buyers will, nevertheless, be prepared to pay for it because they believe that other users will recognize the same cryptocurrency as a store of value.

Another risk, according to the OECD, is that certain governments would try to take action that would effectively forbid the use of virtual currency as money in and of itself. This suggests that cryptocurrencies might be ruled unlawful. The research from the OECD states that "even though virtual currency is not declared illegal, simply the discussion of this possibility damages mutual trust in the future buying power of virtual currency, which is necessary for both parties of the transaction to consider it a store of value."

1.1.1. Definition and Key Properties

Blockchain technologies are essential to innovative developments in education that include technological and technical advancements, the evolution of the educational process, and the actualization of features of innovative educational models that make use of contemporary information and communication technologies.

Blockchain is a decentralized network, also known as a peer-to-peer network made up of individual users called nodes, that is an immutable public distributed ledger that facilitates transactions without the need for a single central middleman. To be more precise, it is a series of blocks that are connected in a sequential manner and hold either open or encrypted data. Each block in the chain carries not only its own data, but also its hash and the hash of the previous block. Proposed in 2008 and launched in 2009, the cryptocurrency Bitcoin is the most well-known application of blockchain technology. The system was developed as an answer to the current financial system, which is dominated by a few giant banks that control the issuing of accounts and the processing of transactions. In reference to this, Bitcoin's founder, Satoshi Nakamoto, said: "Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve."

To offer a more thorough comprehension, multiple further explanations of this technology can be illustrated:

1. A peer-to-peer network with a decentralized register of all transactions that allows users to verify transactions without the need for a certification center.

2. A system that combines data analytic techniques that offer flexibility and scalability with technology that guarantees safe and reliable administration of dispersed data (Wilson, 2017).

3. A dispersed digital ledger that group blocks of cryptographically signed transactions. Following consensus verification and decision-making, each block is cryptographically connected to the one before it (see more in the "Block" and "Consensus" sections). Older blocks become harder to change when new ones are added. All network

copies of the ledger duplicate new blocks, and any discrepancies are automatically settled by applying predefined criteria.

Thus, blockchain technology is built on the principles of decentralized network architecture and utilizes a distributed data ledger governed by the established rules of the chosen consensus algorithm. Based on this, blockchain possesses the following properties:

1. *Decentralization*.

In a decentralized network, there is no need for a third controlling party due to the equal status of each participant and the operation of the consensus algorithm. Decentralization leads to complete consistency in the conducted operations (see further in the "Consensus" subsection).

2. *Immutability*.

Blockchain is envisioned as an immutable data ledger due to the architectural features (see further in the "Structure" subsection). Each participant's action (e.g., a transaction) is recorded in the ledger forever and is not subject to modification.

3. *Anonymity*.

Each participant is assigned an address used in the identity verification process. It is worth noting that blockchain cannot guarantee perfect confidentiality due to certain internal limitations (see further in "Issues and Solutions").

4. *Verifiability*.

The consensus algorithm (see further in the "Consensus" subsection) allows for an independent audit of the entire blockchain periodically and/or depending on specific conditions.

1.1.2. Structure and Classification

The blockchain infrastructure with its constituent structural elements is illustrated in Figure 1.12.

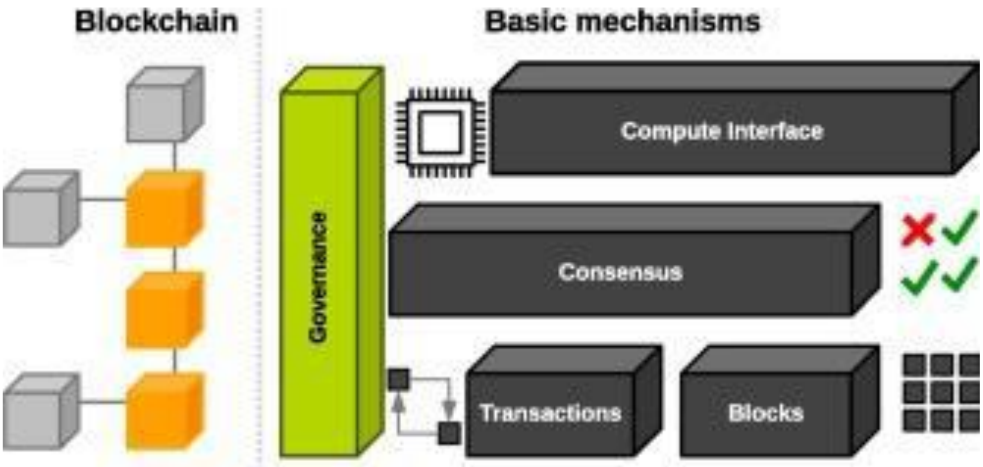
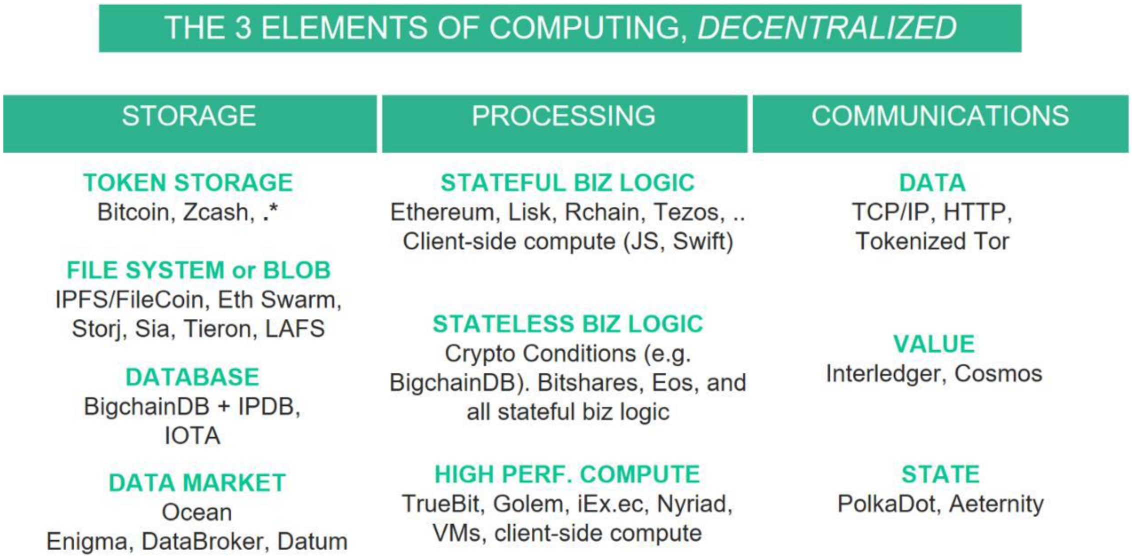


Figure 1.12. Blockchain Infrastructure

The elements of the corresponding decentralized system are presented in Figure 1.13:



THE 3 ELEMENTS OF COMPUTING, *DECENTRALIZED*

STORAGE	PROCESSING	COMMUNICATIONS
TOKEN STORAGE Bitcoin, Zcash, .*	**STATEFUL BIZ LOGIC** Ethereum, Lisk, Rchain, Tezos, .. Client-side compute (JS, Swift)	**DATA** TCP/IP, HTTP, Tokenized Tor
FILE SYSTEM or BLOB IPFS/FileCoin, Eth Swarm, Storj, Sia, Tieron, LAFS		
DATABASE BigchainDB + IPDB, IOTA	**STATELESS BIZ LOGIC** Crypto Conditions (e.g. BigchainDB). Bitshares, Eos, and all stateful biz logic	**VALUE** Interledger, Cosmos
DATA MARKET Ocean Enigma, DataBroker, Datum	**HIGH PERF. COMPUTE** TrueBit, Golem, iEx.ec, Nyriad, VMs, client-side compute	**STATE** PolkaDot, Aeternity

Figure 1.13. Elements of the decentralized system

The primary building element of the blockchain is the block, which functions as a container for both transactions (see below) or other kinds of data (depending on how it is implemented). The hash sum of the data in each block, which is derived using one of the hashing algorithms—SHA1, SHA256, or Quark—connects it to the previous block. A description of the items from the Block Header is given in (Table 1.1), and the internal structure of the block is depicted in (Figure 1.14) below.

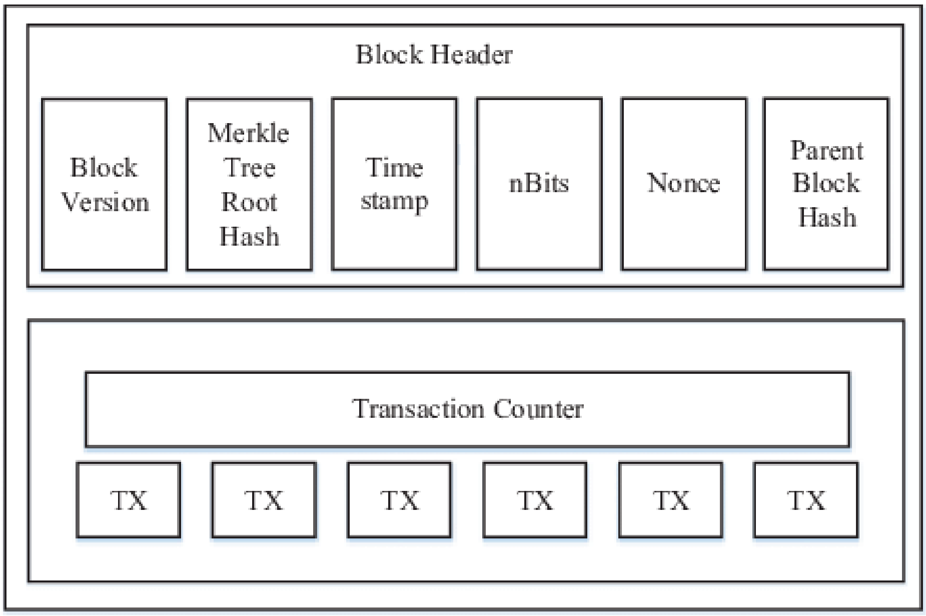
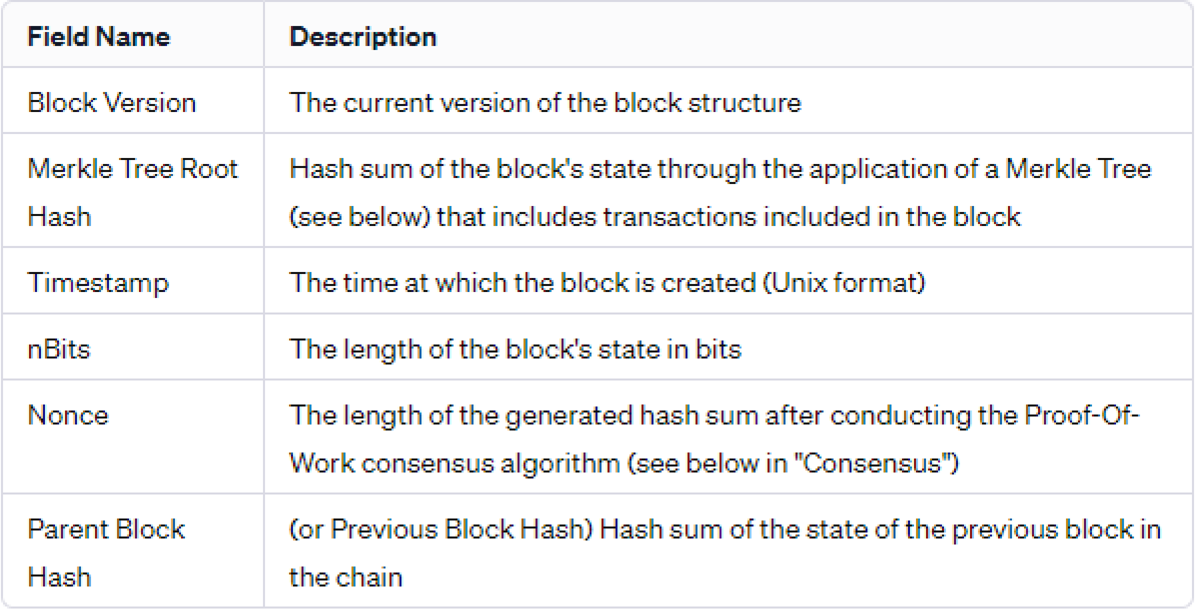


Figure 1.14. Internal Structure of a Block Schema

Table 1.1

Values of Block Elements in Block Header



Field Name	Description
Block Version	The current version of the block structure
Merkle Tree Root Hash	Hash sum of the block's state through the application of a Merkle Tree (see below) that includes transactions included in the block
Timestamp	The time at which the block is created (Unix format)
nBits	The length of the block's state in bits
Nonce	The length of the generated hash sum after conducting the Proof-Of-Work consensus algorithm (see below in "Consensus")
Parent Block Hash	(or Previous Block Hash) Hash sum of the state of the previous block in the chain

At this point, the following technologies are being used:

1. Hash Function for Block State: The hash function is used to link blocks together in a chain, ensuring immutability. In this instance, the content of the block is further verified as valid by applying the hash function to produce a 256-bit string (when employing SHA256).

2. Merkle Tree: Using a set quantity of input data (transactions, for example), this technique builds a hash tree. As the hash sum of the current block, the algorithm in blockchain is frequently used to verify the veracity of the block's content.

An account of the transfer of material or immaterial assets between parties involved is called a transaction. It may also be understood as a component when considering account verification. Certain fields must be present in every transaction that wants to be included in a block (depending on the blockchain technology and version of its transaction structure).

An electronic signature is used in transactions when information is sent and received to verify identity. An encrypted string of any length can be represented by an electronic signature in the context of blockchain technologies, which is created using public and private keys (ECDSA or RSA). The following figure (Figure 1.15) shows the operation of the principle:

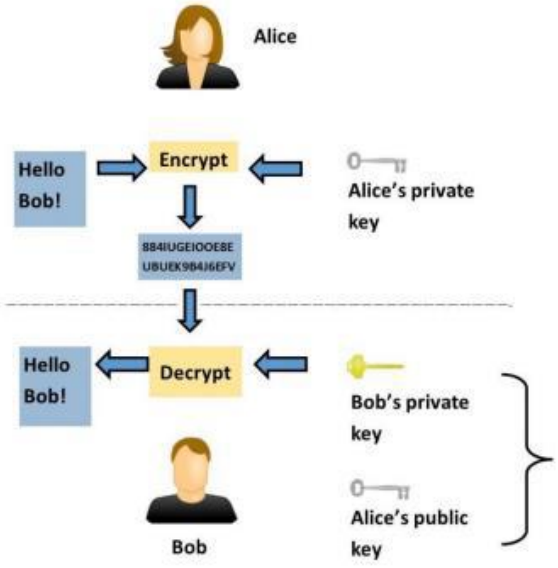


Figure 1.15. Operating Principle of Electronic Signature in Blockchain

Alice, the initial user, transfers pre-encrypted data to Bob, the second user. Using Alice's private key, an electronic signature is created prior to transmission. Bob uses Alice's public key and his private key to decode the data that was received. As a result, Bob confirms the legitimacy of the information received and the validity of Alice's signature.

Because there is no central verification center, the entire blockchain is based on a decentralized network, which facilitates more effective resource allocation. The distributed hash table, or DHT, allows the decentralized network to be used for routing and maintenance of a list of known nodes. The construction of such a network is shown (in slightly simplified form) in (Figure 1.16).

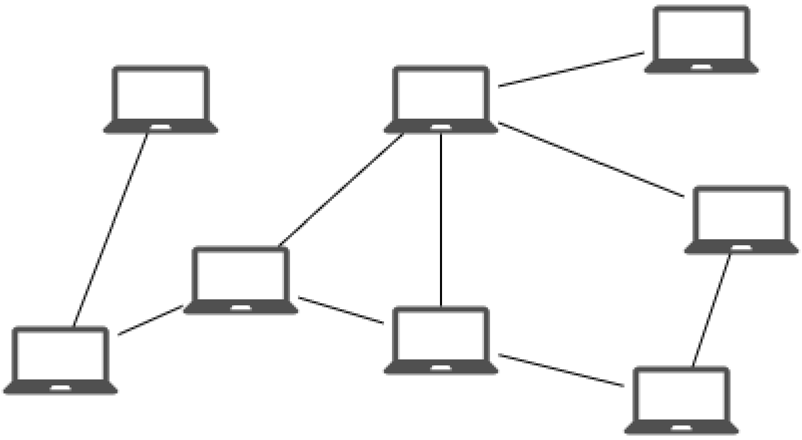


Figure 1.16. Decentralized Network Scheme

Every device that is connected is called a node. The network consists of many identical nodes linked together by a communication protocol, usually TCP/IP-based GRPC or something similar.

Blockchain technologies are typically categorized as public, private, or hybrid (consortium) depending on how private they are. Every record in a public blockchain is available to the whole world, enabling anybody to take part in the process of auditing and adding new blocks. Regarding a private blockchain, the consensus procedure can only be used by nodes that are members of a particular organization (more on this in the "Consensus" article). Because private blockchains are entirely managed by a single entity and only a tiny percentage of nodes are chosen to reach consensus, they are seen as centralized networks. Both public and private properties are incorporated into a hybrid blockchain (consortium). A comparison is conducted encompassing the subsequent aspects:

1. Determining the level of action and information accessibility.

2. Examining authorization. A private blockchain prevents the public from seeing transactions.

3. Unchangeability. Forging transactions in a public blockchain is nearly hard because records are shared among numerous participants. On the other hand, because there are fewer users in a private blockchain, transactions there are more readily falsified.

4. Effectiveness. With so many nodes in a public blockchain, it takes a long time for transactions and blocks to be distributed. This leads to a high latency and a limited amount of blocks issued per unit of time.

5. Centralization level. A public blockchain is decentralized, a hybrid blockchain is partially centralized, and a private blockchain is totally centralized. These are the main distinctions between the three categories of blockchains.

Furthermore, a classification for the financial and non-financial industries based on the orientation of blockchain applications (dApps; see below in the "Smart Contract" part) can be given. Applications for financial blockchain include cryptocurrency exchange Ripple and Bitcoin. Ethereum, a cryptocurrency with sophisticated smart contract capabilities, and Hyperledger, a group of developers building blockchain technologies for enterprise, are examples of non-financial applications.

Blockchain's four main features—decentralization, immutability, anonymity, and verifiability—have shown that they have the ability to completely change conventional businesses. Different consensus algorithms have been developed as a result of the necessity for blockchain users to come to a consensus. An overview of common consensus algorithms in blockchain technology is provided below:

1. The Proof-of-Work (PoW) strategy is used in the Bitcoin network. It involves using a straightforward technique to choose a user, also known as a miner, at random to create and audit new blocks in a decentralized network. The chosen person has to put in a lot of effort (using computing resources to generate the block's hash) because random selection is susceptible to attacks.

2. Proof-of-Stake (PoS) is a PoW substitute that uses less energy. In PoS, miners have to earn the privilege of creating and auditing blocks according to the funds balance. It is thought that those who own more money will be less likely to launch network attacks. Because this method uses no energy, it is more efficient than the prior one. Delegated Proof-

Of-Stake (DPoS) is an enhanced variant that involves voting to choose a miner from a suggested list.

3. The Byzantine Generals' Problem can be solved using the Practical Byzantine Fault Tolerance (PBFT) method, which can withstand up to one-third of malicious attacks. Every round determines a new block, and each round selects a main based on predetermined guidelines. Three stages comprise the complete process: preliminary planning, preparatory work, and finalization. A node is guaranteed to be selected as a trustworthy leader in charge of building the block and auditing data because it proceeds to the next phase if it receives votes from more than two thirds of all nodes in each phase.

1.1.2.1 Smart Contract

A smart contract is a program, typically written in a programming language (most commonly Solidity), designed to execute specific logic within a blockchain. Ethereum was the pioneering platform that introduced smart contracts.

The fundamental operation of a smart contract in the Ethereum blockchain is illustrated in Figure 1.17 below:

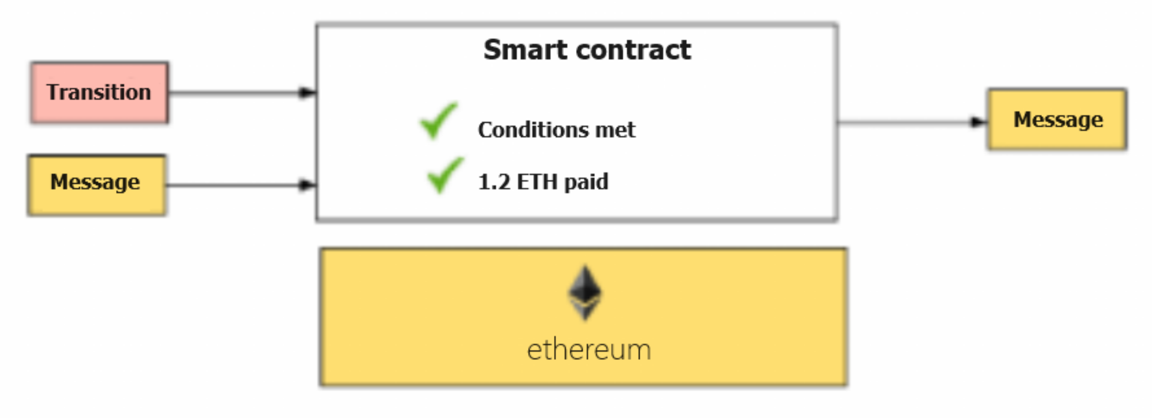


Figure 1.17. Basic Operation Scheme of a Smart Contract in the Ethereum Blockchain

A transaction and a message containing particular data are needed for a smart contract to function. When specific requirements outlined in the smart contract's logic are satisfied, the end user interacting with the contract will receive these data. On different blockchain systems, a smart contract's implementation could be different from the one described above.

Smart contracts have the potential to become DApps, or decentralized applications, by providing the framework for more intricate logic. These apps have the same benefits as the blockchain itself and allow for the transparent and safe handling of user data. The idea of tokens is also introduced in DApps. In contrast to currency, a token is an extra electronic asset that is utilized for application functions (voting, rewards, etc.). It is marked, meaning that a particular token is linked to a particular application.

1.1.3. Issues and Solutions

Despite the significant potential of blockchain technology, it faces numerous challenges that limit its widespread use:

1. Scalability – as the number of transactions increases, blockchain becomes cumbersome because each node must store the entire transaction history. Moreover, due to the initial block size limit and the time interval used to generate a new block, Bitcoin can only process about 7 transactions per second, falling short of the requirement for processing millions of transactions in real-time. The following are some ways to address this issue:

a) Blockchain storage optimization – a new scheme called VerSum allows clients with significant weight to outsource computationally expensive tasks with large input data. It ensures the correctness of computation results by comparing results from multiple servers.

b) Redesign (refactoring of structure and architecture) – bitcoin-NG cryptocurrency suggests splitting a regular block into two parts: a key block for selecting a leader and a microblock for storing transactions. Once the key block is generated, the node becomes the leader responsible for generating microblocks. Thus, a compromise between block size and network security would hypothetically be eliminated.

2. Confidential Data Leakage – Blockchain can preserve a certain level of privacy using public and private keys. However, it cannot guarantee transaction confidentiality, as the values of all transactions and balances for each public key are publicly accessible. To

enhance blockchain anonymity, several methods have been proposed by various blockchain projects, which can be broadly categorized into two types:

a) Mixing. Although user addresses on blockchain are pseudonymous, a user's real identity can still be inferred from them because numerous users regularly utilize the same address for transactions. A mixing service is a type of service that transfers money across several input and output addresses while maintaining anonymity. Then, anyone could confirm that the middleman was dishonest if they failed to send the funds.

b) Anonymity. Zerocoin relies on evidence of zero knowledge. Miners should avoid using digital signatures to validate transactions and should avoid linking payment sources to specific transactions in order to prevent transaction content analysis.

1.2 Overview of the Internet of Things

1.2.1 Typical Characteristics of IoT Systems

It is important to specify the kinds of requirements placed on such items because a key component of the testing process in this job is the computation of specific indicators for a system.

Software requirements can be categorized, systematized in a variety of ways, and metrics that assess compliance with these requirements can be applied in a variety of ways. The six categories of metrics for assessing software product behavior are functionality, dependability, usability, efficiency, maintainability, and portability, according to the ISO/IEC TR 9126—2:2003 standard. In order to compute these metrics, the system must be operated in real-world circumstances. While any software can be tested using any of these metrics, certain categories are more pertinent than others in particular fields, like the Internet of Things.

In the testing process, functional testing frequently comes first. Requirements are categorized as either functional or non-functional, or as everything else. At its core, functionality is the system's ability to provide outcomes that meet user expectations. This category also includes indicators of system security and external compatibility. Therefore, many of the essential criteria for system evaluation are included in the idea of functioning itself.

The most important needs are those that are functional, especially when it comes to the Internet of Things. IoT systems are used to automate and optimize an array of tasks, usually in highly responsible sectors where following instructions to the letter is crucial due to the potentially dire implications of making a mistake. As a result, it's essential to make sure that the system behaves as error-free as feasible. An effective attack on a "smart home," for instance, can possibly take control of vital life-quality systems like lighting or heating. External interference can also be an issue. Furthermore, private information frequently flows through IoT systems, allowing for the sensitive deduction of user characteristics.

Reliability and efficiency criteria stand out as being especially crucial among non-functional requirements. Even while most Internet of Things (IoT) systems don't need to make decisions in real time, they nonetheless need to react to events quickly because a mistake could have disastrous results. Reliability measurements include things like maturity, fault tolerance, and recovery capabilities, while efficiency measures include things like resource load and system reaction time. The fact that most IoT devices have limited resources is another justification for adopting efficiency standards.

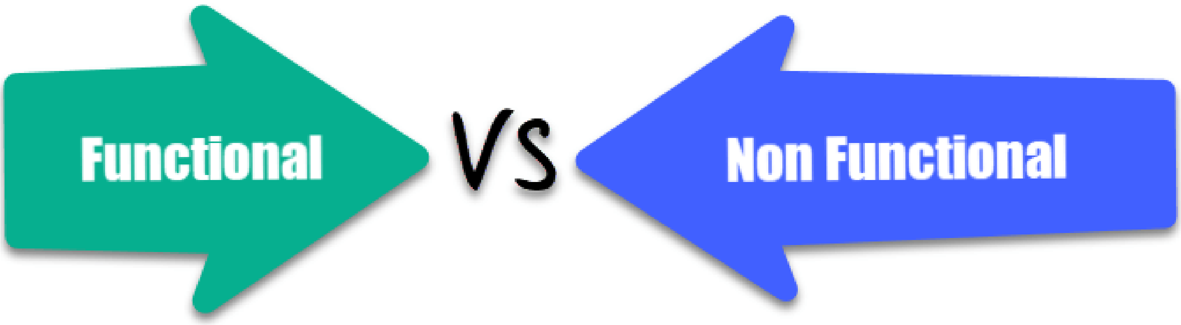


Figure 1.18. Functional and non-functional requirements for IoT

Additional categories of criteria, including usability, maintainability, and portability, might also be relevant to Internet of Things (IoT) systems; however, the ability to automate the computation of these indicators is considerably diminished. Important in the IoT industry, usability, for instance, refers to the simplicity of comprehending, learning, and managing the operation of the system; however, real-user testing is necessary to evaluate these indicators.

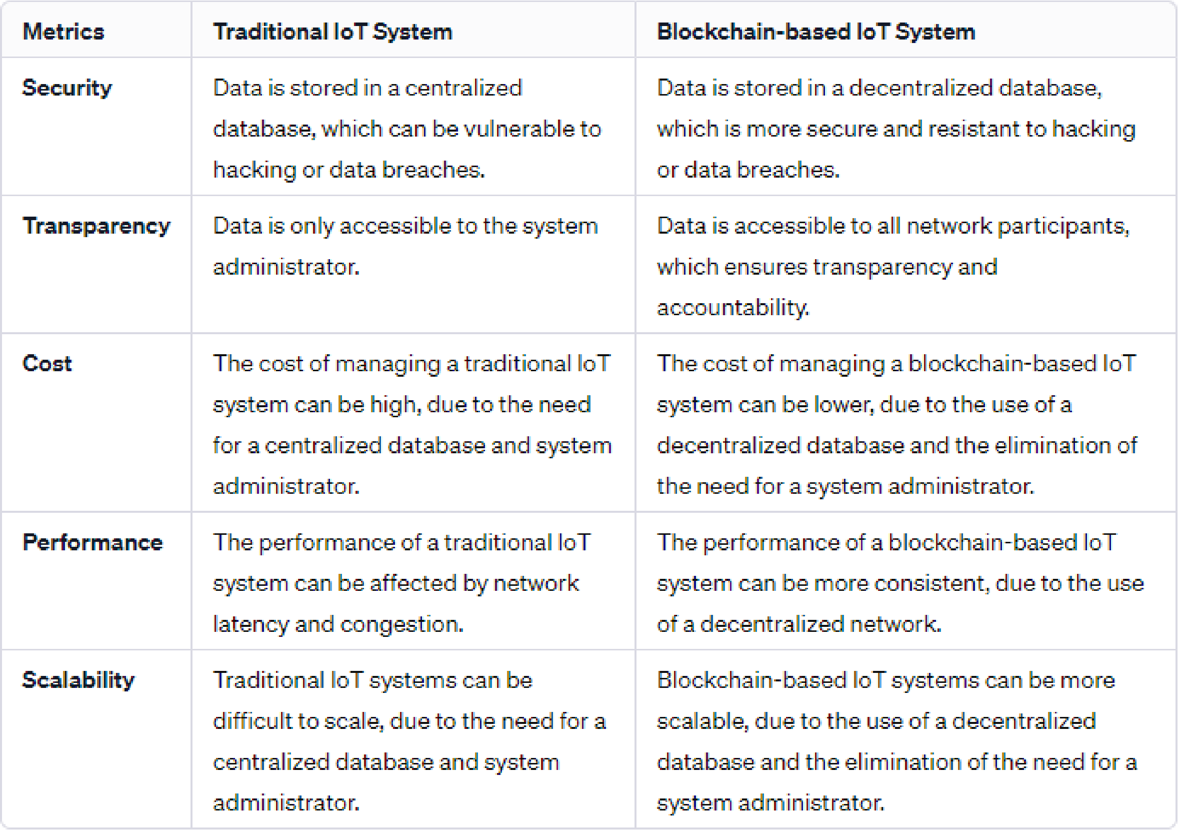
In conclusion, the majority of the described requirements are broad categories; it is necessary to specify the chosen metrics for a particular system or domain. An illustration of this type of analysis will be expounded upon in the subsequent chapters.

1.2.2 Comparison of Traditional and Blockchain-Oriented IoT Systems

The following table shows the performance indicators of traditional systems and those using Blockchain

Table 2.1

Performance indicators of traditional systems and using Blockchain



Metrics	**Traditional IoT System**	**Blockchain-based IoT System**
Security	Data is stored in a centralized database, which can be vulnerable to hacking or data breaches.	Data is stored in a decentralized database, which is more secure and resistant to hacking or data breaches.
Transparency	Data is only accessible to the system administrator.	Data is accessible to all network participants, which ensures transparency and accountability.
Cost	The cost of managing a traditional IoT system can be high, due to the need for a centralized database and system administrator.	The cost of managing a blockchain-based IoT system can be lower, due to the use of a decentralized database and the elimination of the need for a system administrator.
Performance	The performance of a traditional IoT system can be affected by network latency and congestion.	The performance of a blockchain-based IoT system can be more consistent, due to the use of a decentralized network.
Scalability	Traditional IoT systems can be difficult to scale, due to the need for a centralized database and system administrator.	Blockchain-based IoT systems can be more scalable, due to the use of a decentralized database and the elimination of the need for a system administrator.

The implementation of Blockchain technology in Internet of Things (IoT) systems presents benefits that transcend mere comparative metrics. By enabling the use of smart contracts to automate agreements and interactions between IoT devices, blockchain technology has the potential to increase the transparency and efficacy of the system. Moreover, in systems where dependability is of the utmost importance, the decentralized properties of Blockchain bolster resistance to failures.

1.3. Big Data

Achievable data volumes have become comprehensible to humanity in the current era, facilitated by the development of efficient data processing techniques (e.g., neural networks, data science, and machine learning). The potential of big data is substantial, as it can offer solutions to numerous inquiries across various domains such as business, economics, medicine, and more. The business sector, in particular, is notable for the way in which Google, Amazon, and Facebook analyze qualitative user data by analyzing vast quantities of data that travel through their systems.

The term "big data" is subject to various interpretations. Big data is defined by IT specialists as exceedingly large datasets that necessitate substantial processing, storage, and analysis capabilities. Preceding processing, big data frequently comprises a substantial quantity of redundant and corrupted information. Although the present implementation of big data presents a multitude of benefits, it is not devoid of obstacles; the primary concerns encompass the following:

The amount of data produced by the global population is escalating on a daily basis, necessitating enhanced processing and analysis capabilities.

2. The generation of data occurs via diverse channels and in numerous formats, thereby demanding the development of more sophisticated instruments.

3. The accumulation of data from diverse sources can occur at a rate analogous to that of its generation.

4. As a result of the automated nature of data collection, gathered information might contain outliers and false information; the situation is exacerbated when multiple sources are utilized.

The utilization of big data in conjunction with machine learning is akin to employing software to process and analyze data. In this domain, libraries such as MapReduce and Apache Hadoop (HDFS) are utilized as instruments to facilitate the distributed computation of massive datasets in real time. Forecasting, dimensionality reduction, and clustering are frequently implemented algorithms.

Examples of feasible implementations of machine learning encompass:

1) Assessing the correlation between particulars of offenses committed and social attributes.

2) Utilizing unsupervised techniques to aggregate clusters of consumers belonging to a particular product within a retail network.

3) Predicting meteorological conditions in various regions by employing supervised methods in accordance with predetermined criteria.

Memory management is the root cause of the majority of issues associated with the processing and analysis of big data using machine learning (as previously stated in the section describing the primary challenges of utilizing big data).

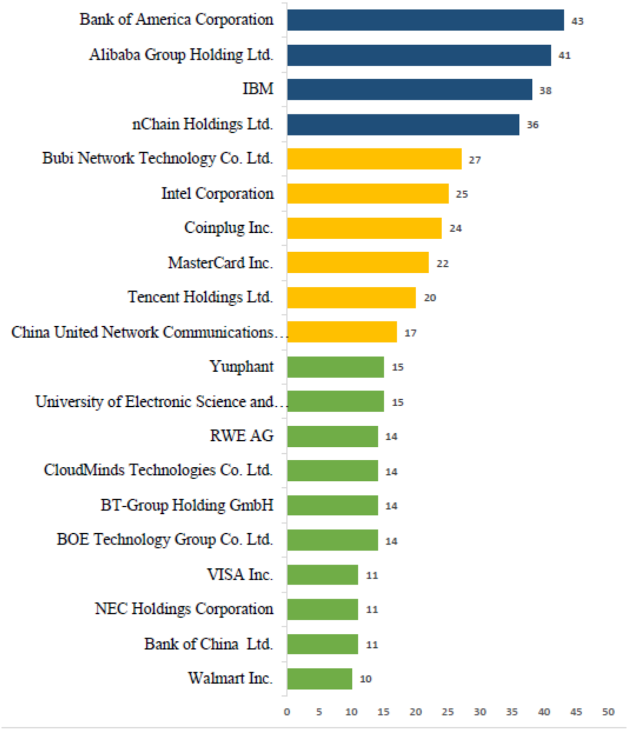


Figure 1.19. Number of patent families from leading companies in patenting blockchain technology

Certainly, the analysis of big data within the education sector is intriguing. The operations of academic institutions inevitably generate vast quantities of data, including student information, scientific publications, and more. The utilization of big data processing and analysis in the field of education yields expeditious outcomes when it comes to assessing student performance, forecasting forthcoming student requirements with precision, enabling timely modifications to the instructional process, and facilitating more efficacious comparative analyses of the labor market and the education industry at large. The advantages are self-evident and originate from the outcomes: enhanced scholastic achievement, accurate allocation among academic programs, and streamlined administration.

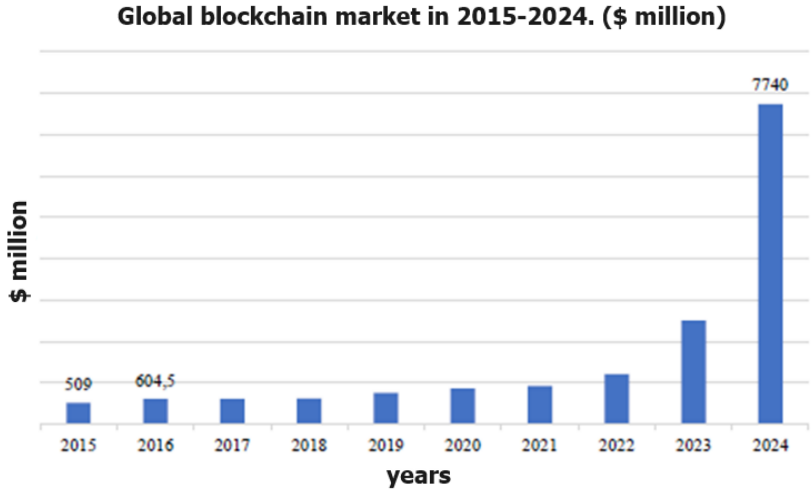


Figure 1.20. Expected dynamics of development of the global market for distributed registry technology

CONCLUSIONS FOR CHAPTER 1

A thorough examination of fundamental principles pertaining to Blockchain technology and the Internet of Things (IoT) was undertaken in this particular segment. An examination was conducted on the definition and fundamental characteristics of Blockchain, including its classification and structure, with particular emphasis on the function of smart contracts within this framework. In addition, a comprehensive examination of Internet of

Things systems was presented, contrasting conventional methodologies with those focused on Blockchain.

The understanding gained regarding Blockchain technology and the attributes of Internet of Things (IoT) systems forms the basis for subsequent investigations in the domains of information security, enhancement of operational efficiency, and the augmentation of functionalities in contemporary information systems. Drawing from the knowledge acquired in this segment, crucial elements have been identified that warrant additional investigation in the qualification process, with the ultimate goal of improving and advancing Internet of Things systems via the incorporation of Blockchain technology.

CHAPTER 2
ANALYSIS OF PRINCIPLES OF CONSTRUCTION AND ENHANCEMENT OF OPERATIONAL QUALITY

2.1 General characteristics of the Internet of Things

The reduced size and cost reduction of electronic components brought about by the advancement of microelectronics have enabled the incorporation of computer processors into a wide range of objects and the implementation of a multitude of miniature sensors. The ability of these devices to communicate with one another in order to exchange commands and data through a network has led to the conception of the Internet of Things (IoT).

Every individual object has the potential to provide a specific degree of automation. For instance, a motion sensor could activate the lighting in a room. Conversely, within the IoT, objects are incorporated into a system capable of concurrently considering a greater number of factors. A broad array of information is readily accessible as a result of this configuration, facilitating analysis and decision-making. By enabling the automation and optimization of processes, the Internet of Things relieves users of a substantial burden and obligation, particularly in domains that necessitate continuous monitoring. The majority of the time, IoT systems are intended to monitor daily processes or provide auxiliary support.

Proposed is a data flow processing paradigm for describing the operation of IoT systems. The system's workflow is predicated on its response to inbound events. It is important to note, however, that not all sensors operate in accordance with this model; control devices may receive observed data at predetermined intervals. As a result, the system processes the input data incrementally and determines when to issue commands to the controlled devices. Furthermore, it is frequently necessary to retain the acquired data for subsequent analysis.

Distinguishing themselves from the conceptualization of data transfers, IoT systems generally function within a heterogeneous setting where devices, which consist of manipulators and sensors, are mobile and diverse entities. With regard to software and hardware components, every device may exhibit variations in functionality and the resources at its disposal. The Internet of Things is dependent on a computing and communication infrastructure for communication. Thus, it is critical to ensure that both data processing and communication between components of the distributed system in question are accurate.

It is pertinent to examine the proper operation and adherence to predetermined criteria of the aforementioned communication and computational system, in light of the aforementioned attributes. When feasible, the technical facets of implementation, including the selection of particular devices or interaction protocols, can be segregated so that attention can be directed towards guaranteeing the accurate operation of the software component. Furthermore, this responsibility entails assessing the appropriateness of a specific methodology that emerges during investigations within the domain of Internet of Things research. Put simply, it is imperative to devise a methodology that permits the following, contingent upon the particular circumstances:

1. Test the system or its prototype against predefined criteria;
2. Or evaluate the system's performance by calculating the specified indicators.

The process of solving one or both of these problems for a particular software product or prototype is called testing.

2.1.1. Structure of the IoT system using Blockchain technology

The IoT system comprises the subsequent fundamental components:

IoT devices, including sensors and actuators, are entities that gather environmental data or execute actions in the physical world.

The infrastructure that connects IoT devices and enables them to exchange data is the IoT network.

An IoT management system is software that analyzes data collected from IoT devices and makes management decisions regarding those devices.

Structure of the IoT system using Blockchain technology.

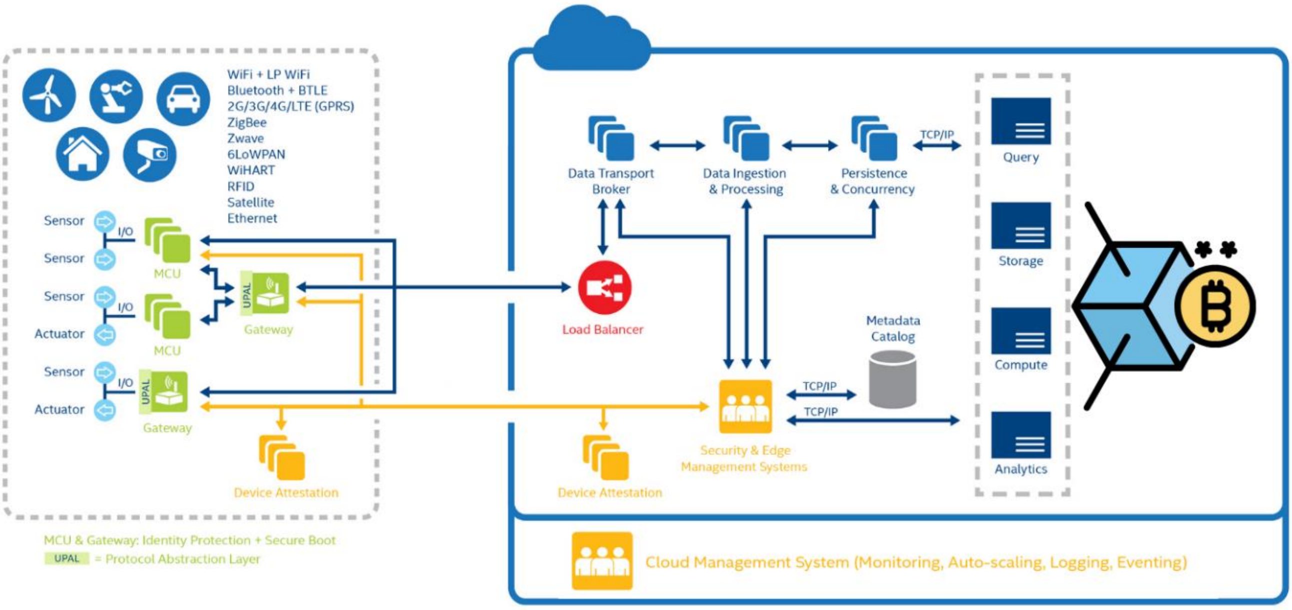


Figure 2.1. Block diagram of an IoT system using Blockchain

As illustrated in the preceding diagram (Figure 2.1), the structure of an IoT system utilizing cutting-edge Blockchain technology was examined in depth. In the current digital environment, this Blockchain integration into the IoT system is a strategic move toward assuring the security and dependability of these systems. Hence, it is imperative to examine the interplay between every constituent of the system and their respective functions in establishing a dependable and secure data exchange milieu within the Internet of Things:

1. *Blockchain network:*

The blockchain network is the central element of the system. It includes a distributed ledger where the full history of transactions is stored. The consensus protocol provides a single point of view for all network participants. Each block contains transaction data, including type, participants, and time.

2. *Smart contracts:*

Smart contracts are programs that automate the terms of transactions. Being in the blockchain, they are activated automatically when the conditions are met. They are used to automate access control, payment for services, and other IoT system functions.

3. *System participants:*

Participants can be individuals, organizations, or IoT devices. They interact with the system through web applications or other tools to perform transactions and utilize resources.

4. *4. IoT devices:*

Physical IoT devices act as sensors or actuators. They collect data and transmit it to the network for processing.

5. *5. Web applications:*

Web applications allow you to interact with the system. Users can manage devices, view data, and perform other functions through an intuitive interface.

6. *6. Tokens:*

Digital tokens are used for various purposes, such as payment for services or access control. They can be stored on a blockchain and used for transactions in an IoT system.

Interaction between components:

- The blockchain network provides a single view of transaction information in the system.

- Smart contracts automate the execution of transactions in the system.

- System participants interact with the blockchain network using web applications or other tools.

- IoT devices collect and transmit data to the system.

- Web applications allow users to interact with IoT devices and the IoT system.

- Tokens can be used for various purposes in the system, such as payment for services, access control, and others.

The IoT system using Blockchain technology can be used to automate access control, payment for services, resource accounting, and system security.

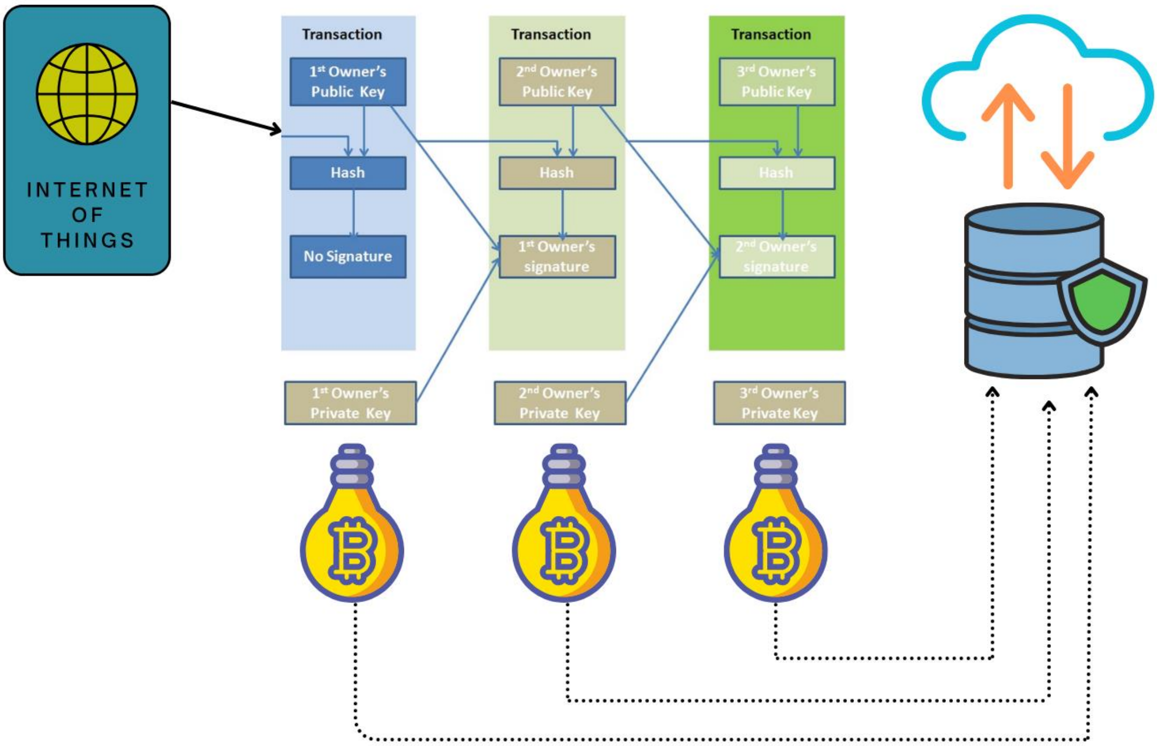


Figure 2.2 Data model for storing information about transactions in the IoT system using Blockchain technology

The previous Figure 2.2 illustrated the data model used to store information about transactions in the IoT system with the integration of Blockchain technology. Therefore, we can identify the main elements of the data model:

1. *Transaction ID* is a unique field that gives each transaction its own identifier. Using a unique ID allows you to uniquely identify and track each individual transaction in the system. This becomes important for determining the history and status of each transaction.

2. Transaction Type - this field defines the nature of the transaction being performed. It allows you to determine, for example, whether it is a payment for services, transfer of resources, or any other specific action. Knowing the type of transaction helps in further understanding its purpose and processing.

3. Transaction Participants - this field indicates the parties involved in the transaction. These can be individuals, organizations, or IoT devices that are interacting. Knowing the participants helps to establish context and track the owners and executors of transactions.

4. Transaction Data - this field contains specific data related to the transaction performed. For example, it can be the amount of payment, the amount of resources transferred, or any other details related to the transaction itself. The information in this field is key to understanding the nature of each transaction and its impact on the system.

5. Transaction Time - this field defines the exact moment in time when the transaction was executed. Specifying the time is important for establishing the chronology of events and allows you to identify dependencies between transactions.

Using Blockchain technology, this data model is an efficient method for storing information regarding transactions in an IoT system. By interacting, the fields of this paradigm furnish the system with a comprehensive and organized information foundation. Adaptations to the implementation are possible in accordance with the particular requirements and attributes of a given application.

2.2 Definition and Evaluation of IoT System Quality

In summary, the following is a concise enumeration of the primary characteristics of IoT systems. These systems are fully integrated into their surroundings and acquire data continuously via sensors. Manual mode renders modeling sensor readings and assessing system performance unfeasible as a result of the substantial volume and absence of human-machine interfaces. These characteristics result in a thorough assessment of software products within the domain of Internet of Things (IoT) systems in their operational setting, necessitating substantial financial and time investments. Even more difficult is the undertaking of investigating hypotheses concerning intriguing approaches.

Consequently, it is necessary to develop a specialized testing program that permits experiments to be performed on the system being evaluated, contrasting a variety of operational scenarios under distinct environmental conditions. The behavior of the system can be compared along multiple degrees of freedom, including external conditions that change, potential states or behavior modifications of controlled devices, and adjustments to the algorithms utilized by the tested system to make decisions. Critically, the testing of said system necessitates an extensive virtual replication of indicators associated with every process functioning within the system.

Simulation modeling is a category of modeling that enables the fulfillment of the specified criteria: an extended duration of virtual time, precise replication of processes, and unrestricted input and output data volume and structure. An examination of simulation modeling techniques that seem to be applicable in the domain of the Internet of Things (IoT) is warranted.

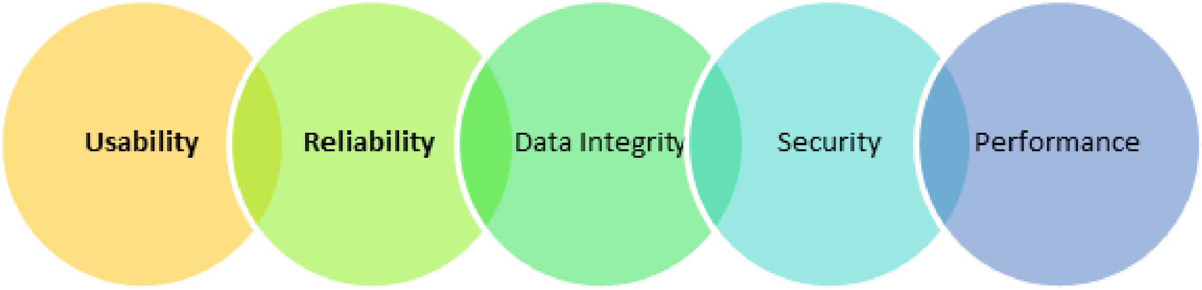


Figure 2.4. Simulation Modeling Requirements

A system is conceptualized as a collection of sub-models comprising their constituent elements, accumulators, fluxes, and auxiliary variables within the system dynamics method. This methodology involves the implementation of a mathematical model that symbolizes a dynamic system of simultaneous equations that are integrated with statistical data sources. For example, environmental factors such as room temperature and humidity can be parametrized as functions of a number of variables, including external temperature, humidity, human presence, heating system status, and more. At each instant during simulation, the necessary indicators are computed utilizing the given formulas. Additionally, the system might incorporate feedback. In the preceding illustration, the control of the heating system is influenced by the room temperature, which subsequently impacts the temperature.

The agent-based approach entails the precise definition of the actions taken by individual agents within the system, which subsequently determines the overall behavior of the system. Agents may be ecological, social, economic, or technical components of the system. Every agent possesses a distinct collection of states, transitions between them, events that initiate these transitions, time delays, and actions that they execute. An instance of this could be a "smart home" system agent who also resides in the residence. A basic model consists of two states, denoted as "at home" and "away," and the agent toggles between them at a specified virtual time.

There are also hybrid methods that combine multiple approaches during the modeling process. Pertaining to the Internet of Things, this approach is especially viable. More precisely, discrete components of the system may be denoted as agents, and the conditions under which they exist may be computed utilizing system dynamics.

Let us conclude this section with a brief discussion of alternative methodologies whose components may be incorporated into the hybrid system in question. To begin with, the discrete-event paradigm places emphasis on transitions, queues, delays, and resources that are initiated by events. The discreteness property of this model can be substituted for continuous fluxes of system dynamics in a hybrid model. Stochastic modeling techniques, which utilize random variables to represent the system's state, can be employed to accommodate the environment's non-deterministic characteristics. The most precise model can be determined through the use of evolutionary modeling.

Prior to examining the application of Node-RED in simulation modeling, it is prudent to perform a concise evaluation of a prevalent solution currently in use in this domain. The graphical editor Simulink provides a variety of components for constructing models; it is an integrated environment for design and modeling that incorporates MATLAB to facilitate numerical solution methods. In this environment, the construction of a model entails the interconnection of blocks that perform elementary operations including but not limited to summation, multiplication by a constant, and time integration. Users are then able to execute the simulation and observe the outcomes as graphics or data files.

Assuming the model is constructed appropriately, the Simulink environment can provide high modeling precision by utilizing MATLAB. As an illustration, the step can be automatically adjusted by the system to guarantee the utmost precision. In addition, Simulink offers an extensive variety of model components, rendering it applicable to virtually any field.

Figure 2.5. MatLab logo

However, this solution is not devoid of flaws; the relative difficulty of entrance persists, despite the implementation of a graphical representation. As an expert product, Simulink is comparatively expensive, particularly for researchers or developers who lack access within a particular organization. In relation to the testing and development procedures, it is not feasible to utilize a Simulink-generated model directly; instead, the current system necessitates the construction of an independent model. Due to these various factors, there are circumstances in which the implementation of Simulink becomes impracticable or, at best, inefficient.

2.3 Classification and Methods of Testing IoT System Quality

As previously described within the scope of this study, the testing process entails the computation of specific performance indicators that are utilized to assess the system's quality. In some cases, an intermediary review for adherence to predetermined criteria may also be performed during the testing phase. This obligation may manifest in two contexts: when a pre-existing product necessitates verification of its functionality for accuracy, and when conducting preliminary investigations into the field to identify the most auspicious methodologies.

Frequently, the operational conditions of IoT systems restrict the ability to detect changes to extended time intervals. To verify the accurate response to seasonal variables, for instance, the system must be tested for at least a year; a lesser time period would fail to encompass the complete range of possibilities. Certain occurrences, however, are so uncommon that they might not transpire despite such extensive testing. Extremely high or low temperatures, which may occur only once every few years, are one example.

Occasionally, it is feasible to conduct testing on a pre-existing system while considering every aspect of its physical implementation. Conversely, there are situations in which the product is conceptual or non-existent, rendering the testing of a theoretically developed approach imperative. Construction of a physical implementation of the system incurs substantial financial and material expenses in this instance. It is noteworthy to mention that even when dealing with a pre-existing system, there may be merit in segregating the software from its hardware implementation. Specifically, it becomes feasible to duplicate particular specified scenarios in order to verify the accuracy of specific modifications. Furthermore, as previously stated, the duration of the research may present an obstacle if it becomes imperative to monitor developments transpiring over protracted timespans. In such situations, it may be logical to employ technologies that enable the acceleration of this process.

Notwithstanding the aforementioned obstacles, the importance of testing within the domain of the Internet of Things should not be undervalued. This stage is required due to the stringent functionality, dependability, and efficiency requirements. However, during the initial phases of development, it might be more practical to forego the physical implementation of the system in favor of software technologies.

When employing simulation, emulation, or imitation technologies, it is critical to acknowledge that in order to accomplish this task, a distinct testing infrastructure must be constructed. Frequently, specific modifications to both the testing and the tested systems are required in order to function collaboratively.

It is worth noting that the intricacy may arise when it comes to formulating testing criteria or requirements that accommodate numerous conflicting objectives. IoT system tasks frequently entail multiple prescriptions, necessitating a compromise; frequently, the nature of the relationship between them remains undefined throughout the research phase. Thus, it is essential that the testing system be adaptable in order to facilitate a seamless transition between various quality indicators.

2.4 Techniques and Peculiarities of Testing with Blockchain in IoT Systems

Based on an examination of simulation modeling as a methodology for testing the Internet of Things (IoT) and current solutions tailored for this purpose, specific considerations emerge as pivotal in the process of selecting simulation environment technologies. Determining deficiencies in current solutions that could potentially render them unsuitable for particular duties is critical. In such situations, the creation of a novel approach or system becomes especially pertinent.

The functionality of simulation modeling tools should encompass the ability to simulate and administer an extensive array of testing scenarios and devices, in addition to performing diverse quality assessments. Since the developed system ought to be extensible and readily modifiable, the range of technological capabilities is the most important criterion for its selection.

Although widely used for simulation modeling, Simulink imposes a significant obstacle to entry in terms of both the necessary expertise and available resources. Thus, an effort is made to formulate a methodology that is more readily comprehensible to the human eye. Although a visual environment is considered beneficial, visual representation is not sufficient on its own. Furthermore, the development process of the user is streamlined when library-formatted components are accessible to address particular duties.

Furthermore, it is critical to have the capability of transferring the developed system between various execution environments, ensuring a smooth transition from a prototype to the final product.

Lastly, an additional disadvantage to consider when evaluating Simulink is its substantial cost, which stems from its access and distribution model. It is advisable to utilize open-source software or, failing that, implement a payment model that is contingent upon the utilization of resources.

2.4.1 Node-RED development tool

Originally, in adherence to von Neumann's principles, a computer program was represented as a series of operations transpiring in a predetermined sequence. The emphasis is on commands in this paradigm, whereas data remains static. Each instruction modifies a value but does not affect the position of the data; the processor then proceeds to the subsequent instruction. The von Neumann model's shared memory does not present any challenges for single-threaded programs; however, it does confound parallelization efforts. An alternative data flow-based architecture was suggested. A program is represented as a directed graph in which data "flows" between commands in this instance. Every individual operation operates as an opaque entity, characterized by clearly defined inputs and outputs.

Stream programming is an evolution of the data flow programming concept. This paradigm disregards the intrinsic content of processes and represents a program as a network of them. The establishment of connections between processes within the network facilitates the transmission of data segments. Using this framework, programs are inherently loosely coupled. The only way in which network nodes are connected is through the format of the data they generate as output and receive as input.

Developed by IBM and implemented in the JavaScript programming language, Node-RED is a visual development tool that operates on the stream programming paradigm. Node-RED conceptualizes an application as a network of nodes, wherein each node fulfills a distinct function, such as receiving input data, internally processing that data, and subsequently transmitting it throughout the network. Data transmission between nodes is managed by the network.

In order to group and structure nodes into a unified conceptual entity, Node-RED implements the notion of a "flow." By presenting a flow as a distinct page within the editor, an intermediary level of context is established between a single node and the entire system. While not all nodes in a flow are required to be interconnected, the term "flow" can also denote a collection of nodes that are interconnected.

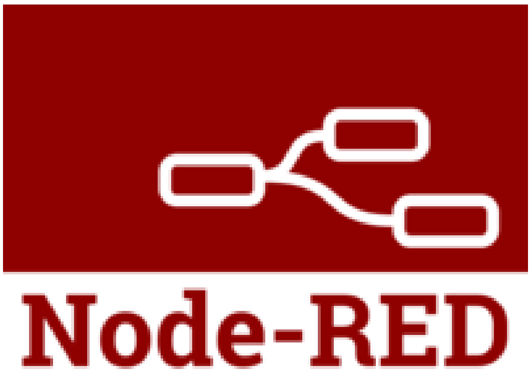


Figure 2.6. Node-RED logo

Every node in a flow awaits either messages from the node that came before it or an external occurrence that is not associated with the flow's activity. An example would be an external event, such as an HTTP request. Processing occurs once a message or event has been received by the node. After reaching its destination, the node has the capability to transmit a message. The number of output ports is not limited by the number of input ports on a node. Nodes engage in the exchange of messages, which are objects written in JavaScript, via connections known as wires.

Context allows information to be transferred between nodes in addition to messages. Node-RED establishes three distinct context levels: node-level, flow-level, and global. At the node-level, information is accessible solely to the node that generated it. At the flow-level, information is accessible to all nodes within the flow.

The execution environment for Node-RED is Node.js, and the development process is executed via a web browser. Users can add nodes, establish wire connections between them, and import and export flows in JSON format within the flow editor. JavaScript is utilized to implement custom nodes in Node-RED, while HTML is employed for the purpose of visualization.

Every individual node incorporates the "Observer" pattern internally, which allows for the notification of events to wired nodes. Flow input nodes are capable of managing HTTP requests, subscribing to external services, and listening on ports. A processing node receives data, executes predetermined operations, and subsequently communicates with subsequent nodes via events. Additionally, a node is capable of establishing connections with external services, generating supplementary events, and interacting with the operating system. For the duration of the flow, configuration nodes may be utilized to store configuration information that is shared.

There are three distinct levels within the Node-RED program: global, flow-level, and node-level. The global level comprises the complete program, comprising every node, its parameters, and interconnections. The initiation of execution occurs simultaneously with the concurrent recording of the global context. It is feasible to achieve continuous execution by implementing modifications and restarting the entire program. Every node is capable of receiving data simultaneously, and they all function in parallel.

The expulsion rate is significant in two situations. To begin with, variables that are shared by multiple nodes may be stored within the flow context. Secondly, structuring is facilitated by program division into multiple flows, which are depicted by separate tabs in the Node-RED visual editor. It is noteworthy to mention that while all flows operate concurrently, certain flows may be deactivated.

Ultimately, the level of nodes is of significant importance. With the exception of the capability to incorporate a custom-developed node, the Function node is the most versatile node in terms of functionality. By implementing any algorithm in this node via JavaScript, distinct behaviors are possible at node init, termination, and with each activation. A node of this nature may produce numerous outputs.

Specific nodes with a narrower purpose may be substituted for the Function node, which nevertheless generalizes particular operations, for a number of common duties. The Change node is an example of such a node; it permits the setting of context variable values and the modification of message properties. The Switch node is utilized to direct a message to one of multiple flow branches in accordance with input data or context variables. While this node by default generates messages for all its outputs that match the specified rules, it can be configured to only transmit messages when the first matching rule is met.

Concurrently, specialized nodes are implemented to perform particular functions, including the parsing of diverse data formats, processing requests according to a designated protocol, facilitating file input-output, and exhibiting graphical user interface elements. External node collections may also be linked in Node-RED to accomplish duties for which the default collection does not contain a suitable node.

Apart from the visual editor, Node-RED offers a variety of supplementary views that facilitate the examination of system behavior. The "dashboard," which displays graphical interface elements specified by special nodes, is the most versatile. The software provides functionality for generating text, graph, and image outputs, in addition to functioning with control elements like input fields and buttons.

Node-RED provides the functionality to initiate message flow manually through the Inject node and access transmitted messages via the Debug node. Multiple debug nodes may be incorporated to present every message interpreted by the Debug node in a distinct debugging interface.

Within the domain of the Internet of Things (IoT), Node-RED presents a number of merits in comparison to alternative choices: the capacity to abstract from the system's concrete implementation, visual representation, and support for a wide range of platforms. Although Node-RED does impose supplementary expenses on data transmission and processing, it is generally regarded as a suitable addition to the majority of systems, similar to any supplementary layer. Nevertheless, certain systems may present challenges that surpass the capabilities of Node-RED, albeit this can be mitigated in part through the use of user extensions. Despite this, the Node-RED tool is highly compatible with the development of IoT systems, and its prowess in this domain extends to its abilities in testing and modeling such systems. An elaborate elucidation of the prospective application of Node-RED within this framework will be furnished.

The IoT system is conceptualized as an individual Node-RED flow, despite the fact that it can be implemented autonomously and linked via network nodes with relative ease.

A program for conducting simulation experiments is implemented in a distinct flow or flows. This program comprises data sources, generators of diverse metrics (such as system time), and nodes that are tasked with communicating with the tested system and analyzing its behavior.

No constraints are placed on the formats of data when utilizing Node-RED; however, they must be capable of being represented as JavaScript objects. The primary obstacle is posed by restrictions on the frequency of events. In practical application, it has been noted that signal transmission rates exceeding 10 cycles per second cause observable delays within the system. Therefore, when the time resolution in the system is one hour, it is possible to attain a 36,000-fold acceleration over real-time. However, when the resolution is reduced to one minute, the acceleration is only 600-fold. Additional reductions in the virtual time interval between two signals are impractical, given that experiments in IoT systems require time scales ranging from one day to one year.

Node-RED seems to be a viable instrument for simulation modeling due to its extensive collection of nodes and the flexibility with which they can be combined to simulate virtually any desired metric. From the perspective of the developer, visual programming simplifies the construction of complex relationships between metrics, thereby facilitating user comprehension of the system's architecture. Furthermore, the simplification of testing duties is achieved when the system being evaluated was built upon Node-RED.

CONCLUSIONS FOR CHAPTER 2

A comprehensive analysis of the foundational principles that govern the development and enhancement of the operational quality of Internet of Things (IoT) systems, with a specific focus on their integration with Blockchain technology, has been conducted in this chapter. A synopsis of the overarching attributes of the Internet of Things was provided, with consideration given to the impact of Blockchain-based system architecture. An assessment and characterization of the quality of Internet of Things (IoT) systems were carried out through the application of a categorization of testing methodologies, investigation of testing techniques and peculiarities utilizing Blockchain technology.

Considerable emphasis was placed on the Node-RED development tool, which is indispensable for the pragmatic investigation and understanding of testing methodologies and intricacies in Internet of Things (IoT) systems. The insights gained and the outcomes of the analysis form the basis for future investigations that seek to optimize and improve the quality of Internet of Things systems through the implementation of Blockchain technology. This chapter delineates fundamental elements that will be scrutinized and expanded upon in the following sections of this study.

CHAPTER 3

THEORETICAL ASPECTS OF PROBABILITY AND ATTACK STRATEGIES IN BLOCKCHAIN FOR IOT

3.1 Analysis of Blockchain applications

3.1.1 Operation principles of Smart Contracts

Smart contracts, an intriguing implementation of blockchain technology, serve as a critical component in facilitating transactions. Conventional contracts frequently incorporate intermediaries, including regulatory bodies, banks, notaries, and registrars. Nevertheless, the proliferation of blockchain technology has rendered these intermediaries superfluous, thereby paving the way for the implementation of "smart contracts."

Smart contracts, which originate from the English language, are computer programs designed to automate and streamline the process of carrying out a wide range of contracts or transactions. The decentralized nature of blockchain technology gives rise to this technology, which exhibits considerable potential in diverse sectors, including education.

Figure 3.1. Using smart contracts

Practical implementations of the concept, which originated in 1994, became achievable with the advent of blockchain technology, most notably the Ethereum project led by Vitalik Buterin, a Canadian-Polish programmer. Fundamentally, a smart contract is a computer program that is specifically engineered to optimize and mechanize the adherence to various contract categories or transactions. The open interface of blockchain technology and the decentralized nature of smart contracts enable the formation of distributed autonomous organizations, which can function as a prototype for artificial intelligence.

A smart contract is defined by the consulting firm Oliver Wyman as "an agreement between two or more parties that is computationally enforced and features a digital signature." A software agent, functioning as a third virtual party, possesses the capability to implement and satisfy a minimum portion of the stipulations outlined in such agreements.

As defined by Melanie Swan, a smart contract is a method of forming agreements via blockchain using cryptocurrency. By defining and executing automatically on the basis of blockchain code, this technology eradicates the necessity for trust between parties, thus reducing the risks associated with human factors.

A more precise definition of the term "smart contract" is required.

A smart contract is a computer algorithm that is specifically engineered to facilitate the creation and upkeep of commercial agreements within the framework of blockchain technology. Agreements of this nature may be formed peer-to-peer (P2P) between two individuals, P2O between an individual and an organization, or P2M between an individual and a machine.

As agreed-upon conditions, smart contracts facilitate the automation of payments and the exchange of currency or other assets. The contract is set to autonomously execute when a predetermined condition is fulfilled (e.g., when item "1" is sold on exchange "2"). At that point, the contracting parties exchange assets (e.g., funds, digital currency, ownership rights, data). The transaction is subsequently duplicated and validated on the blockchain.

Smart contracts enable the secret exchange of assets, thereby introducing a novel type of virtual agreement that has the capacity to disrupt the legal system as a whole. Smart contracts, despite being code fragments that implement actions automatically upon the fulfillment of predetermined conditions, are not yet regarded as conventional contracts in the eyes of the law. However, they can function as substantiation of problem-solving capabilities, and numerous sectors are investigating potential uses of these contracts. Nevertheless, broad implementation of smart contracts is anticipated by specialists in the far-off future, given that the technology is presently in its experimental phase and has not yet reached a level of development suitable for the introduction of commercial products.

In order to initiate the construction of a smart contract, the following components are necessary:

- The subject of the contract requires that the program be able to access the goods or services that are associated with the contract, as well as the capability to automatically give or restrict access to those goods or services.

- The agreement is initiated by each party by signing the contract using their own private keys when using digital signatures.

- All of the parties are required to sign the contract terms, which are the conditions of the smart contract that are presented in the form of a certain sequence of actions.

- The models outlined above between two individuals (P2P), an individual and an organization (P2O), or an individual and a machine (P2M) are some examples of contract participants.

- The smart contract is kept in a distributed manner across the platform's nodes and is recorded in the blockchain of this platform. The blockchain contains each and every one of these components within it.

3.1.2 Description of the Initial Coin Offering Principle and Token Concepts

Investments can be raised through a process known as an Initial Coin Offering (ICO), which involves selling investors a certain quantity of new cryptocurrency units that have been obtained through a one-time or accelerated issuance.

Additionally, the phrase "Initial Token Offering" (ICO) is utilized, and the term "crowdsale" is sometimes identical with the meaning of ICO.

Figure 3.2. Initial Coin Offering

A token is a unit of value that is issued by a private entity within a blockchain system. The term "token" comes from the English word "token," which can be interpreted as a sign or an identification.

It has been said by D. Brenner that the following is the typical order of events that takes place during a token presale:

1. The dissemination of a white paper, which in common parlance is a description of the network and plans for its forthcoming development.

Before the first token is generated, the announcement of an impending initial coin offering (ICO) and the publication of the source code are planned.

3. The deployment of the network and the generation of tokens through mining; the possibility of reserving tokens for the founders as a reward for contribution to the development of the network and the idea.

4. ICO promotion and token sale to interested parties.

5. Work on developing applications, generating a network effect, and providing support for the network; as the network expands, there will be a greater demand for tokens, which will result in an increase in the value of user tokens.

The following components are often included in the framework of a white paper to be more specific:

A brief overview of one sentence is included on the title page, along with the company's emblem and name.

Two, the table of contents of the document.

3. An abstract is a condensed explanation of the research endeavor that is often presented on a single page.

4. The introduction takes into account the existing state of affairs in the specific market segment in which the business intends to operate; trends that are developing a particular market; and reasons that are controlling developments.

5. The premises section provides an explanation of the problem that led to the creation of the project as well as the risk that is related with the ongoing development of this problem.

6. A description of the project should include the following components: goals, objectives, mission, social and commercial relevance, operational mechanics, description of the prototype, examples of how the project might be used, and user roles. Every single one of these items has the potential to be either a component of the overall description or separate subsections.

7. The Marketing Analysis provides a description of the market realities and the demand for the project.

8. The Technical Section provides descriptions of the technologies and the specifics of their application.

9. Token Description and Financial Model is a comprehensive document that provides holders with information regarding the coin that has been issued and the economic rationale behind it.

10. The Development Roadmap outlines the important stages of project development together with their respective deadlines.

11. The term "project team" refers to the personnel who are working on the project and the duties that they are playing. More faith is placed in the project when the members of the team have a higher level of authority.

A conclusion provides a summary, discusses the most important issues, and emphasizes the most important components of the project.

Tokens can be earned through activities such as mining in Bitcoin, Ethereum, or Sia networks, as well as content creation on platforms like Steemit. Tokens, recorded on the blockchain, can be freely bought and sold for any cryptocurrency or fiat money.

Token-Stocks (crypto-stocks) grant holders the right, in exchange for investments, to receive dividends from the network's income or transaction fees. For example, in the Sia network, 3.9% of the income from storage is paid to Siafund holders—tokens representing shares in the network. Token-stocks often represent stakes in Decentralized Autonomous Organizations (DAOs), where tokens are programmatically issued, funds are raised through their sale, and contracts are made with developers. Additionally, holders of DAO token-stocks have the right to propose business ideas and vote on existing proposals in proportion to their token-stock holdings. Examples include Digix, a DAO built on the Ethereum platform, Golem, SingularDTV, and Sia.

There are three advantages to conducting ICOs for entrepreneurs and project founders:

1. Access to Larger Funding Rounds – ICOs provide the opportunity to secure a larger funding round in a shorter time compared to traditional venture capital, while allowing the project to maintain full control over how shares are distributed.

2. Instant Public Relations and Ecosystem Building – ICOs involve thousands, sometimes tens of thousands of participants, fostering a strong community interested in the project's success from the early stages of development. This instant community engagement is a shift from the involvement of a limited number of funds and underwriters, providing not just smart money but also crowd wisdom.

3. Market Feedback and Early Adopters is similar to kickstarter, where product manufacturers gather orders years ahead of production, ICO interest signals the potential market reaction to the proposed product in the blockchain space. ICO investors act as a form of prediction market, often more accurate than expensive analysts and consultants.

In the book "Blockchain. Blueprint for a New Economy," researcher and founder of the Blockchain Research Institute, Melanie Swan, identifies three conceptual application areas for this technology:

- Blockchain 1.0, Currency - Cryptocurrencies are applied in various applications related to financial transactions, such as payment systems and digital payments.

- Blockchain 2.0, Contracts - Applications in the fields of economics, markets, and finance that deal with various types of instruments, including stocks, bonds, futures, collateral, legal titles, assets, and contracts.

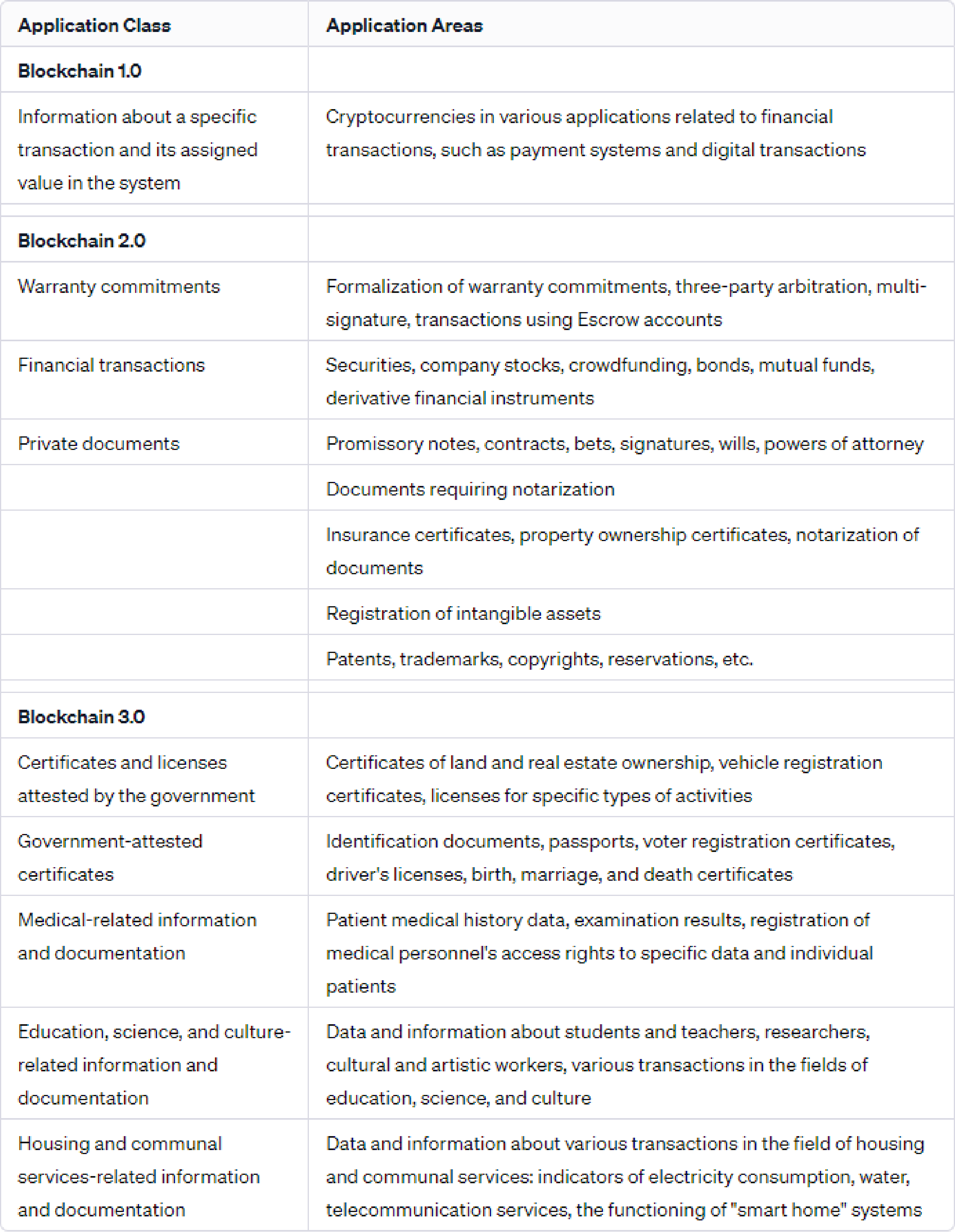
- Blockchain 3.0, Applications that go beyond financial transactions and markets, extending to areas such as government management, healthcare, science, education, and more.

Developers of a wide variety of comprehensive information systems, notably those working to advance the methodology within the "Smart City" idea, have investigated whether or not it is possible to adopt technologies that utilize distributed ledgers. Table 3.1 provides a variety of instances of initial developments that have been made using blockchain applications. These examples are divided according to classifications.

The table was prepared by the writers, taking into consideration the information that was published on the website of "Ledra Capital" in one of the blog series that was titled "Bitcoin Series 24: The Mega-Master Blockchain List."

Table 3.1

Application of distributed ledger technology in Blockchain applications



Application Class	Application Areas
Blockchain 1.0	
Information about a specific transaction and its assigned value in the system	Cryptocurrencies in various applications related to financial transactions, such as payment systems and digital transactions
Blockchain 2.0	
Warranty commitments	Formalization of warranty commitments, three-party arbitration, multi-signature, transactions using Escrow accounts
Financial transactions	Securities, company stocks, crowdfunding, bonds, mutual funds, derivative financial instruments
Private documents	Promissory notes, contracts, bets, signatures, wills, powers of attorney
	Documents requiring notarization
	Insurance certificates, property ownership certificates, notarization of documents
	Registration of intangible assets
	Patents, trademarks, copyrights, reservations, etc.
Blockchain 3.0	
Certificates and licenses attested by the government	Certificates of land and real estate ownership, vehicle registration certificates, licenses for specific types of activities
Government-attested certificates	Identification documents, passports, voter registration certificates, driver's licenses, birth, marriage, and death certificates
Medical-related information and documentation	Patient medical history data, examination results, registration of medical personnel's access rights to specific data and individual patients
Education, science, and culture-related information and documentation	Data and information about students and teachers, researchers, cultural and artistic workers, various transactions in the fields of education, science, and culture
Housing and communal services-related information and documentation	Data and information about various transactions in the field of housing and communal services: indicators of electricity consumption, water, telecommunication services, the functioning of "smart home" systems

A majority of blockchain applications are now in the process of being developed, and the key areas of application for blockchain technology are primarily within the banking and finance industries. There is a wide range of technological solutions that are based on blockchain technology that have the potential to transform the financial system. These solutions include interbank settlements, transactions between legal and natural people, payments, securities, and credit histories.

Microtransactions are quickly becoming one of the most important and potentially fruitful avenues in the commercial and financial sectors. Transactions involving fractions of a cent were not within the realm of possibility for internet users until relatively recently. The development of applications that are based on blockchain technology makes the implementation of such payments more feasible and practical. This makes it possible to effectively monetize social networks by providing an alternate method of payment for completion of modest activities such as completing surveys or providing freelance editing services for a variety of unique clients.

Traceability of the supply chain is the key to the potential application of blockchain technology in commercial transactions. Numerous cases in the past have resulted in the suspension of production across entire industries due to the contamination of products by a single manufacturer. In circumstances like these, prompt action is of the utmost importance, and blockchain technology is ideally suited for tasks like these. Using blockchain technology, all suppliers will be able to independently and dependably identify their products, and retail networks will be able to provide consumers with accurate information regarding the origin and route of the ingredients that are contained in the product that they have purchased. Provenance, for instance, is a firm that has effectively implemented blockchain technology in grocery stores. This serves as an example. The implementation of blockchain technology on a worldwide scale for huge organizations is a more challenging challenge, and major retail chains are currently making enormous efforts to address this issue.

Although there has been a little decrease in the level of excitement surrounding Bitcoin-based consumer goods, the blockchain technology that underpins them continues to be appealing due to the lower costs associated with them, particularly in the context of global peer-to-peer transactions.

The protection of intellectual property is another area in which blockchain technology can be utilized. The American firm Kodak, which has a long and illustrious history, intends to implement blockchain technology in order to protect the copyrights of photographs and images that are registered on its platform. It is especially important to keep this in mind in this day and age of liberalized internet, when it has become increasingly difficult to safeguard such rights. In order to invest in this endeavor, Kodak has already begun collection of funds. The music industry has a huge demand for photos and photographs, in addition to other types of media. PeerTracks, MUSE, Bittunes, and Ujo Music are examples of blockchain projects that are tackling issues related to the infringement of copyrights and the domination of music platforms. These projects are guaranteeing that creators receive appropriate pay. It is noteworthy that Sony, a Japanese technology powerhouse, has submitted a patent application to the United States Patent and Trademark Office for the purpose of utilizing blockchain technology for the purpose of copyright protection. According to their argument, the technical mechanisms of copyright protection (DRM) that are currently in use, which are designed to ensure operational compatibility, "may not be very reliable and rely on a single exceptional point of failure." It is possible that the user will lose all of the content that they have acquired if the rights protection system or service provider goes out of business or fails in some other way. The system that Sony has developed is capable of functioning across a wide range of content and data, including but not limited to movies, television, video, music, audio, games, scientific data, medical data, and more.

In addition, Sony has submitted yet another patent application concerning the application of blockchain technology in the field of education, with the intention of preserving information such as user data, learning experiences, and certifications. They have also investigated blockchain technology in the context of a concept that is not directly related to education. This concept is the Internet of Vehicles, which makes it possible for drivers to share information about the current state of the roads in a decentralized network.

This concept is partially aligned with another potential approach, which is the Internet of Things (IoT), which also incorporates blockchain technology because to the decentralized nature of blockchain technology.

3.1.3 Implementation Model of Blockchain Technology for Organizing Scientific Research Placement Scenarios

The system functions in a decentralized fashion, and all of the individual participants are on an equal footing. However, the following are the most important roles:

Participants who are responsible for confirming transaction hashes and adding them to the blockchain are referred to as miners. They "mine" new bitcoin and receive a "salary" in the form of transaction fees based on their mining activity. The quantity of bitcoin that may be released is restricted, and anyone who are able to properly add a block to the blockchain are responsible for generating a new chain of blocks.

Developers are communities that are focused on improving, altering, fixing, and resolving vulnerabilities in the system in order to guarantee that the system functions properly, that productivity is maximized, and that security is maintained.

- Individuals, organizations, and resources that have the ability to facilitate the purchase of bitcoin using fiat currency or other cryptocurrencies.

The clients of the system who are interested in purchasing, exchanging, or transferring cryptocurrencies. The participants in the system are equal, as was indicated previously, and this enables any user to take on any of the roles that are available.

On the basis of these fundamental functions and the characteristics of blockchain technology, an attempt can be made to establish a system for education and research, or some processes inside it would be possible.

An illustration of the operation of the proposed system and the players in it can be found in (Figure 3.3).

The blocks consist of the research that was carried out by the participants. These blocks are arranged into chains according to the manner in which they are relevant to particular topics, and they have the capability to reference other blocks from different chains (themes).

Researchers are required to generate a one-of-a-kind researcher identity that is assigned to their research upon placement in order to establish a connection to the system.

A one-of-a-kind digital signature is also provided to each block in order to prevent any tampering with data that has already been submitted, hence ensuring the data's safety. Each participant is responsible for performing a mathematical verification of the signature, which is analogous to the role that miners play in the blockchain network.

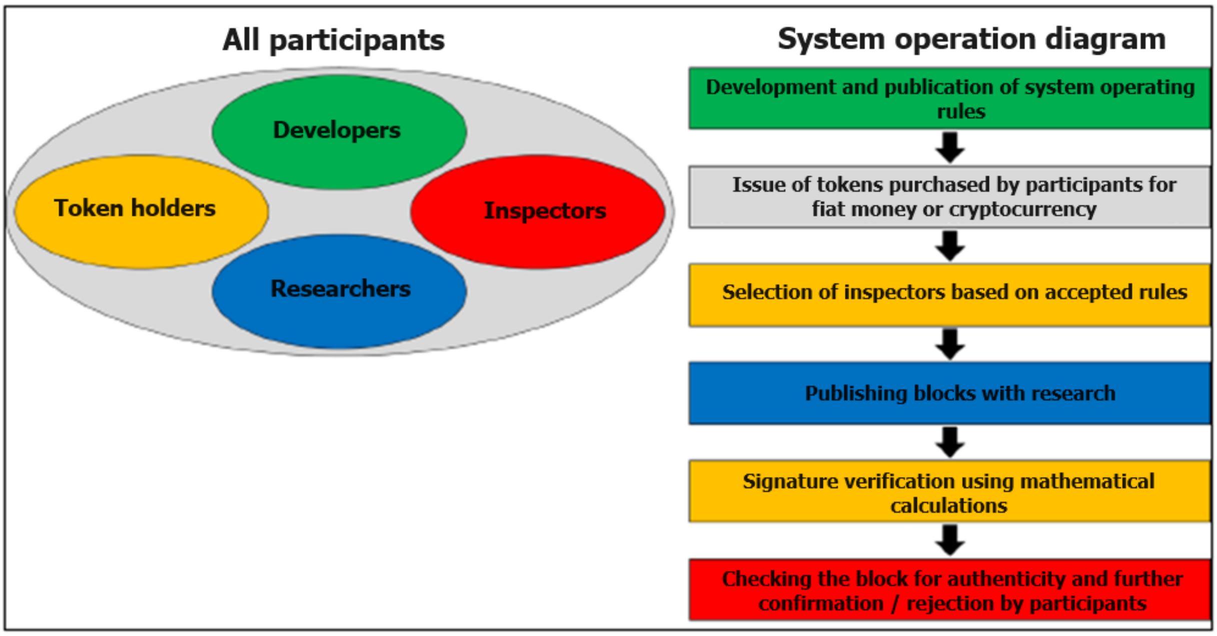

All participants
Developers
Token holders
Inspectors
Researchers
System operation diagram
Development and publication of system operating rules
Issue of tokens purchased by participants for fiat money or cryptocurrency
Selection of inspectors based on accepted rules
Publishing blocks with research
Signature verification using mathematical calculations
Checking the block for authenticity and further confirmation / rejection by participants

Figure 3.3. Operational Model of Blockchain Technology Utilization as a Chain of Research Blocks

The concept of anonymity is ensured by the fact that the one-of-a-kind digital signature is not connected to any personal information. Nevertheless, in a manner analogous to that of cryptocurrencies, individuals have the option of revealing their identify by linking their researcher identifier with their persona during the process. Because of this, researchers are able to work together by forming organizations (such as research teams, educational institutions, and related entities). In addition, participants have the option of conducting business either directly under their own personal name or on behalf of an organization.

Participants in the system will authenticate research by referring to certain blocks or complete blockchains that have been validated in the past. Each block or blockchain will contain information that is either confirmed or denied. The inclusion of the block in the blockchain will next be confirmed or rejected by further parties who are taking part in the validation process.

Tokens will be awarded to participants as a reward for verifying blocks. These tokens will give access to verify the block, publish research, and possess real-world value, which will ensure the financial stability of the system. If the system is successful in acquiring popularity and integrating with established trading platforms and exchanges, then it will be possible to exchange or acquire tokens on these platforms and exchanges.

In order to prevent the widespread confirmation of false research by people who are not qualified, the certification of the validity of the block will be limited to particular participants. One or more of the following may be included among the selection criteria: the quantity of issued research, the volume of verified blocks, and others.

There is the possibility of implementing a rating system in order to govern block publications. Participants who have a defined identify and whose research is persistently lacking in verifiability would be subject to increasingly larger token costs with each submission for verification. By taking this method, the workload of the system will hopefully be reduced.

Researchers will be incentivized to publish legitimate studies in order to avoid paying huge fees for submitting their research to the blockchain. This will ensure that they receive significant incentives for successfully adding studies to the blockchain.

Token holders will be in possession of a valuable asset and will have the opportunity to "mine" it by validating signatures and having the ability to either confirm or reject verifications. The validators of a block that are the earliest and those that are the most accurate will gain the biggest rewards, which will ensure that data is both fast and relevant.

In order to ensure the safety of their tokens, developers, who are active participants in the system, will be concerned about the system's ability to run correctly and securely. Since this is the case, the system is in accordance with the prerequisites for self-regulation.

In light of the fact that any participant is able to take on several responsibilities, equal involvement is encouraged. As the blockchain continues to amass a vast database that contains only the most recent information, it will draw new players who are eager to acquire tokens in order to have access to this "knowledge treasure trove."

Due to the fact that each block is protected by a signature and possesses a unique identity, this approach removes the requirement for comprehensive patenting, which in turn considerably reduces the complexity of the bureaucratic process.

In spite of the fact that the system can give the impression of being somewhat utopian, with researchers possibly not being interested in block verification or researchers not being ready to pay for submission privileges, the advantages and the potential of the technology can act as drivers of development.

It is of the utmost importance to acknowledge that not every research should be made public for the simple reason that it may be harmful to individuals or the environment. Consequently, it is vital to have a filtering mechanism that ensures compliance with regulations and maybe moral norms, which takes into account ethical issues.

3.2 Examples of Using Blockchain for Information Security in IoT

3.2.1 Security Aspects and Attacks in PoS Consensus Protocols

Proof of Stake (PoS) consensus protocols play a pivotal role in blockchain systems by determining the entities eligible to create new blocks and receive corresponding rewards. Security aspects and potential attacks associated with PoS consensus protocols include:

1. *Block Withholding Attack:*

In this attack, a network participant, holding a specific quantity of stakes (cryptocurrency), refrains from confirming new blocks, thereby retaining a portion of their stakes within the network.

Possible consequences may lead to consensus loss and a reduction in network security.

2. *Attack Strategies:*

- Strategy 1 (DoS Attack): An attacker abstains from confirming blocks on the main chain, opting for an inactive strategy.

- Strategy 2 (Double Confirmation Attack): The attacker confirms blocks on the main chain but utilizes their stakes to create an alternative branch.

3. *Withholding Attack Modification (Power Splitting Attack):*

This attack involves the malicious actor splitting their stakes among two or more nodes, granting them the ability to choose which blocks to confirm or withhold.

Among the potential implications is that it will become more difficult to detect and defend against attacks that involve block withholding strategies.

The mathematical precision that Grunspan and Perez-Marco displayed in their statements and reasoning is one of the most striking aspects of their impressive body of work. Grunspan used Rosenfeld's assumption without providing any proof, notably the concept that the process of creating "honest" and "dishonest" blocks in the network may be characterized by a negative binomial distribution. The authors of the study establish that Grunspan adopted Rosenfeld's assumption without providing any proof. On the other hand, it is necessary to point out that the authors of this work did not make any attempt to get rid of the assumption that instantaneous block propagation occurs simultaneously. Furthermore, by employing special functions, they first demonstrate that the chance of forking reduces exponentially with the length of the fork. This is the evidence that they present.

The primary finding of Grunspan and Perez-Marco's study, which takes into account the assumption of zero synchronization time, is completely in agreement with the result that Rosenfeld presented, which is known as Theorem 1.2. On the other hand, it is of the utmost importance to emphasize that this research completely justifies this outcome. Bernoulli, binomial, negative binomial, exponential, Erlang, and Poisson probability distributions were the six types of probability distributions that were required in order to accomplish this goal. As a result, the evidence is shown to be complicated, even when the assumption of zero synchronization time is taken into consideration, which makes the study substantially easier to understand.

A comparison of the logarithmic expressions of attack success probabilities produced according to Nakamoto's and Grunspan's formulas is presented in Figure 3.4. This figure also includes a detailed illustration of the comparison.

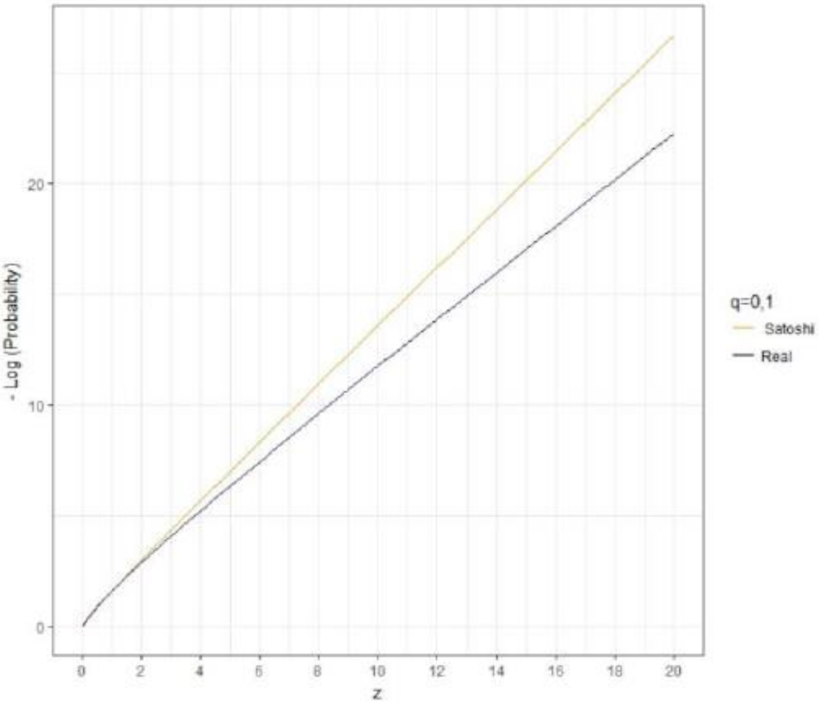


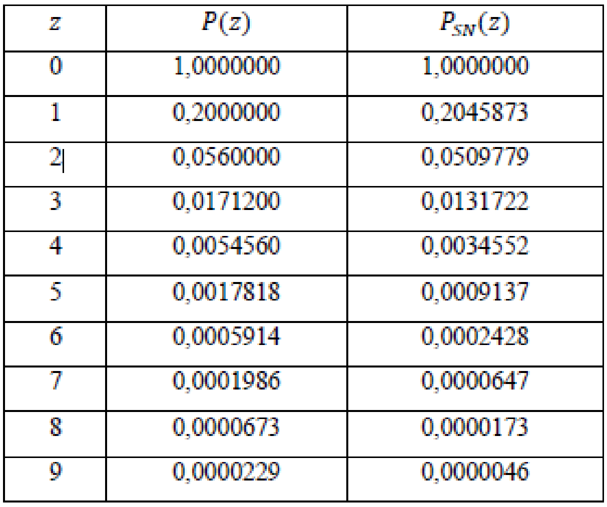
Figure 3.4. Attack Success Probabilities According to Nakamoto and Grunspan

For attackers with computational capacity equal to 0.1, the y-axis displays the logarithm (with a minus sign) of the success probability function. The x-axis depicts the number of blocks, while the y-axis displays the logarithm. Yellow is used to represent the numerical values of success probability acquired from Nakamoto's method, while blue is used to illustrate the results gained from Grunspan's approach. Block numbering is indicated in both directions.

Another set of findings that are comparable can be found in Tables 3.2 and 3.3.

Table 3.2

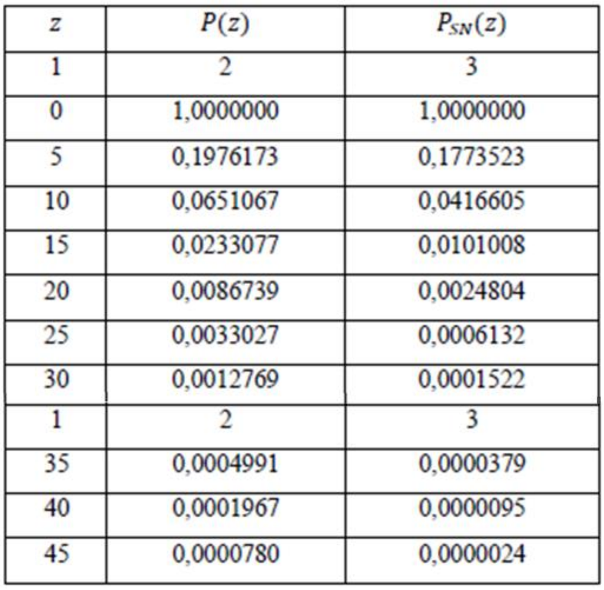
Success probabilities according to Nakamoto's and Grunspan's methods for q = 0.1.



z	$P(z)$	$P_{SN}(z)$
0	1,0000000	1,0000000
1	0,2000000	0,2045873
2	0,0560000	0,0509779
3	0,0171200	0,0131722
4	0,0054560	0,0034552
5	0,0017818	0,0009137
6	0,0005914	0,0002428
7	0,0001986	0,0000647
8	0,0000673	0,0000173
9	0,0000229	0,0000046

Table 3.3

Success probabilities according to Nakamoto's and Grunspan's methods for q = 0.3.



z	$P(z)$	$P_{SN}(z)$
1	2	3
0	1,0000000	1,0000000
5	0,1976173	0,1773523
10	0,0651067	0,0416605
15	0,0233077	0,0101008
20	0,0086739	0,0024804
25	0,0033027	0,0006132
30	0,0012769	0,0001522
1	2	3
35	0,0004991	0,0000379
40	0,0001967	0,0000095
45	0,0000780	0,0000024

Following conducting a study of Tables 3.2 and 3.3, it becomes apparent that the data that Grunspan has offered reflect situations that are less favorable in comparison to those that Nakamoto has provided. To put it another way, it seems as though the likelihood of an attack happening successfully is higher. The occurrence of this issue can be ascribed to the fact that Nakamoto's assumptions were quite inaccurate.

3.2.1.1 Probability of Attack Success Based on the Number of Confirmation Blocks

The goal and approach of carrying out the Block Withholding Attack for the Proof-of-Stake protocol are, in essence, comparable to those of an attack of a similar nature carried out for the Proof-of-Work protocol. In this part, we will investigate precise formulas for the chance of a successful Block Withholding Attack in the PoS protocol. We will also demonstrate that this probability is dependent on the number of confirmed blocks as well as the percentage of bad actors that are present in the network. One of the most important things to keep in mind is that the time it takes for the network to synchronize is almost irrelevant for the Proof-of-Stake protocol. This is because the time window in which a stakeholder is required to construct a block is typically substantially greater than the time it takes for the network to synchronize. In addition, the time required to generate blocks for the Proof-of-Stake protocol is significantly less than that required for the Proof-of-labor protocol due to the marked reduction in the amount of computational labor involved. Both of these aspects contribute significantly to the benefits that the PoS protocol offers.

First, let's go over basic notations so that we may continue our conversation. Let's say that J is a representation of the blocks that make up the "correct" version of the blockchain, which was created by miners who were honest. Transaction X, in which the attacker carried out a transfer of funds to the provider, is included by miners in a block as part of a particular block. In accordance with the regulations governing the acceptance of transactions, the supplier anticipates receiving z confirmation blocks after block. According to what was stated earlier, this is done in order to make the process of replacing the chain that contains the block with another chain that contains a block that contains an alternate transaction Y more difficult. Determine the number of confirmed blocks that, given a certain fraction of attackers, guarantee that the probability of success of the Block Withholding Attack does not exceed a specified value. For example, for the sake of certainty, let's assume that the attacker constructs a fork beginning from block, which precedes the block with transaction X. This will allow us to determine the probability of success of the Block Withholding

Attack. In this part of the article, we will examine two different assault execution tactics and determine the likelihood of success for each of them.

3.2.1.2 Strategy 1: The attacker does not acknowledge blocks from the main branch

The adversary does not form blocks in the main chain during his timeslots. He uses these timeslots to form an alternative chain that starts with block B_{i-1} but after z blocks of $B_{i+1},B_{i+2},\dots,B_{i+z}$ are formed, he tries to create an alternative branch starting with a block that precedes B_i block . Note that this branch must necessarily start before the B_i block, otherwise the block with transaction “Y” will contain an incorrect transaction that uses coins that have already been spent and will be removed from the blockchain along with all blocks referring to it.

Let the alternative chain with a branching point B_{i-1} at be the chain, $B_1,\dots,B_{i-1},B_i',B_{i+1}'$ where' B_i are the blocks generated by the attacker. It is important that according to this strategy (the adversary does not form his blocks in "honest" chains), all blocks in the chain $B_{i+1},B_{i+2},\dots,B_{i+z}$ as well as block B_{i-1} formed by honest participants. To succeed, the adversary must build an alternative chain that is longer than the "honest" chain.

This is possible only if, for some *s* after the formed blocks $B_{i+1},B_{i+2},\dots,B_{i+z}$, the number of enemy timeslots between the slot $t(B_{i-1})$ and the slot with the number *S is* not less than the number of "fair" slots for the same time interval. In this case, he can form a chain:

$$B_0,\dots,B_{i-1},B_i',B_{i+1}',\dots,B_r' \;, \tag{1.1}$$

for some *r*, where all $B_i',B_{i+1}',\dots,B_r'$ blocks are created in the time intervals belonging to the attacker, a B_r' is created in the time interval number *s*.

Therefore, a necessary and sufficient condition for a successful attack is the existence of a sequence of time intervals after $t(B_{i-1})$ when the number of slots belonging to the attacker is not less than the number of "honest" slots.

Suppose that among n participants, exactly t ($t < n / 2$) are malicious and $n - t$ *are* honest.

Thus, $p = (n - t) / \text{n}$ is the probability that the next timeslot belongs to an honest miner, and $q = t / n$ *is the* probability of an alternative event.

Let $\xi_i,\ i \geq 1$ be a sequence of random variables that take two values:

$$\xi_i = \begin{cases} -1, \text{ with probability } q, \\ 1, \text{ with probability } p. \end{cases} , \tag{1.2}$$

where -1 corresponds to the attacker's timeslots, 1 corresponds to the timeslots of honest miners.

Let's define the following random variables:

$$S_0 = 0,\ S_n = \sum_{i=1}^{n} \xi_i; , \tag{1.3}$$

$$S_0^- = 0,\ S_n^- = \sum_{i=1}^{n} (-\xi_i \vee 0) \text{ та } S_0^+ = 0,\ \ S_n^+ = \sum_{i=1}^{n} (\xi_i \vee 0). , \tag{1.4}$$

For some, let's define another random variable $k \in N$:

$$\tau_k = min\{l \geq 1 : S_l^+ = k\}. , \tag{1.5}$$

Now the problem of calculating the probability of success of an attack can be formulated as the problem of calculating the probability of the following event for $k = z + 1$

$$A(k)=\{\exists\, m>\tau_k : S_m^- \geq S_m^+\},\,, \qquad (1.6)$$

where S_m^-, S_m^+ are defined in accordance with (1.1) - (1.3).

For further definitions, we will need a result related to random walks, namely the player's bankruptcy lemma.

In notation (1.1) - (1.3), we define random variables:

$$S_n^{(k)}=S_n+k\,,\; S_0^{(k)}=k\,.\,, \qquad (1.7)$$

We also define the event $C_k=\left\{\exists\, l\in \mathrm{N}: S_l^{(k)}=0\right\}$ and denote its probability by . Then by $q_k=P\left(C_k\right)$ Lemma 1.1:

$$q_k=\begin{cases}1, \; if \;\; q\geq p,\\ \left(\dfrac{q}{p}\right)^k, else.\end{cases}\,, \qquad (1.8)$$

To prove the main result about the probability of success of a block spoofing attack, we need some definitions and properties of special functions.

Definition 1.1. A regular incomplete beta function is a function

$$I_x\left(a,b\right)=\sum_{l=a}^{\infty}C_{b+l-1}^{l}x^l\left(1-x\right)^b=\frac{B_x\left(a,b\right)}{B\left(a,b\right)}\,, \qquad (1.9)$$

where $B_x\left(a,b\right)=\int\limits_0^x t^{a-1}\left(1-t\right)^{b-1}dt$ is an incomplete beta function;

beta function:

$$B\left(a,b\right)=B_1\left(a,b\right)=\int\limits_0^1 t^{a-1}\left(1-t\right)^{b-1}dt=\frac{\Gamma\left(a\right)\Gamma\left(b\right)}{\Gamma\left(a+b\right)}\,, \qquad (1.10)$$

gamma function:

$$\Gamma(x)=\int_{0}^{\infty} t^{x-1}e^{-t}dt \quad , \tag{1.11}$$

Lemma 1.2: A regular incomplete beta function satisfies the symmetry relation:

$$I_p(a,b)+I_q(a,b)=1\text{, для } 0\leq p,q\leq 1\text{, } p+q=1\text{.} \quad , \tag{1.12}$$

From Lemma 1.1 and the definition of a negative binomial distribution, we obtain the following corollary.

Corollary 1.1: In the given notation:

$$\sum_{l=0}^{z} C_{z+l}^{l} q^{z+1} p^{l} = \sum_{l=z+1}^{\infty} C_{z+l}^{l}\ p^{z+1} q^{l} \quad , \tag{1.13}$$

Now let's formulate the main result of this paragraph.

Theorem 1.3: In the given notation, the probability P_z of success of a block spoofing attack, provided that z confirmation blocks are received, is equal to:

$$P_z=\begin{cases} 1, & \text{if} \quad q\geq p; \\ P(A(z+1))=2\sum_{l=0}^{z} C_{z+l}^{l} p^{l} q^{z+1} \end{cases} \quad , \tag{1.14}$$

or, using the local Moivre-Laplace theorem, for the corresponding *p*, *q*, and *z*:

$$P_z=2p\sum_{l=0}^{z}\frac{\varphi\left(\frac{zq-lp}{\sqrt{(z+l)pq}}\right)}{\sqrt{(z+l)pq}} \quad , \tag{1.15}$$

or by using a regular partial beta function:

$$P_z = 2I_q\left(z+1, z+1\right), \tag{1.16}$$

which for sufficiently large z can be written as

$$P_z = \mathrm{O}\left(\left(4pq\right)^{z+1}\right), \tag{1.17}$$

Proof. Let's define the following events:

$$H_l = \{\tau_{z+1} = z+1+l\} = \{S^{-}_{\tau_{z+1}} = l\}, \quad l \in \{0,1,\ldots\}, , \tag{1.18}$$

where *Hl* *is an* event that means that the opponent has accumulated *l* blocks by the time the slot with the number τ_z starts. It is important that the events *Hl*, *l* $\in$ {0,1,...} form a complete group of events.

Then, using the full probability formula:

$$P(A(z+1)) = \sum_{l=0}^{\infty} P(A(z+1)/H_l)P(H_l), \tag{1.19}$$

The probability of an event *Hl*, *l* $\in$ {0, 1,...}, is defined as

$$P(H_l) = C^l_{z+1+l-1}p^{z+1}q^l = C^l_{z+l}p^{z+1}q^l, \tag{1.20}$$

$$\sum_{l=0}^{\infty} C^l_{z+l}p^{z+1}q^l = 1, \tag{1.21}$$

According to Lemma 1.1,

$$P(A(z+1)/H_l)=\begin{cases}(\frac{q}{p})^{z+1-l}, & \text{if } q<p \text{ and } l<z+1;\\ & 1,\ \text{else.}\end{cases}\quad , \tag{1.22}$$

Let's rewrite (1.9) using (1.10) - (1.12):

$$\begin{aligned}P(A(z+1))&=\sum_{l=0}^{z}C_{z+l}^{l}p^{z+1}q^{l}(\frac{q}{p})^{z+1-l}+\sum_{l=z+1}^{\infty}C_{z+l}^{l}\,p^{z+1}q^{l}=\\&=\sum_{l=0}^{z}C_{z+l}^{l}p^{z+1}q^{l}+\sum_{l=z+1}^{\infty}C_{z+l}^{l}\,q^{z+1}p^{l}=\\&=1-\sum_{l=z+1}^{\infty}C_{z+l}^{l}\,p^{z+1}q^{l}+\sum_{l=z+1}^{\infty}C_{z+l}^{l}q^{z+1}p^{l}.\end{aligned}\quad , \tag{1.23}$$

From Definition 1, Formula (1.4) and Lemma 1.1, as well as Corollary 1.1 and Formula (1.13), we obtain

$$P\left(A(z+1)\right)=1-I_p(z+1,z+1)+I_q(z+1,z+1)=2I_q(z+1,z+1)=2\sum_{l=0}^{z}C_{z+l}^{l}\,q^{z+1}p^{l}, \quad , \tag{1.24}$$

and formulas (1.5) and (1.7) are proved.

To prove formula (1.6), for the corresponding *z*, *p*, and *q* (if *z* · *p* · *q* > 25 or *p* ≤ 0.9 and $n\cdot p\cdot q>5$), the last expression can be written as $C_{z+l}^{l}p^{z+1}q^{l}$ або $pC_{z+l}^{l}p^{z}q^{l}$ and apply the local Moivre-Laplace theorem:

$$C_{z+l}^{l}p^{z}q^{l}=\frac{\varphi\left(\frac{zq-lp}{\sqrt{(z+l)\,pq}}\right)}{\sqrt{(z+l)\,pq}}, \quad , \tag{1.25}$$

Where $\varphi(x)$ is the standard normal distribution density

$$\varphi(x)=\frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}}. \quad , \qquad (1.26)$$

To prove formula (1.8), we note that

$$I_q(z+1,z+1)=\frac{1}{2}I_{4q(1-q)}\left(z+1,\frac{1}{2}\right)=\frac{1}{2}I_{4qp}\left(z+1,\frac{1}{2}\right),\ \text{коли}\ 0\le q\le\frac{1}{2}. \quad , \qquad (1.27)$$

For fixed *x*, *b* ($b>0$, $0<x<1$), with $a\to\infty$, for each $n=0$, 1…, the following equality is true:

$$I_x(a,b)=\Gamma(a+b)x^a(1-x)^{b-1}\times$$
$$\times\left(\sum_{k=0}^{n-1}\frac{1}{\Gamma(a+k+1)\Gamma(b-k)}\left(\frac{x}{1-x}\right)^k+\mathrm{O}\left(\frac{1}{\Gamma(a+n+1)}\right)\right). \quad , \qquad (1.28)$$

So, for $n=0$ we get:

$$P(A(z+1))=2I_q(z+1,z+1)=I_{4pq}\left(z+1,\frac{1}{2}\right)=$$
$$=\Gamma(z+1.5)(4pq)^{z+1}(1-4pq)^{-\frac{1}{2}}\times\mathrm{O}\left(\frac{1}{\Gamma(z+2)}\right)=\mathrm{O}\left((4pq)^{z+1}\right). \quad , \qquad (1.29)$$

The theorem is proved.

The logarithm of the probability of a fork, Pz, which is described in formula (1.7) (on the y-axis), is shown to be $(4pq)^{z+1}$ dependent on the value of z (on the x-axis) in the following figure, which illustrates the relationship between the two variables for various percentages of the attacker. Because the graphs for the logarithm of the probability are straight lines, the value of Pz itself drops exponentially with z. This is because the graphs represent the probability. According to formula (1.8), the rate of decay of the function P (A($z + 1$)) with increasing *z is the* same as that of the function .

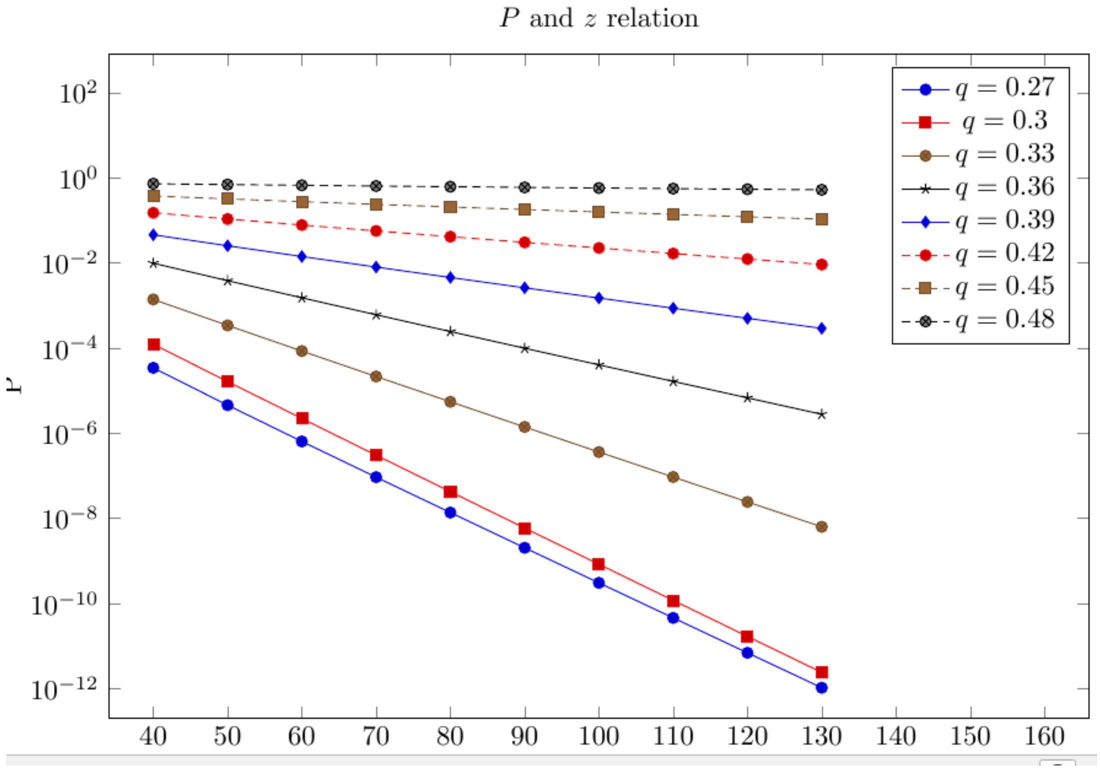


Figure 3.5. Plots of the logarithm of the probability of attack success

Table 3.4 shows the minimum values of z for different values of the attacker's share q that satisfy the condition $P(A(z))<10^{-3}$:

Table 3.4

The minimum number of acknowledgment Pz blocks at which

q	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45
z	10	10	15	20	25	60	150	540

3.2.1.3 Strategy 2: The attacker confirms blocks from the main branch

When deploying this tactic, the attacker will construct his blocks on the main chain while assuming the identity of a trustworthy participant. This will continue until the transaction has received the necessary amount of confirmations. Subsequently, he initiates an assault by establishing a chain that provides an alternative.

Similarly, to the previous scheme, in the alternative chain, it can use all its time slots after the moment when the B_{i-1} block was generated. The difference is that all the blocks in this chain are generated in consecutive timeslots without gaps, i.e., only z time slots are enough to generate z acknowledgment blocks for the B_i block.

To create an alternative chain starting from the block B_{i-1} , the attacker can use all of his own timeslots (starting from the moment after the slot number i-1 when B_{i-1} was formed).

We will use the notation introduced earlier. For some $k \in$ N we define the following event:

$$E(k) = \{\exists\, m \geq k : S_m^- \geq S_m^+\}. , \tag{1.30}$$

Then to calculate the probability of success of the attack, it is enough to calculate

$$P(E(z+1)), \tag{1.31}$$

Theorem 1.4: In the given notation, the equality holds

$$P(E(z+1)) = (2q)^{z+1}. , \tag{1.32}$$

Proof. Let's define the events:

$$H_l = \{S_{z+1}^- = l\}, l = \overline{0, z+1}. , \tag{1.33}$$

Event *Hl* means that the enemy has accumulated *l* timeslots between $t(B_{i-1})$ and $t(B_{i+z})$. In addition, the events *Hl*, *l* $\in \{0,1,...\}$ form a complete group of events.

Then, using the full probability formula:

$$P(E(z+1)) = \sum_{l=0}^{z+1} P(E(z+1)/H_l)P(H_l) \quad , \qquad (1.34)$$

The probabilities of events *Hl*, $l \in \{0,1,...\}$ are defined as the probability of a binomial distribution:

$$P(H_l) = C_{z+1}^{l} q^l p^{z+1-l}, \quad l = \overline{0, z+1}, \qquad (1.35)$$

We obtain the probabilities $P(E(z+1) / Hl)$ using Lemma 1.1:

$$P(E(z+1)/H_l) = \begin{cases} (\frac{q}{p})^{z+1-l}, & if \ \ q < p \ \ and \ \ l \le z+1; \\ 1, & else. \end{cases} \quad , \qquad (1.36)$$

Let's rewrite (1.15) using (1.16) and (1.17):

$$P(E(z+1)) = \sum_{l=0}^{z+1} C_{z+1}^{l} q^l p^{z+1-l} \left(\frac{q}{p}\right)^{z+1-l} =$$

$$= \sum_{l=0}^{z+1} C_{z+1}^{l} q^{z+1} = q^{z+1} \sum_{l=0}^{z+1} C_{z+1}^{l} = q^{z+1} \cdot 2^{z+1} = (2q)^{z+1}. \quad , \qquad (1.37)$$

The theorem is proved.

Comparing formulas (1.7) and (1.14), we can see that the first strategy is more profitable for the enemy. Indeed, under the condition $p > \frac{1}{2} > q$ we obtain the following inequality:

$$4pq > 4 \cdot \frac{1}{2} q = 2q, \quad , \qquad (1.38)$$

therefore, the probability of a fork in the second strategy is less than its probability in the first strategy, with the same values of q and z.

3.2.1.4 Modification of the block spoofing attack: power sharing attack

In this part, we will consider a variant of the block spoofing attack, which we will refer to as the "power split attack," and we will establish an upper bound on the probability that it will be successful.

The primary characteristic that sets this alteration apart from others is that the attacker makes an effort to lessen the amount of computing resources that are available to honest miners by establishing circumstances in which a portion of these resources are squandered. A classic assault is one in which the attacker develops his chain in a covert manner during the duration of the attack, until it reaches a length that is greater than the main chain. At the precise moment that this occurs, he announces his generated chain, and miners that are trustworthy convert to using it. Within the framework of our suggested change to the attack, the chain is only published by the attacker when its length is equivalent to the length of the chain that is honest. In this particular scenario, the attack will only be effective if the conditions that are listed below are satisfied:

1) Honest miners will build two chains concurrently by splitting into two branches and generating two chains.

2) The honest branch will be the location where the first block is established. In the event that this does not occur, the existence of the alternate branch, and consequently the assault itself, will be disclosed prior to the successful completion of the attack.

Description of the attack:

5. Attacker A wants to buy goods from supplier B. To do this, A creates a transaction tx_1 with payment to B and sends it to the blockchain (Figure 3.6).

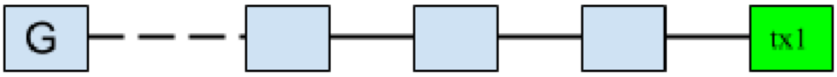


Figure 3.6. Transaction tx1 is included in the last block

- Following this, the attacker will instantly begin the process of constructing an alternative branch of the blockchain, which will be orange in color, but they will not make this branch public. It is imperative that he always keep the system in a state in which the chain of honest miners is either longer (as shown in Figure 3.6-8) or the same length (as shown in Figure 3.8) as the alternative chain.

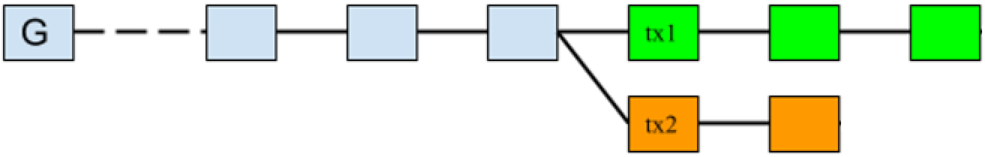


Figure 3.7. The main chain of the blockchain is ahead of the alternative one by one block

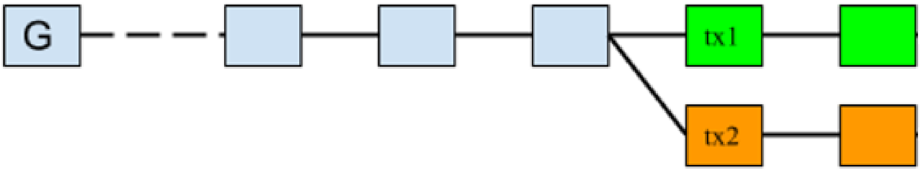


Figure 3.8. The main and alternative blockchain chains have the same length

- The attack will not take place if the first block of the alternative branch is made available to the public (see to Figure 3.8 for further information). Honest miners will switch to generating an alternative branch, which will result in the seller receiving a signal that his transaction does not have sufficient confirmation and simply flew off of the blockchain. This will occur because honest miners will switch to creating an alternative branch. A signal informing the seller of the presence of an alternate branch will not be sent to them until these conditions are satisfied. The signal will only be transmitted in the event that the alternative branch is successful in outrunning the chain that is honest. The seller continues to wait for the required number of confirmation blocks until that time comes, during which time he is unaware of the alternate transaction and does not recognize that he is being attacked.

- Immediately following the delivery of the items to the attacker, the latter has the ability to establish a secondary branch in the event that it becomes longer than the primary branch. Following that, transaction tx1 will be removed from the blockchain, and transaction tx2 will be put in its place. It is inevitable that the blockchain will continue to develop along the chain of the attacker, and the payment that was made to seller B will be deleted permanently. At the same moment, the goods and the money will be delivered to perpetrator A, who is the attacker.

Now, let's take a look at the significance of the attack's name. It is important for honest miners to select the branch that has the greater "amount of work done" when there are two branches of the same length that are operating simultaneously. On the other hand, considering that the synchronization time is not zero, it is possible that certain miners will see one of the branches as representing a larger duration. Assuming that every miner has an equal chance of beginning the development of a certain branch, the total computing power of all miners who are honest will be divided in half.

With the appearance of each new block, the probability of such a situation is equal to $\frac{1}{2}$ so the upper estimate of the probability of such an attack, provided there are z confirmation blocks, is equal to $\left(\frac{1}{2}\right)^z$ this probability decreases exponentially with the number of confirmation blocks.

3.3 Advantages and Disadvantages of Using Blockchain for Security in IoT

3.3.1 Benefits of Using Blockchain for IoT Security

The following advantages of using Blockchain technology to ensure IoT security can be highlighted:

- *Decentralized structure;*
- *Data immutability;*
- *Transparency;*
- *Improved transaction security;*
- *Resistance to attacks.*

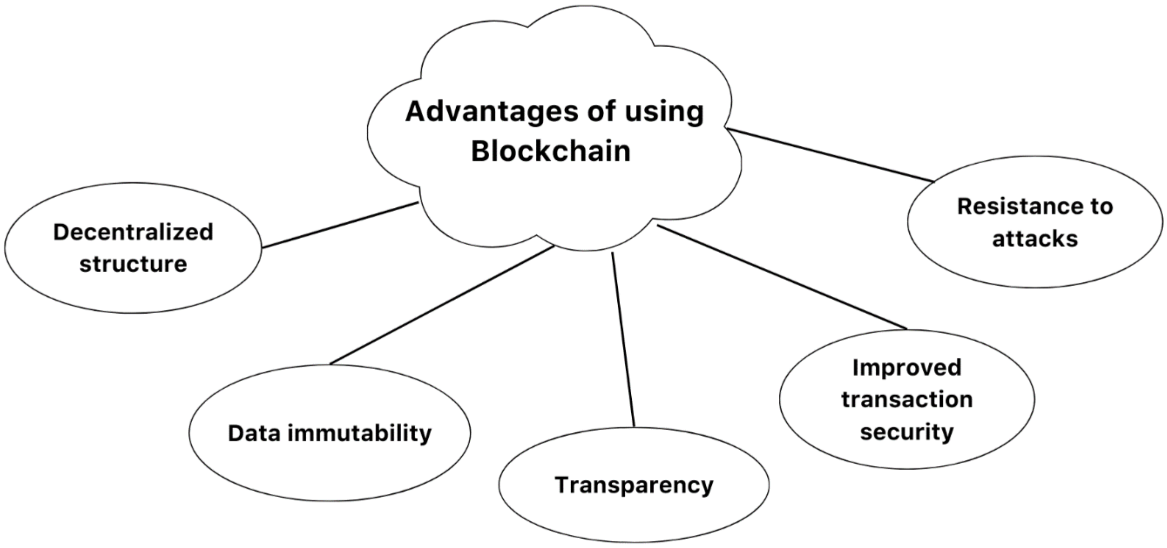


Figure 3.9. Advantages of using Blockchain technology

Decentralized blockchain structure and its impact on IoT security.

At a time when the Internet of Things (IoT) is becoming increasingly popular, modern technology is confronted with the difficulty of ensuring security. Integration of blockchain technology, which offers a decentralized data management framework, is one of the promising alternatives that might be implemented. Thus, it is necessary to investigate the ways in which the decentralized character of blockchain technology contributes to the enhancement of network security in the Internet of Things (IoT).

1- *Defining the decentralized structure of blockchain.*

In the context of a network, a blockchain can be understood as a distributed database that is held on numerous nodes. A blockchain is a distributed ledger that stores information in blocks, with each block including information on the block that came before it. This creates a chain of blocks. Due to the decentralized nature of the system, there is no central authority or facility for the storing of data.

2. *Difficulty of data hacking and modification*.

In traditional centralized systems, where data is stored in one central location, attackers can focus their efforts on attacking this point of vulnerability. In a blockchain, however, each node stores a copy of the entire blockchain, and for a successful attack, an attacker must change data on most nodes in the network at the same time.

3. Defense against a single point of vulnerability.

Thus, thanks to its decentralized structure, blockchain reduces the risks associated with a single point of vulnerability, which is especially important in the context of large-scale IoT adoption. The impossibility of a centralized attack increases the resilience of the entire network.

4. *Enhancing security in the IoT.*

In the context of the Internet of Things, where devices are constantly exchanging data, the decentralized structure of the blockchain provides strong protection against threats like data tampering or malicious tampering.

The decentralized structure of blockchain is a powerful tool for securing the Internet of Things. Integrating this technology can significantly reduce the risks of centralized attacks and create a more resilient and secure environment for IoT network communications.

Data immutability in blockchain and its role in ensuring information integrity.

Blockchain technology is distinguished by the immutability of data, which is one of its key properties. The immutability of data in blockchain is a vital quality that guarantees the dependability, integrity, and security of information from any potential attacks that could alter it. When it comes to the successful deployment of blockchain technology in a variety of domains that call for a high level of trust and data protection, this idea is an essential component.

1- *Features of data immutability in blockchain.*

Blockchain is a distributed ledger in which data is stored as blocks connected by a chain. Each block contains a hash of the previous block, which creates a unique chain of blocks. The information in a block is recorded in the form of transactions and subjected to cryptographic hashing.

2. *The principle of data immutability.*

The principle of data immutability means that once a block is added to the chain, its contents cannot be changed without the consent of the majority of the network participants. Each new block is built on the basis of the previous block and contains information about all previous blocks, making it extremely difficult to change a single block.

3. *The role of data immutability in ensuring integrity*.

Data immutability plays a critical role in ensuring the integrity of information on the blockchain. This means that once information has been added to the blockchain, it becomes an integral part of the chain, and any attempt to change the data causes the hashes of all subsequent blocks to change, which is immediately detected by the network.

4. *Preventing data modification attacks.*

As a result of the immutability of the data, blockchain technology effectively prevents any attempts to alter the content. Even if an attempt were made to alter a single block, it would necessitate the recalculation of all following blocks as well as the approval of the majority of network participants. This would make such assaults extremely difficult to execute and an extremely rare occurrence.

The role of transparency in blockchain technology.

Transparency in blockchain technology is a key element that brings a new level of trust and integrity to data management. This aspect of blockchain significantly reduces fraud risks and provides a solid foundation for the development of more open and transparent business processes.

1. *The principle of transparency in blockchain.*

Transparency in blockchain is based on the principle that data is open to all participants in the network. Each block contains information about transactions and the previous block, and this information is available to all participants in the network. This openness creates the conditions for maximum transparency in data management.

2. *Data accessibility for all participants.*

Blockchain is designed so that every participant in the network has access to a complete historical record of transactions. This removes the limitations that would exist in centralized data management systems where access may be restricted. In blockchain, each participant can verify the history and legitimacy of the data.

3. *Reducing fraud risks.*

The transparency of blockchain data significantly reduces fraud risks. Because every transaction is recorded and available for verification by all participants, data manipulation becomes extremely difficult. This creates a trusting environment where participants can be confident that processes are fair and transparent.

4. *Increased trust between participants.*

Through transparency, blockchain fosters trust among network participants. All parties are able to observe changes in data, and no one can hide or distort information without the explicit consent of other participants. This creates the basis for more trusting and mutually beneficial relationships.

<u>Improved transaction security on the blockchain</u>.

A considerable enhance in the security of transactions is brought about by the incorporation of encryption and cryptographic techniques into the blockchain. This not only makes the system less susceptible to manipulation, but it also provides a trustworthy environment for those who are participating in the network. In a world where digital transactions are the norm, these technologies not only guarantee the confidentiality of an individual's data but also increase the standard for integrity and authenticity.

1. *The role of encryption in blockchain.*

Encryption mechanisms play a key role in securing transactions on the blockchain. Each transaction is encrypted using cryptographic algorithms, making transaction data available only to those who have the appropriate key. This prevents unauthorized access and ensures the confidentiality of information.

2. *Protection from interference.*

Through the use of cryptography, the blockchain creates a mechanism that protects transactions from tampering. Each block contains a hash of the previous block, and changing data in one block will require recalculating the hash for all subsequent blocks. This makes it virtually impossible to make changes to past transactions without detection, which increases the security of the system.

3. *Key benefits of cryptography in transactions.*

- Data Integrity: Cryptography ensures the integrity of transaction data. Any change of data in the block will be instantly noticed, which reduces the risks of manipulation.

- Confidentiality: Data encryption ensures the confidentiality of information in transactions. Only participants with the correct keys can decrypt and read the data.

- Authentication: Cryptography also provides authentication of network participants. Unique keys authenticate participants and prevent tampering.

4. Complexity of cryptographic algorithms.

The cryptographic algorithms used in the blockchain are complex and computationally expensive, which creates an additional layer of protection. This makes it virtually impossible to conduct attacks on transactions using modern computing resources.

3.3.2 Disadvantages of Using Blockchain for IoT Security

In despite the fact that it is excellent in protecting data, blockchain is sadly plagued by a number of drawbacks that must be taken into consideration while contemplating its use in the Internet of Things. Finding ways to improve scalability, minimize power consumption, and make the integration process easier are all part of the things that are being worked on in this area.

When it comes to ensuring the safety of the Internet of Things, the following drawbacks of utilizing Blockchain technology might be identified:

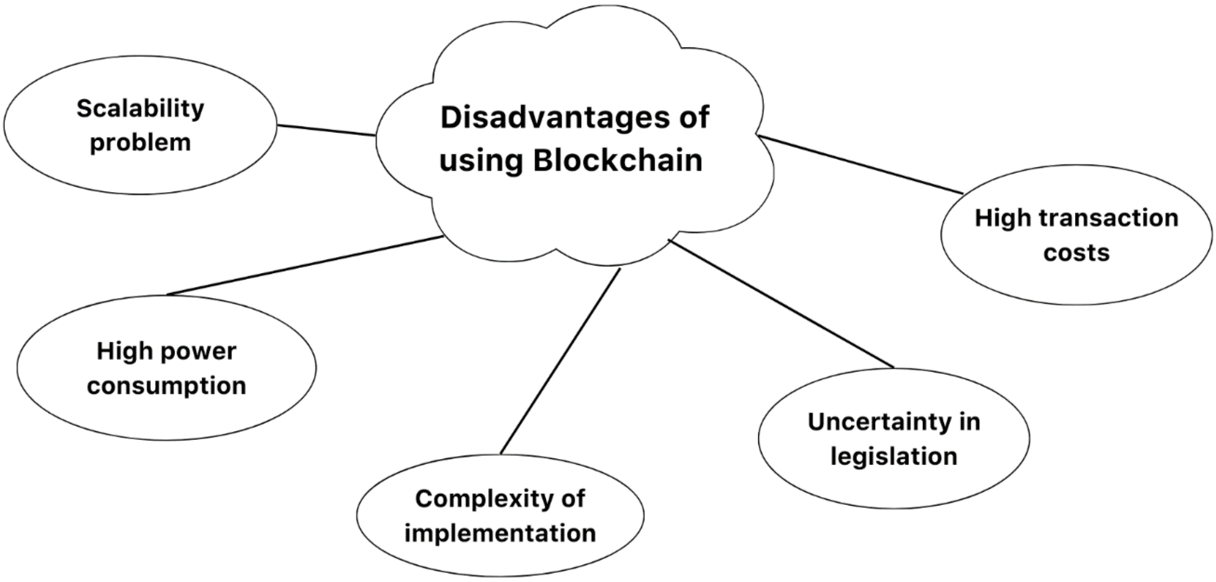

Disadvantages of using Blockchain
Scalability problem
High transaction costs
High power consumption
Uncertainty in legislation
Complexity of implementation

Figure 3.10. Disadvantages of using Blockchain technology

1. *Scalability problem.*

To date, one of the major drawbacks of blockchain is its scalability, especially when network activity is high. This can cause delays in transaction processing, making blockchain less efficient in a mass market environment.

2. *High power consumption.*

Some blockchains, especially those that use Proof of Work, require huge computational resources, which leads to high energy consumption. This is an important consideration given today's demands for sustainability and energy efficiency.

3. *Complexity of implementation.*

Integrating blockchain into existing IoT systems can be complex and requires significant infrastructure changes. This can be a barrier to widespread adoption of the technology in practical applications.

4. *Uncertainty in legislation.*

In some jurisdictions, legislation regarding the use of blockchain in IoT can be ambiguous, creating legal risks. The lack of clear regulation may make it difficult for the technology to be widely adopted.

5. *High transaction costs.*

It is possible for transaction costs to be rather expensive, depending on the particular implementation of the blockchain and the cryptocurrency that they are linked with. This restricts the adoption of blockchain technology in situations where the costs of transactions are of fundamental importance.

In light of this, it is essential to be aware of the drawbacks associated with this technology, despite the fact that blockchain technology provides a number of substantial benefits for enhanced security in the Internet of Things (IoT). In the context of the Internet of Things (IoT), blockchain offers a number of advantages, including a decentralized structure, immutability of data, transparency, and enhanced transaction security.

However, it is important to take into consideration the negatives, which include problems with scalability, high energy consumption, complexity in implementation, regulatory uncertainty, and high overall transaction costs. Additional research and development is required to address these concerns in order to make blockchain a more effective and cost-effective solution for ensuring the security of the internet of things (IoT).

CONCLUSIONS FOR CHAPTER 3

During the scope of this chapter, a thorough investigation into the theoretical elements of applying Blockchain technology to protect Internet of Things (IoT) systems was carried out. Within the first paragraph, a comprehensive examination of the many uses of Blockchain was carried out. This investigation included the operational principles of smart contracts and the notions of token issuance.

For the purpose of developing scenarios involving the deployment of scientific research, a particular focus was placed on providing an explanation of the Initial Coin Offering (ICO) principle as well as the application of Blockchain technology. This expanded the understanding of the possibilities of Blockchain beyond the mere exchange of cryptocurrencies, highlighting its potential applications in the fields of science and research.

After this, some instances of how Blockchain technology can be used to protect information in the Internet of Things were shown. Investigations were conducted into many security elements as well as various sorts of attacks, with a special focus on Proof-of-Stake (PoS) consensus methods. When it comes to knowing how to attain a high level of security in Internet of Things networks by utilizing Blockchain, the analysis of attack success probability, various techniques, and adaptations of attacks, such as the power-sharing attack, become crucial components. The process of calculating the chance of an assault being successful has emerged as an extremely significant stage, as it offers an objective method for evaluating the efficiency of the techniques that have been implemented.

Additionally, both the benefits and drawbacks of utilizing Blockchain technology for Internet of Things (IoT) security were investigated. The absence of intermediaries, reliability, and the immutability of data were among the identified positives. On the other hand, disadvantages such as scalability constraints and high prices were noted. Through this, a more complete picture of the opportunities and limitations of deploying Blockchain technology for the purpose of ensuring the safety of modern Internet of Things systems was revealed.

In light of the growing number of cyber dangers and problems, the findings that were gained in this chapter serve as a foundation for further research and the creation of effective strategies for applying Blockchain technology to defend Internet of Things systems.

CHAPTER 4
DEVELOPMENT OF PROPOSALS FOR PRACTICAL IMPLEMENTATION

4.1. Overview of Development Tools

As it comes to the development of the system, the implementation technologies that were selected are extremely important.

We decided to use the Java programming language for the design of the system because it is well-known for its wide collection of standard libraries that provide encapsulated functionality.

The JavaScript programming language was utilized in the process of building an all-encompassing automated system, with the frameworks Node.js and React.js being utilized. It was decided to use the MongoDB database for the storage of the data.

Assuming that the system will function on the Internet is a prevalent assumption. Through the usage of the HTTPS protocol, every interaction that takes place between the user and the system on the Internet takes place. There are four different kinds of HTTP requests that are used to carry out all of the data manipulation operations that take place on the internet. The REST architectural pattern is the foundation for data transport:

- GET – retrieve information.
- POST – save information.
- PUT – update information.
- DELETE – delete information.

Relevant information within HTTP requests is conveyed in JSON format. The implemented system utilizes the first two types of requests.

4.1.1 Mongo DB

Through doing away with tables, schemas, SQL queries, foreign keys, and a great deal of other components that are typical of relational databases, MongoDB presents a revolutionary approach to the development of databases. On the other hand, in contrast to relational databases, MongoDB provides a data model that is document-oriented. This results in higher scalability, faster performance, and more ease of use.

However, despite the fact that traditional databases have their problems and that MongoDB has its advantages, it is vital to acknowledge that jobs are different and that the approaches that are used to solve them are also different. If you have a scenario that involves complicated and architecturally diverse data storage, MongoDB might be a good option for you. On the other hand, standard relational databases might be more suitable for certain circumstances. This could also be accomplished through the utilization of a hybrid strategy, which involves storing one data type in MongoDB and another in conventional databases.

In order to facilitate the transmission of data in a seamless manner while preserving its integrity, the complete MongoDB system can be represented by a number of nodes that are located on separate physical machines.

When it comes to the sharing and storage of data, one of the most widely used standards is JSON, which stands for JavaScript Object Notation. Data that is architecturally complicated can be efficiently described using JSON. MongoDB's method of data storage is comparable to that of JSON, despite the fact that JSON is not officially utilized. BSON, which is an abbreviation for "Binary JSON," is the format that MongoDB uses for its storage options.

Data operations such as searching and processing can be completed more quickly with the help of BSON. In spite of the fact that BSON has a number of advantages in terms of speed, it does have a few small drawbacks: The space required to store data in JSON format is typically less than that required by BSON structured data. The enhanced speed, on the other hand, makes the trade-off more than acceptable.

MongoDB is a database management system that is built in C++, which allows it to be easily deployed on a variety of systems, including Windows, Linux, MacOS, and Solaris.

Even while it is possible to get the code and assemble MongoDB on one's own, it is strongly advised that one utilize official libraries.

Relational databases are used to store tuples, whereas MongoDB is used to store documents. When compared to tuples, documents have the ability to contain information that is structurally complicated and can serve as repositories for both keys and values. One way to think about a document is as a container that may be used to associate keys with particular data sets.

The idea of a primary key is something that both relational databases and MongoDB have in common, despite the fact that they are structured differently. When referring to relational database management systems, the term "primary key" is used to describe a column that has an index that is generated automatically and serves to identify a single record. In MongoDB, every document is assigned a one-of-a-kind identifier that is referred to as the "_id." In the event that it is not explicitly mentioned, MongoDB will construct a value for it automatically.

Each key is connected to a particular value in the database. However, it is crucial to take into consideration a particular aspect: in contrast to relational databases, which have a clearly defined structure with fields, and in which a field can be assigned a value of NULL if it does not have a value (depending on the individual database settings), MongoDB operates in a different manner. A key that is not useful is simply left out of the document and is not used if it does not have any value.

The world of traditional SQL is characterized by tables, whereas the world of MongoDB is characterized by collections. A broad array of objects with varying structures and property sets can be contained within collections, in contrast to relational databases, which consist of tables that store objects that are uniformly constructed and rigidly structured.

There are a number of replicas that make up the data storage system that MongoDB uses. This set may also contain a set of subsidiary nodes in addition to the primary node that it contains. Additionally, the integrity of all subsidiary nodes is preserved, and they are immediately updated in tandem with the primary node. In the event that the primary node breaks down for any reason, one of the secondary nodes will take over as the primary node.

Working with MongoDB databases and scaling them further is made substantially simpler by the absence of a hard database design and the ease with which a new schema may be created with minimal changes to the notion of data storage. Furthermore, it helps developers save time by removing the need to consider the creation of a new database schema and the elimination of the need to spend time generating complex queries.

4.1.2 Description of the Java Programming Language

For creating the system prototype, the Java programming language was chosen for the following reasons:

- Object-Oriented Programming (OOP) – in Java, everything is an object. Classes can be easily extended due to its object-oriented model.

- Platform Independence – unlike many other languages, including C and C++, Java, when created, wasn't compiled for a specific machine platform but into platform-independent bytecode. This bytecode is interpreted in the Java Virtual Machine (JVM), where it currently operates.

- Simplicity – learning and getting started with Java remain straightforward.

- Architectural Neutrality – he compiler generates architecture-neutral file format objects, making compiled code executable on various processors.

- Robustness – efforts are made to eliminate errors in different situations, relying mainly on compile-time, error-checking, and runtime checking.

- Multithreading – with features for multithreading, programmers can write applications that can perform countless tasks simultaneously. The introduction of this constructive feature in Java allows developers to create sophisticated interactive applications.

- Interpreted Nature – java bytecode is translated into machine instructions for execution and isn't stored anywhere. This process makes it faster and more analytical since binding occurs as an additional lightweight process.

- High Performance – the introduction of a Just-In-Time compiler allowed achieving high performance.
- Dynamic Nature – Java programming is considered more dynamic than C or C++, adapting to changes in variable conditions.

4.2 Description of Software Implementation

The automated system is developed based on the "Client-Server" principle and is capable of operating over the Internet. Each user needs to download server instances to their local machine and load a replica of the blockchain.

4.2.1 Description of the Blockchain Algorithm in the Automated Energy Resource Accounting System

An example of a chain structure is included in the operating concept. The chain is made up of blocks, and the blocks are organized according to the transactions that are generated by users of the system (for example, money transfers). The SHA-2 algorithm is used to compute a hash value for each block, which is generated based on the data included within the block (including transactions). This value is stored alongside the set of transactions that are contained within the block. Following the order in which they were created, each block is arranged in a queue in sequence. In addition to the hash value that was computed based on the data contained within the current block, the hash value of the block that came before it is also included. As part of the process of calculating the hash value of the current block, the hash value of the block that came before it is also taken into consideration. Because of this characteristic, the chains are formed. Any modification to even a single character will result in a significant change in the hash value, which will then lead to changes in the hash values of all subsequent blocks (which indicates an attempt to tamper with the data).

Because of the system's structure and the operational concept that it operates on, it is not possible to manipulate the data in the system. This is because doing so would demand enormous computational resources, which would ultimately be inefficient and expensive.

In addition to a digital signature, transactions are required to include the sender's address, the recipient's address, the time the transaction was created, and any other pertinent information. Both the sender and the destination addresses are wallets that are implemented by users through the use of asymmetric encryption and provided as a public key that is accessible to all users of the network. The timestamp is a representation of the time at which the transaction was created. A user is required to possess a pair of keys that are generated from a public key and a private key in order for the blockchain network to function successfully. Using the private key, which is only accessible to the person who owns the key, it is possible to generate a digital signature that will be a positive match when compared to the public key. The public key is checked to ensure that it has not been forged by this technique.

Through the use of flowcharts, the following diagrams present an illustration of the operational philosophy that underpins the blockchain.

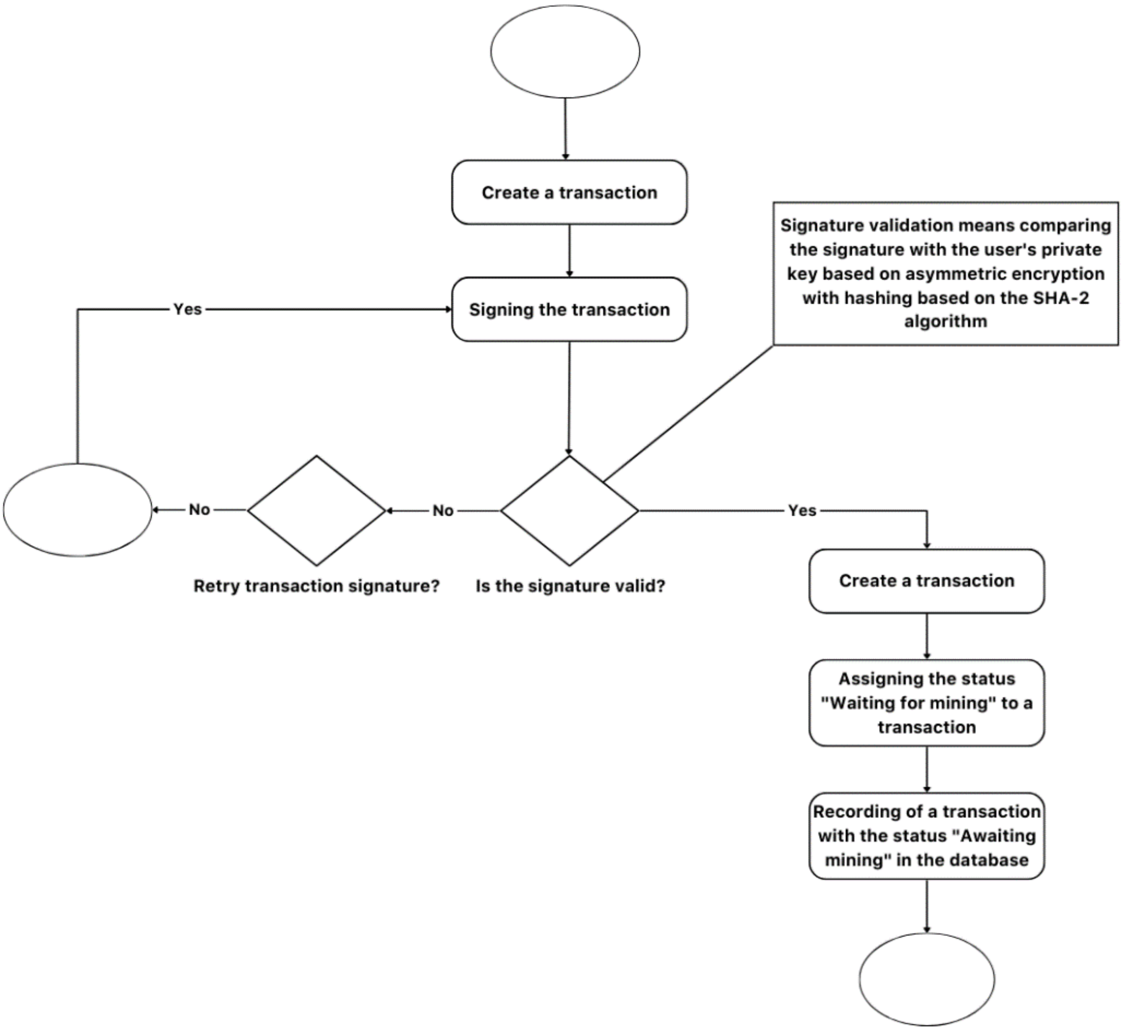

Create a transaction
Signature validation means comparing the signature with the user's private key based on asymmetric encryption with hashing based on the SHA-2 algorithm
Yes
Signing the transaction
No
No
Yes
Retry transaction signature?
Is the signature valid?
Create a transaction
Assigning the status "Waiting for mining" to a transaction
Recording of a transaction with the status "Awaiting mining" in the database

Figure 4.1. Transaction creation algorithm

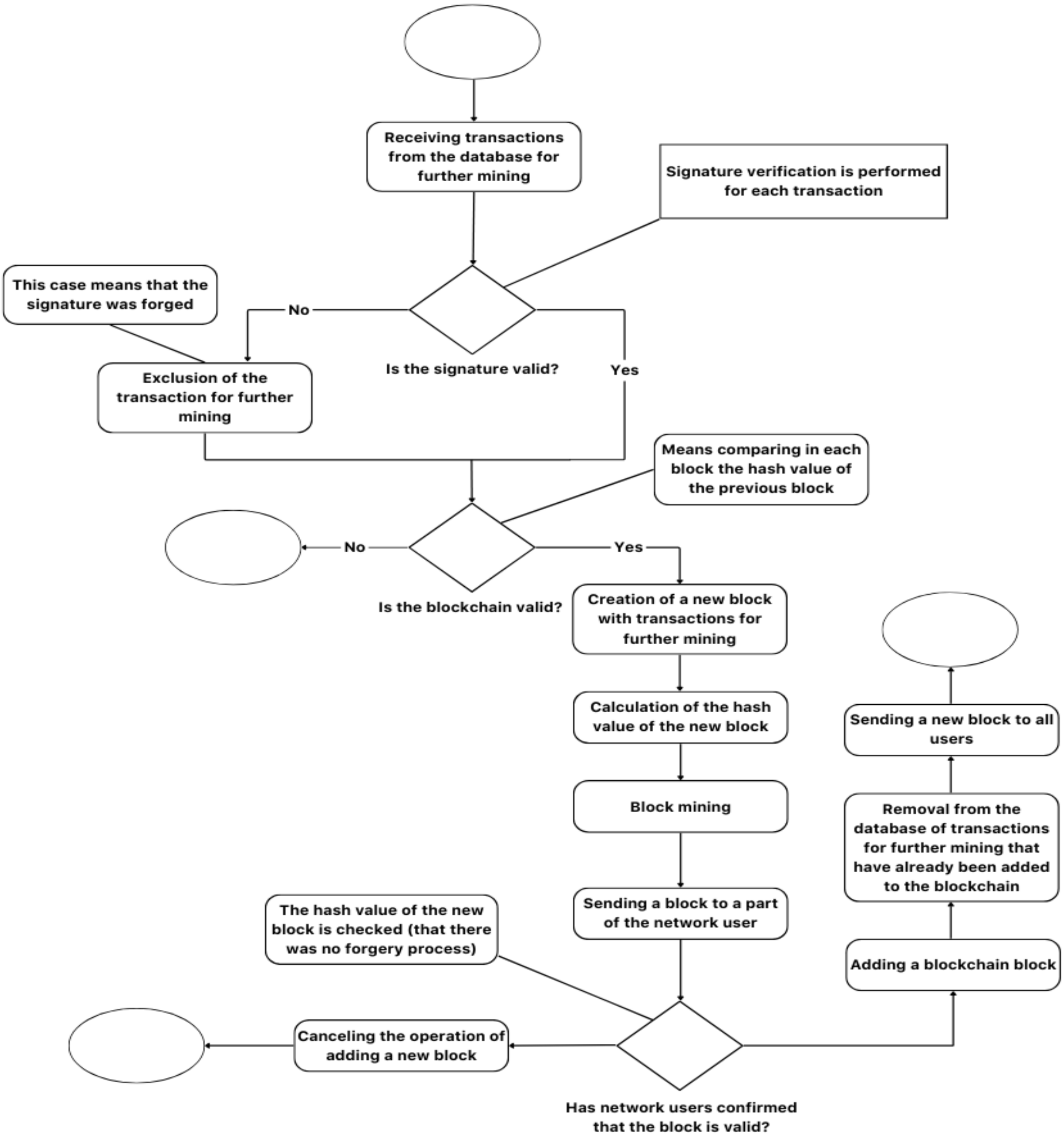

Receiving transactions from the database for further mining
Signature verification is performed for each transaction
This case means that the signature was forged
No
Is the signature valid?
Yes
Exclusion of the transaction for further mining
Means comparing in each block the hash value of the previous block
No
Yes
Is the blockchain valid?
Creation of a new block with transactions for further mining
Calculation of the hash value of the new block
Block mining
Sending a block to a part of the network user
Sending a new block to all users
Removal from the database of transactions for further mining that have already been added to the blockchain
Adding a blockchain block
The hash value of the new block is checked (that there was no forgery process)
Canceling the operation of adding a new block
Has network users confirmed that the block is valid?

Figure 4.2. The blockchain update algorithm from the beginning of the selection of transactions to the introduction of a new block into the chain

The proof-of-work mechanism, which is sometimes referred to as mining, is another essential component of blockchain technology. A variable known as difficulty is responsible for determining the ideal number of leading zeros that should be included in the hash value of each and every block. “A” other variable, which is referred to as the nonce, is involved in the computation of the hash value. A recalculation of the hash value is performed as a result of the incrementation of the nonce variable that occurs during mining. This recalculation will continue until all of the characters in the hash value that fall within the range of [0, difficulty] are completely made up of zeros. The amount of time required for mining increases exponentially with the difficulty of the task, which enables the duration of the process to be adjusted according to the computational capability of the network.

After a block has been successfully mined, it is broadcast to all or the majority of the participants in the network. Each of these participants then confirms the chain's validity by taking into consideration the newly mined block. Recalculating the hash value in each block is a necessary step in the verification process. The check is carried out on each block because each block holds both its own hash value and the hash value of the block that came before it. In the block that is now being processed, the hash value that was stored in the block that came before it is compared with the hash value that was stored in the block that came before it. On the condition that the majority of network participants (or all of them) acknowledge that the verification process was successful, the block is added to the chain, and all of the network members update the chain with the new block.

4.2.2 Program Architecture and Algorithms

The system functions as a decentralized network comprising nodes representing individual users, each of which possesses identical functionality contingent upon their role (e.g., miner or system user). An infrastructure task is executed by a solitary bootstrapper server, which ensures that users are synchronized with one another. In MongoDB terminology, the bootstrapper server houses an aggregation of users known as the "user pool".

A user must have a server running on their local workstation that receives and processes data requests (back-end server) and a server that provides the user interface (front-end server) in order to begin using the system. Within the network, two distinct user roles exist: those who are actively mining blocks and those who are engaging in the creation of transactions. Every individual occurrence of the user interface and data processing servers constitutes a network node.

A determination was reached during the architectural design phase to incorporate a dedicated server in order to allocate duties. This server has been specifically engineered to execute a single mission. The justification for this choice is to prevent the formation of excessive dependencies among code components in the event that the codebase is modified or expanded. The lack of functional separation presents difficulties in the maintenance of code. Moreover, it was determined that in the event that the blockchain lacks any blocks or the network is devoid of users, the initial block (genesis block) would be generated by the bootstrapper server.

User engagement with the bootstrapper server is intended to elicit information regarding other users on the network. The operational mechanism by which the miner and the bootstrapper server operate is analogous.

As part of their collaboration, the miner is responsible for receiving transactions submitted by the user. The miner announces the newly mined block to all nodes once it has been completed. Upon successful validation and the absence of any prior additions to the blockchain, the block is affixed. In exchange for the completed task, the miner is rewarded monetarily.

The notion of user-miner interaction requires the user to generate and distribute a transaction to all miners. The examples of the network, use case diagram, and class diagram for the automated system are presented in Figures 4.3 to 4.4.

A strategic determination was reached during the architectural design phase to implement a dedicated server for the purpose of task segregation. This server has been specifically engineered to perform a single mission. The rationale behind this decision was to prevent the codebase from becoming overly dependent on one another, which could pose difficulties in terms of maintenance during the implementation of modifications or the addition of new features. Additionally, it was determined that the bootstrapper server would produce the initial block, referred to as the genesis block, in the absence of any blocks in the blockchain or users in the network.

Data exchange occurs during the interaction between the user and the bootstrapper server in order to obtain information pertaining to other users on the network. An analogous mode of operation is discernible between the bootstrapper server and the miner.

The collaboration between a user and a miner involves the miner receiving user-generated transactions. Once a block has been mined effectively, the miner distributes the newly created block to all nodes. Appending the block to the blockchain, contingent upon its successful validation and lack of prior addition, results in the miner receiving a reward for the accomplished task.

The user-miner interaction concept revolves around the user initiating a transaction and disseminating it to all miners. Figures 4.3 to 4.6 provide visual representations of network examples, a use case diagram, and a class diagram for the automated system.

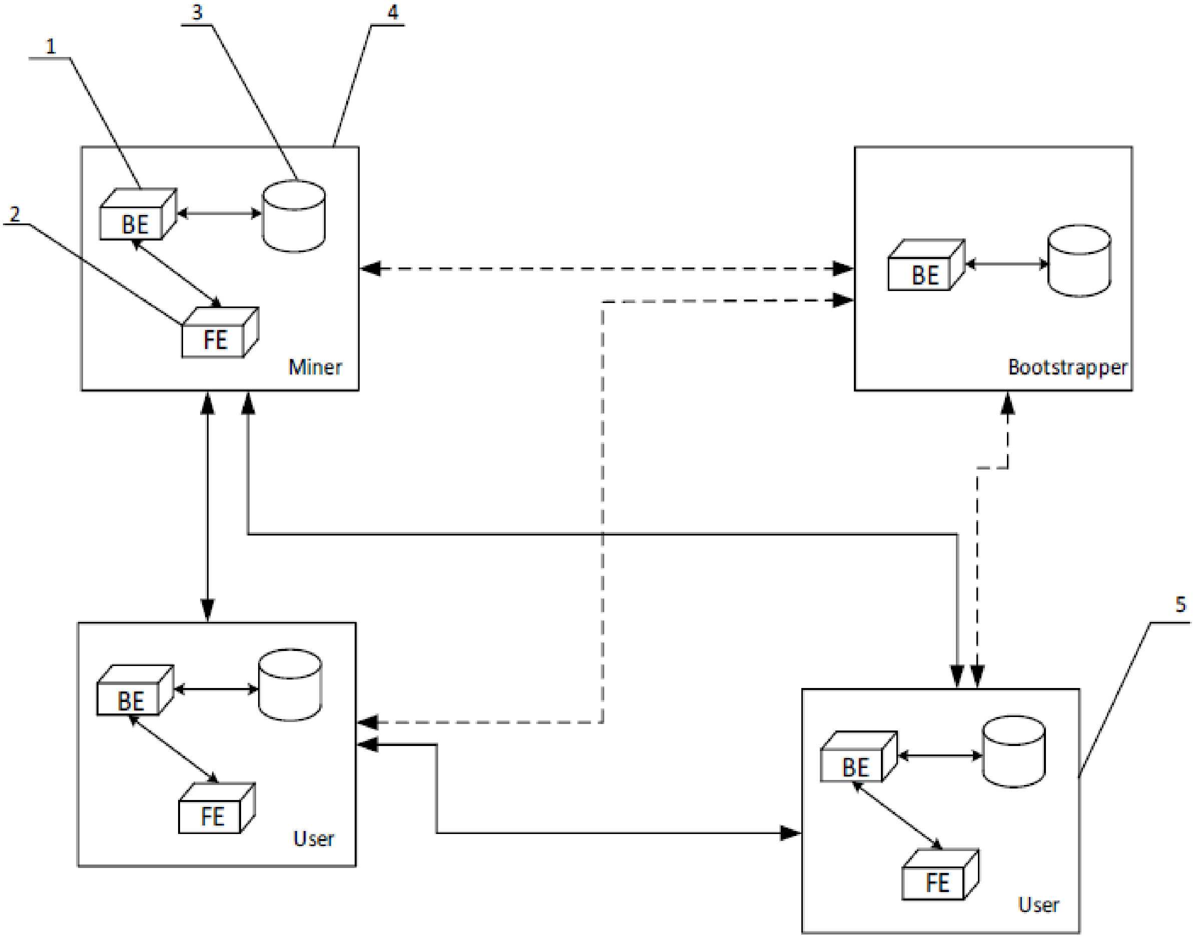
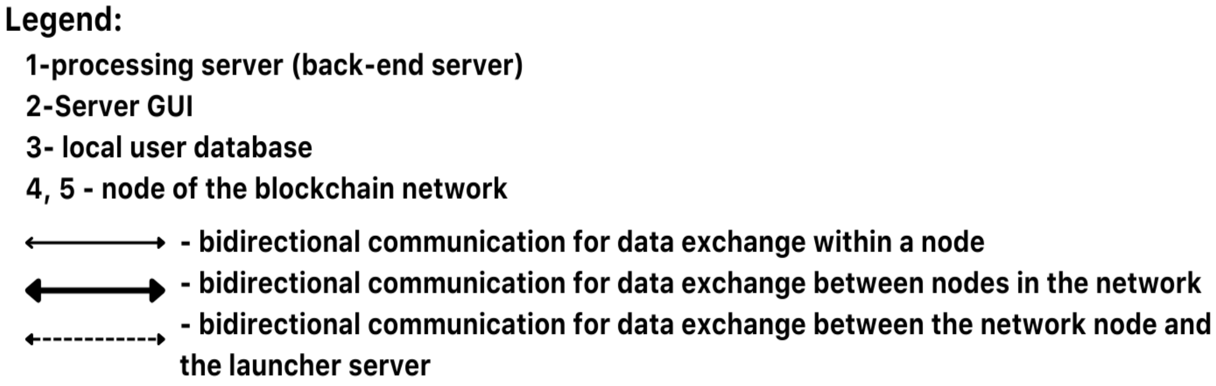


Figure 4.3. Example of a network with two users and one miner



Legend:

1-processing server (back-end server)

2-Server GUI

3- local user database

4, 5 - node of the blockchain network

⟷ - bidirectional communication for data exchange within a node

⬌ - bidirectional communication for data exchange between nodes in the network

⇠-----------⇢ - bidirectional communication for data exchange between the network node and the launcher server

Figure 4.4. Legend

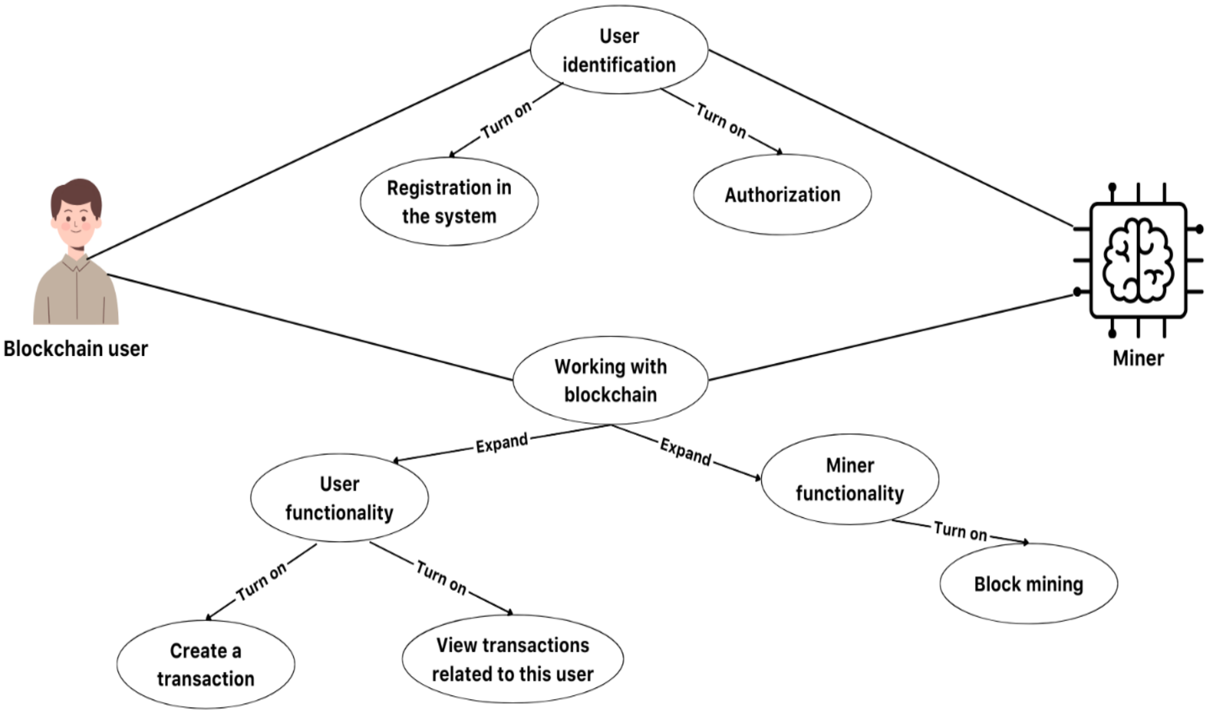


Figure 4.5. Diagram of precedents of the system being designed

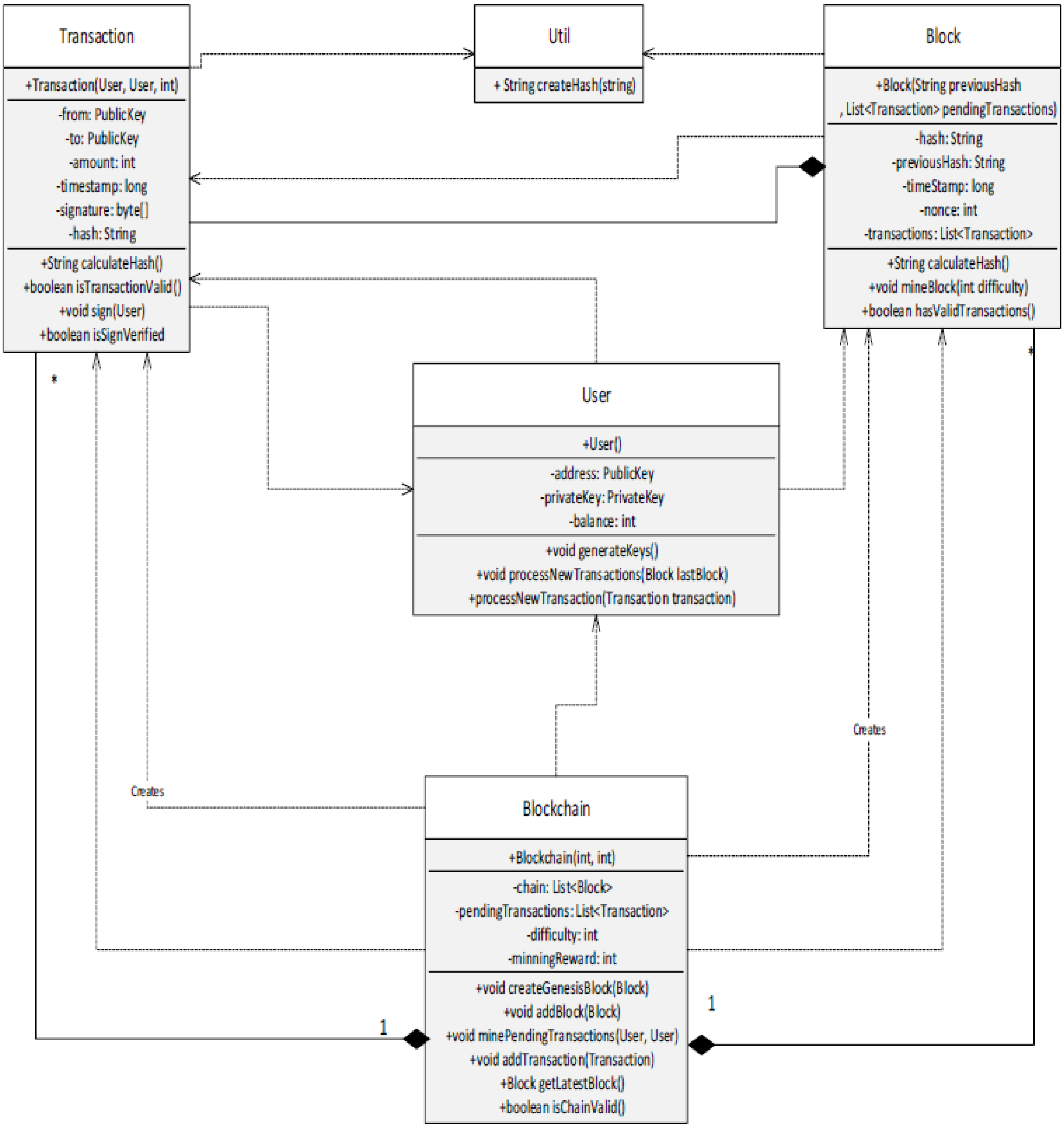
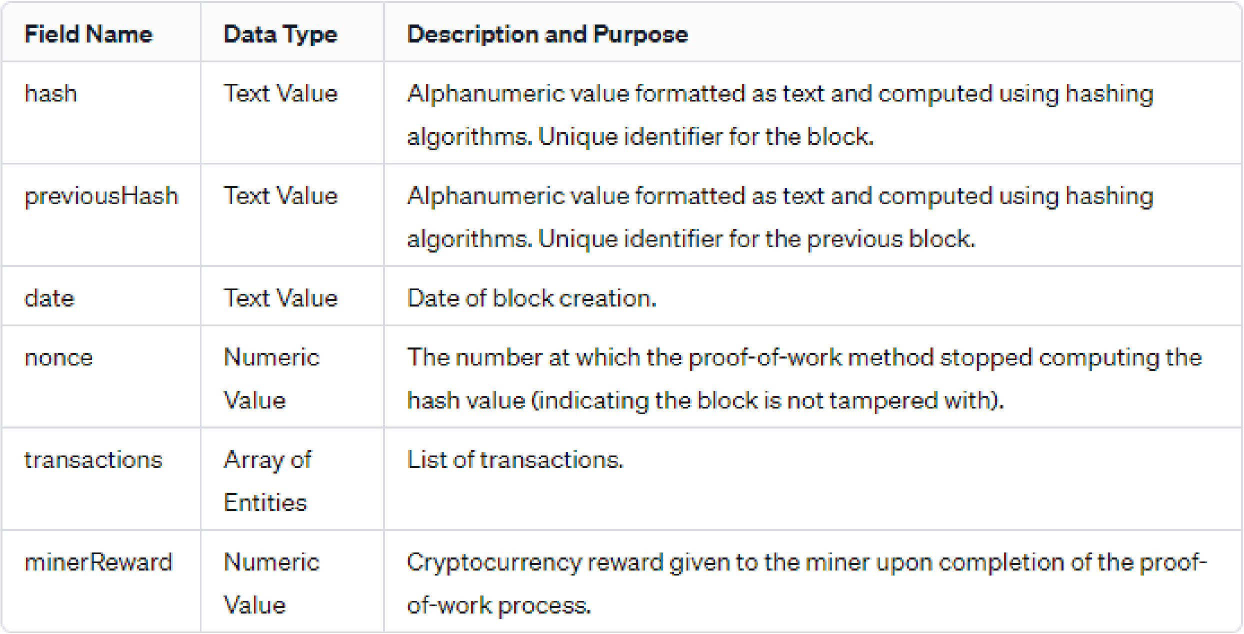


Figure 4.6. Class diagram of the designed system

The organizations comprising the blockchain are responsible for storing information and serve as the fundamental components of the system. Tables 4.1 through 4.2 present a comprehensive summary of the following entities:

Table 4.1

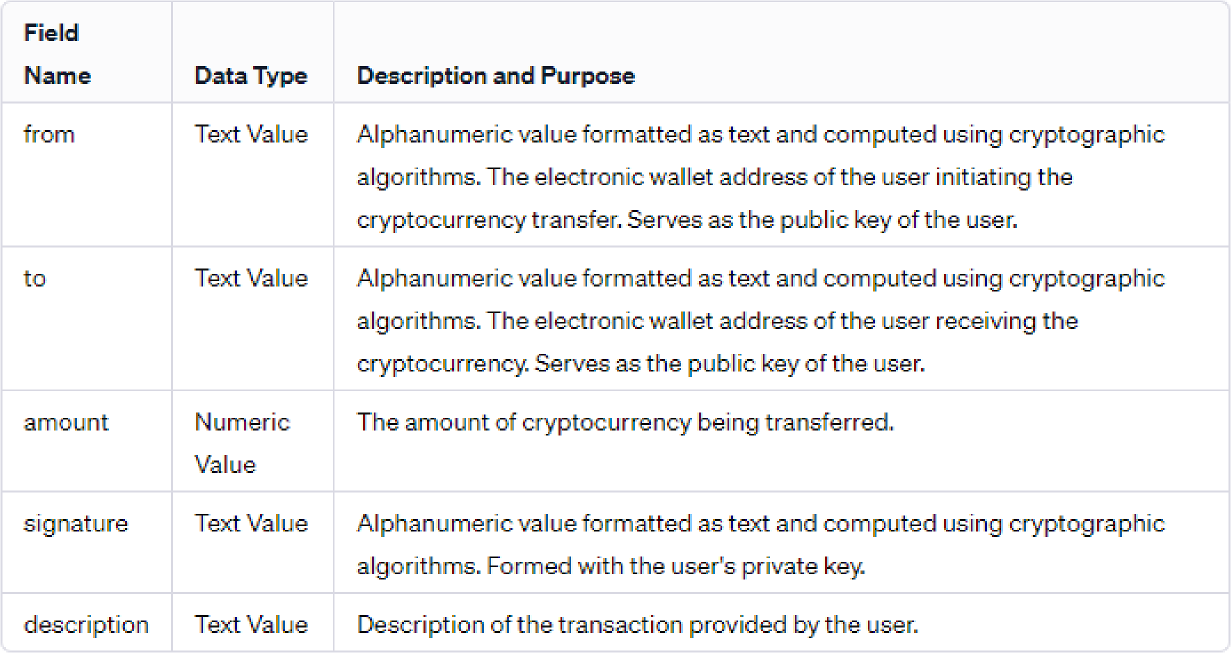
Entity "Block"



Field Name	Data Type	Description and Purpose
hash	Text Value	Alphanumeric value formatted as text and computed using hashing algorithms. Unique identifier for the block.
previousHash	Text Value	Alphanumeric value formatted as text and computed using hashing algorithms. Unique identifier for the previous block.
date	Text Value	Date of block creation.
nonce	Numeric Value	The number at which the proof-of-work method stopped computing the hash value (indicating the block is not tampered with).
transactions	Array of Entities	List of transactions.
minerReward	Numeric Value	Cryptocurrency reward given to the miner upon completion of the proof-of-work process.

Table 4.2

Entity "Transactions"



Field Name	Data Type	Description and Purpose
from	Text Value	Alphanumeric value formatted as text and computed using cryptographic algorithms. The electronic wallet address of the user initiating the cryptocurrency transfer. Serves as the public key of the user.
to	Text Value	Alphanumeric value formatted as text and computed using cryptographic algorithms. The electronic wallet address of the user receiving the cryptocurrency. Serves as the public key of the user.
amount	Numeric Value	The amount of cryptocurrency being transferred.
signature	Text Value	Alphanumeric value formatted as text and computed using cryptographic algorithms. Formed with the user's private key.
description	Text Value	Description of the transaction provided by the user.

Language features of JavaScript provide encapsulated functionality for generating private and public keys, as well as hashing information used in the project.

4.2.3 Mechanism of User Authorization and Authentication Using JSON Web Tokens

The server generates tokens based on POST requests to /signup and /login. In subsequent requests, if the server doesn't find a token, it responds with a 401 error, providing a description of the issue.

Token Verification:

Token verification involves checking the Authorization header for the presence of text. If absent, a "No token provided" message is sent. If text is present, token validation and user lookup are performed. If the process is successful, the HTTP request is executed; otherwise, it is denied.

4.2.4 Validation Algorithm for a New Block

A vital part of blockchain technology, the algorithm that verifies the existence of a new block guarantees the system's functionality and dependability. Comprehending this facet is crucial for the continued advancement and refinement of this novel methodology concerning the exchange of data and digital assets. It comprises the subsequent phases:

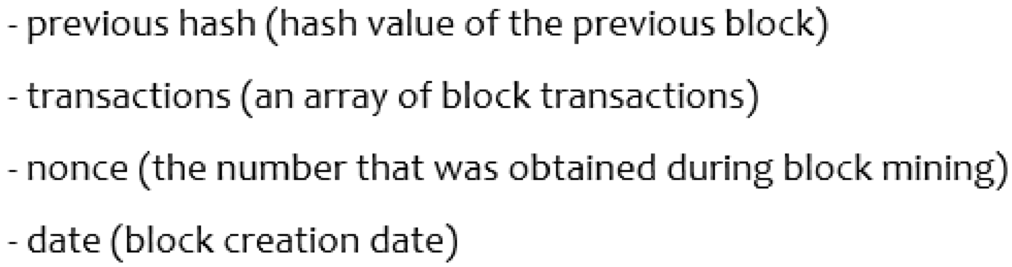
1. Consensus Determination: - This is one of the fundamental phases. A variety of techniques are utilized by distinct blockchain networks, including Proof of Work (PoW), Proof of Stake (PoS), and others.

2. Proof of Work (PoW): - Within the Proof of Work (PoW) framework, miners compete to resolve intricate mathematical challenges, with the initial solver being granted privileges to append a new block. This procedure demands substantial computational resources.

3. Proof of Stake (PoS): - Participants who hold a specific quantity of cryptocurrency are granted the privilege to generate new blocks in an equivalent manner to their ownership in the PoS system. While this approach conserves energy, it does demand a degree of confidence from the participants.

The following conditions must be fulfilled for a block to be deemed valid: - The hash value of the prior block must be identical to the hash value of the new block.

• The hash value entered in the new block must correspond to the hash value recalculated using the data in the block.



- previous hash (hash value of the previous block)
- transactions (an array of block transactions)
- nonce (the number that was obtained during block mining)
- date (block creation date)

Figure 4.7. Hash value

Under the condition that these two criteria are met, the new block is considered valid, untampered, and can be added to the blockchain.

4.3 User Interaction with the Software System

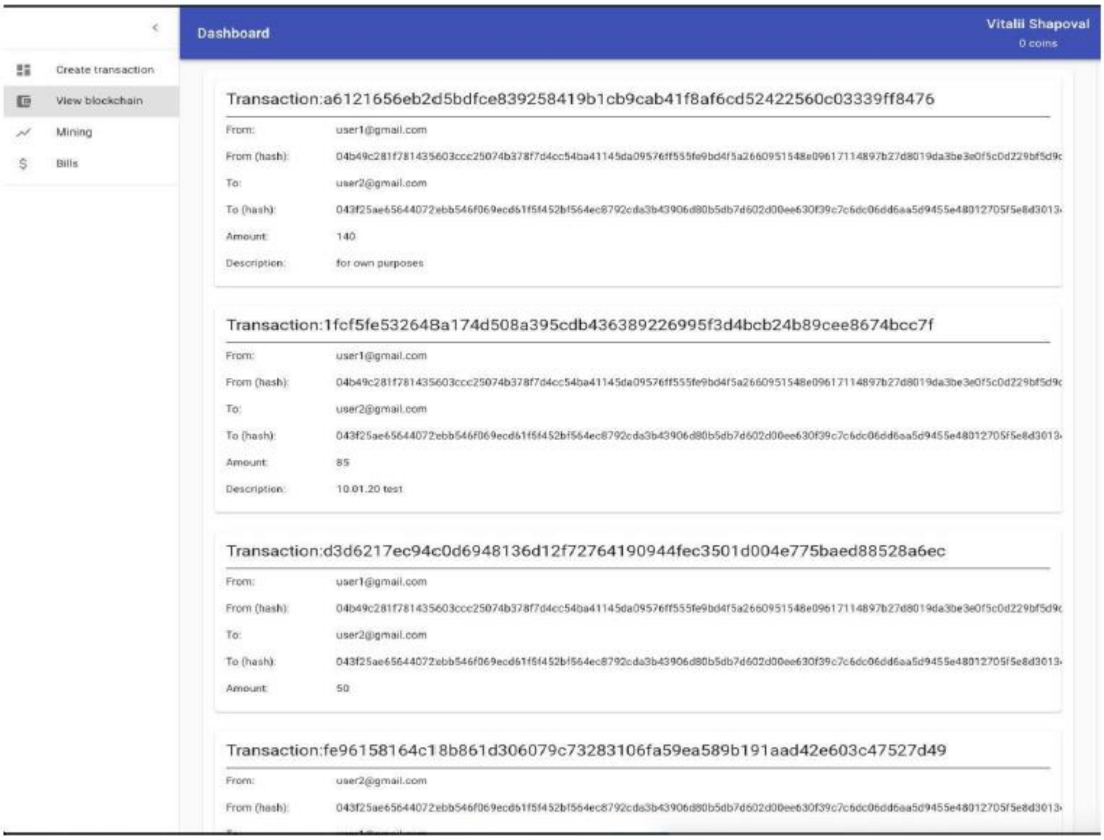
This section illustrates the process of creating a transaction and entering new information into the blockchain through the user interface and the database.

4.3.1 Requirements for Additional Software

Working with the blockchain imposes performance requirements on hardware. The minimum requirements include an Intel Core i3 processor, 8 GB of RAM, and 256 GB of free space on the hard drive. Additionally, MongoDB and NPM need to be installed for storing the blockchain locally and running the servers.

4.3.2 Program Execution Results

Upon successful registration and login, users are granted access to a journal of initiated transactions, which details the actions executed by all other users. This information is accessible via the "View blockchain" tab. The transaction log provides information including the transaction's sender and recipient, the amount transferred, and the hash value of the electronic wallets used by the users (Figure 4.8).



Transaction:a6121656eb2d5bdfce839258419b1cb9cab41f8af6cd52422560c03339ff8476

From:	user1@gmail.com
From (hash):	04b49c281f781435603ccc25074b378f7d4cc54ba41145da09576ff555fe9bd4f5a2660951548e09617114897b27d8019da3be3e0f5c0d229bf5d9c
To:	user2@gmail.com
To (hash):	043f25ae65644072ebb546f069ecd61f5f452bf564ec8792cda3b43906d80b5db7d602d00ee630f39c7c6dc06dd6aa5d9455e48012705f5e8d3013
Amount:	140
Description:	for own purposes

Transaction:1fcf5fe532648a174d508a395cdb436389226995f3d4bcb24b89cee8674bcc7f

From:	user1@gmail.com
From (hash):	04b49c281f781435603ccc25074b378f7d4cc54ba41145da09576ff555fe9bd4f5a2660951548e09617114897b27d8019da3be3e0f5c0d229bf5d9c
To:	user2@gmail.com
To (hash):	043f25ae65644072ebb546f069ecd61f5f452bf564ec8792cda3b43906d80b5db7d602d00ee630f39c7c6dc06dd6aa5d9455e48012705f5e8d3013
Amount:	85
Description:	10.01.20 test

Transaction:d3d6217ec94c0d6948136d12f72764190944fec3501d004e775baed88528a6ec

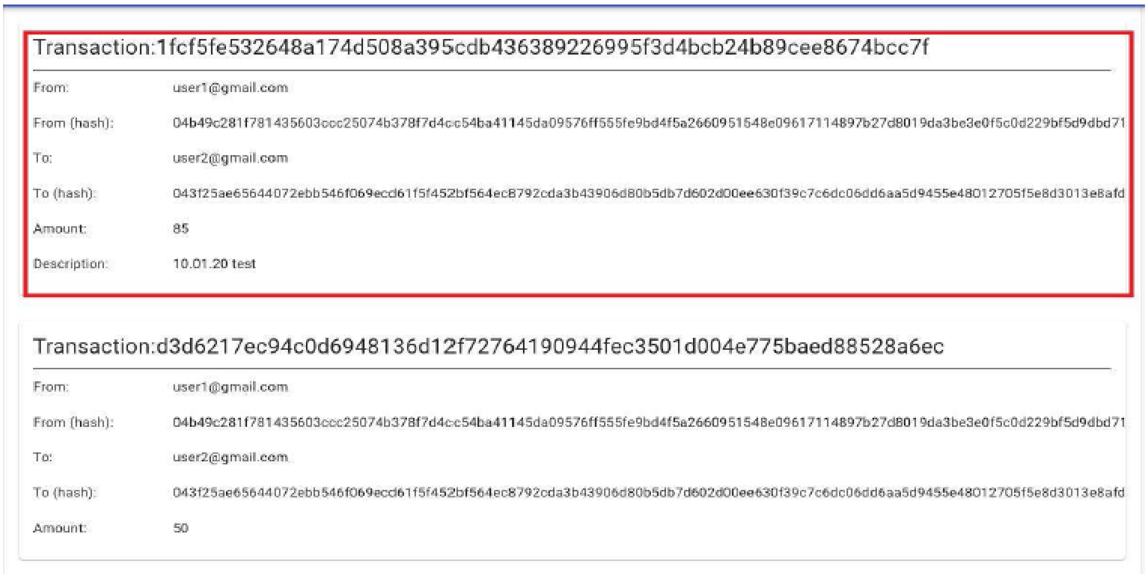
From:	user1@gmail.com
From (hash):	04b49c281f781435603ccc25074b378f7d4cc54ba41145da09576ff555fe9bd4f5a2660951548e09617114897b27d8019da3be3e0f5c0d229bf5d9c
To:	user2@gmail.com
To (hash):	043f25ae65644072ebb546f069ecd61f5f452bf564ec8792cda3b43906d80b5db7d602d00ee630f39c7c6dc06dd6aa5d9455e48012705f5e8d3013
Amount:	50

Transaction:fe96158164c18b861d306079c73283106fa59ea589b191aad42e603c47527d49

From:	user2@gmail.com
From (hash):	043f25ae65644072ebb546f069ecd61f5f452bf564ec8792cda3b43906d80b5db7d602d00ee630f39c7c6dc06dd6aa5d9455e48012705f5e8d3013

Figure 4.8. Transaction list page

Until the moment of creating a new transaction and its mining, the table that stores them is represented in Figure 4.9.



Transaction:1fcf5fe532648a174d508a395cdb436389226995f3d4bcb24b89cee8674bcc7f

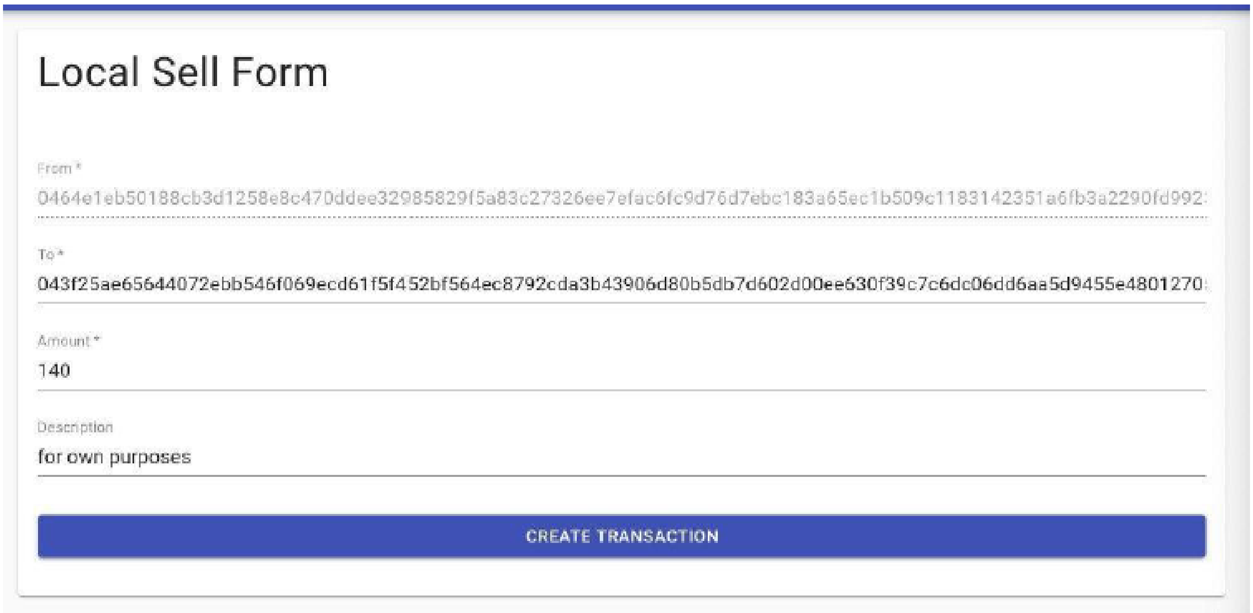
From:	user1@gmail.com
From (hash):	04b49c281f781435603ccc25074b378f7d4cc54ba41145da09576ff555fe9bd4f5a2660951548e09617114897b27d8019da3be3e0f5c0d229bf5d9dbd71
To:	user2@gmail.com
To (hash):	043f25ae65644072ebb546f069ecd61f5f452bf564ec8792cda3b43906d80b5db7d602d00ee630f39c7c6dc06dd6aa5d9455e48012705f5e8d3013e8afd
Amount:	85
Description:	10.01.20 test

Transaction:d3d6217ec94c0d6948136d12f72764190944fec3501d004e775baed88528a6ec

From:	user1@gmail.com
From (hash):	04b49c281f781435603ccc25074b378f7d4cc54ba41145da09576ff555fe9bd4f5a2660951548e09617114897b27d8019da3be3e0f5c0d229bf5d9dbd71
To:	user2@gmail.com
To (hash):	043f25ae65644072ebb546f069ecd61f5f452bf564ec8792cda3b43906d80b5db7d602d00ee630f39c7c6dc06dd6aa5d9455e48012705f5e8d3013e8afd
Amount:	50

Figure 4.9. The last block (highlighted in red) before mining a new block presented in the graphical interface

In the event that a user wishes to initiate a new transfer, they need to navigate to the "Create transaction" tab (Figure 4.10), specify the hash value of the electronic wallet, the transfer amount, and a brief description of the transaction if necessary.



Local Sell Form

From *
0464e1eb50188cb3d1258e8c470ddee32985829f5a83c27326ee7efac6fc9d76d7ebc183a65ec1b509c1183142351a6fb3a2290fd992

To *
043f25ae65644072ebb546f069ecd61f5f452bf564ec8792cda3b43906d80b5db7d602d00ee630f39c7c6dc06dd6aa5d9455e4801270

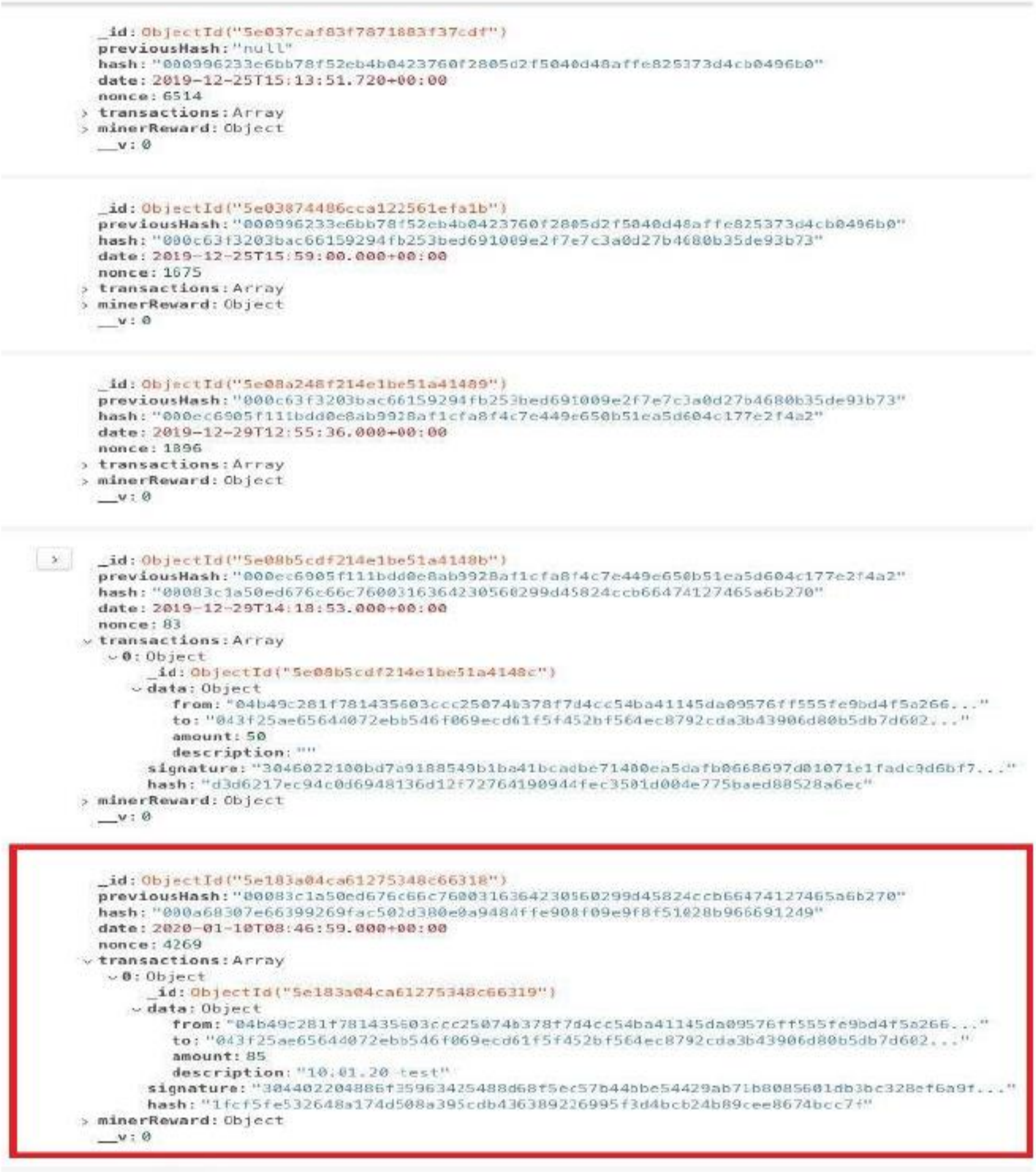
Amount *
140

Description
for own purposes

Figure 4.10. Transaction creation page

Once a transaction is initiated by the user, it is added to the transaction pool where it awaits mining.

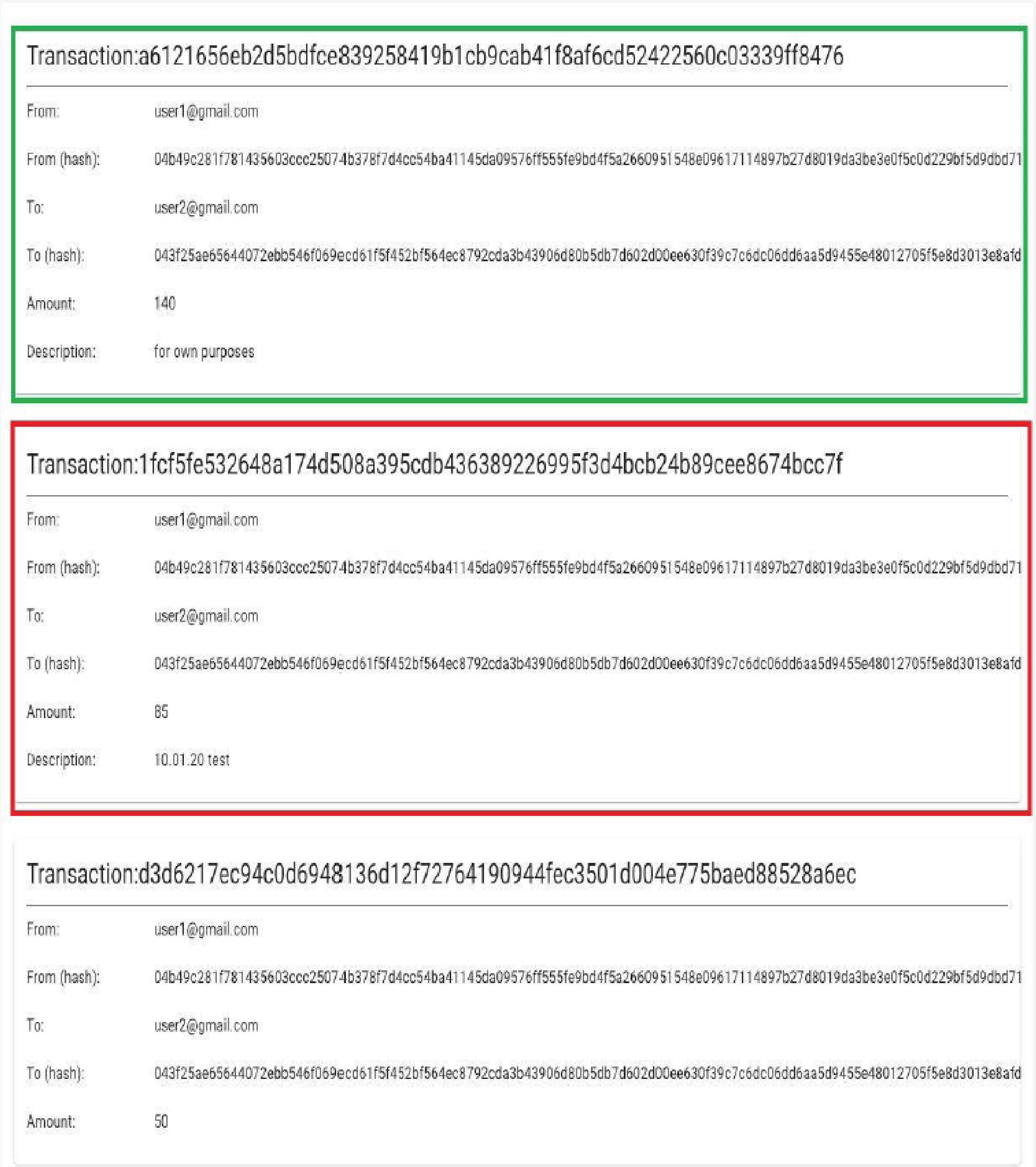
The database prior to the block mining process is depicted in Figure 4.11. The collection comprises every block, containing its hash value, the previous block's hash value, the date of block creation, the nonce value signifying the completion of block mining, and a collection of transactions.



```
  _id: ObjectId("5e037caf83f7871883f37cdf")
  previousHash: "null"
  hash: "000996233e6bb78f52eb4b0423760f2805d2f5040d48affe825373d4cb0496b0"
  date: 2019-12-25T15:13:51.720+00:00
  nonce: 6514
> transactions: Array
> minerReward: Object
  __v: 0

  _id: ObjectId("5e03874486cca122561efa1b")
  previousHash: "000996233e6bb78f52eb4b0423760f2805d2f5040d48affe825373d4cb0496b0"
  hash: "000c63f3203bac66159294fb253bed691009e2f7e7c3a0d27b4680b35de93b73"
  date: 2019-12-25T15:59:00.000+00:00
  nonce: 1675
> transactions: Array
> minerReward: Object
  __v: 0

  _id: ObjectId("5e08a248f214e1be51a41489")
  previousHash: "000c63f3203bac66159294fb253bed691009e2f7e7c3a0d27b4680b35de93b73"
  hash: "000ec6905f111bdd0e8ab9928af1cfa8f4c7e449e650b51ea5d604c177e2f4a2"
  date: 2019-12-29T12:55:36.000+00:00
  nonce: 1896
> transactions: Array
> minerReward: Object
  __v: 0

  _id: ObjectId("5e08b5cdf214e1be51a4148b")
  previousHash: "000ec6905f111bdd0e8ab9928af1cfa8f4c7e449e650b51ea5d604c177e2f4a2"
  hash: "00083c1a50ed676c66c7600316364230560299d45824ccb66474127465a6b270"
  date: 2019-12-29T14:18:53.000+00:00
  nonce: 83
v transactions: Array
  v 0: Object
       _id: ObjectId("5e08b5cdf214e1be51a4148c")
    v data: Object
         from: "04b49c281f781435603ccc25074b378f7d4cc54ba41145da09576ff555fe9bd4f5a266..."
         to: "043f25ae65644072ebb546f069ecd61f5f452bf564ec8792cda3b43906d80b5db7d602..."
         amount: 50
         description: ""
       signature: "3046022100bd7a9188549b1ba41bcadbe71400ea5dafb0668697d01071e1fadc9d6bf7..."
       hash: "d3d6217ec94c0d6948136d12f72764190944fec3501d004e775baed88528a6ec"
> minerReward: Object
  __v: 0

  _id: ObjectId("5e183a04ca61275348c66318")
  previousHash: "00083c1a50ed676c66c7600316364230560299d45824ccb66474127465a6b270"
  hash: "000a68307e66399269fac502d380e0a9484ffe908f09e9f8f51028b966691249"
  date: 2020-01-10T08:46:59.000+00:00
  nonce: 4269
v transactions: Array
  v 0: Object
       _id: ObjectId("5e183a04ca61275348c66319")
    v data: Object
         from: "04b49c281f781435603ccc25074b378f7d4cc54ba41145da09576ff555fe9bd4f5a266..."
         to: "043f25ae65644072ebb546f069ecd61f5f452bf564ec8792cda3b43906d80b5db7d602..."
         amount: 85
         description: "10.01.20 test"
       signature: "304402204886f35963425488d68f5ec57b44bbe54429ab71b8085601db3bc328ef6a9f..."
       hash: "1fcf5fe532648a174d508a395cdb436389226995f3d4bcb24b89cee8674bcc7f"
> minerReward: Object
  __v: 0
```

Figure 4.11. The last block (highlighted in red) before mining a new block presented in the database

After successfully mining a new block, the transaction will appear in the "View blockchain" window (Figure 4.12).



Transaction:a6121656eb2d5bdfce839258419b1cb9cab41f8af6cd52422560c03339ff8476

From: user1@gmail.com

From (hash): 04b49c281f781435603ccc25074b378f7d4cc54ba41145da09576ff555fe9bd4f5a2660951548e09617114897b27d8019da3be3e0f5c0d229bf5d9dbd71

To: user2@gmail.com

To (hash): 043f25ae65644072ebb546f069ecd61f5f452bf564ec8792cda3b43906d80b5db7d602d00ee630f39c7c6dc06dd6aa5d9455e48012705f5e8d3013e8afd

Amount: 140

Description: for own purposes

Transaction:1fcf5fe532648a174d508a395cdb436389226995f3d4bcb24b89cee8674bcc7f

From: user1@gmail.com

From (hash): 04b49c281f781435603ccc25074b378f7d4cc54ba41145da09576ff555fe9bd4f5a2660951548e09617114897b27d8019da3be3e0f5c0d229bf5d9dbd71

To: user2@gmail.com

To (hash): 043f25ae65644072ebb546f069ecd61f5f452bf564ec8792cda3b43906d80b5db7d602d00ee630f39c7c6dc06dd6aa5d9455e48012705f5e8d3013e8afd

Amount: 85

Description: 10.01.20 test

Transaction:d3d6217ec94c0d6948136d12f72764190944fec3501d004e775baed88528a6ec

From: user1@gmail.com

From (hash): 04b49c281f781435603ccc25074b378f7d4cc54ba41145da09576ff555fe9bd4f5a2660951548e09617114897b27d8019da3be3e0f5c0d229bf5d9dbd71

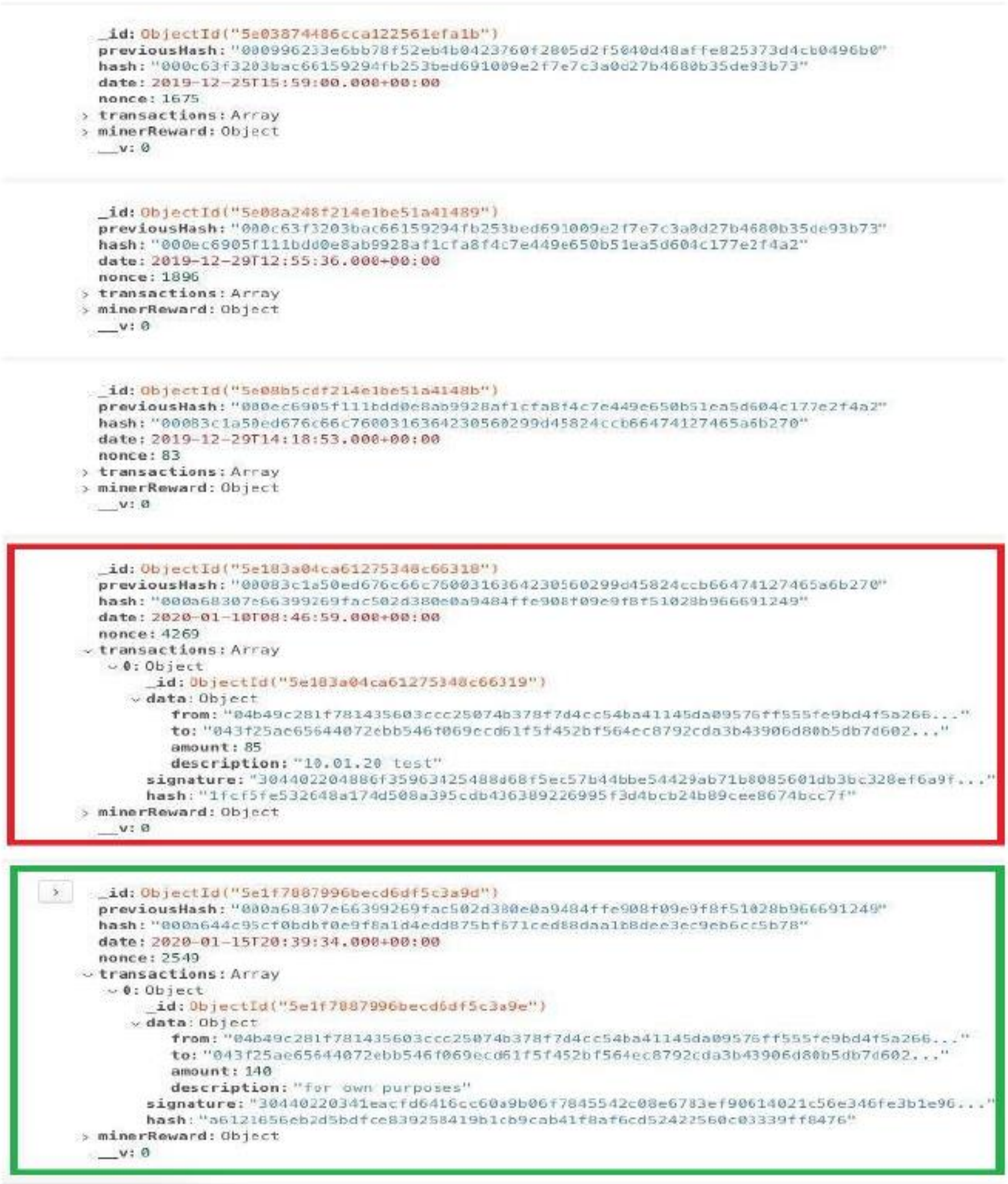
To: user2@gmail.com

To (hash): 043f25ae65644072ebb546f069ecd61f5f452bf564ec8792cda3b43906d80b5db7d602d00ee630f39c7c6dc06dd6aa5d9455e48012705f5e8d3013e8afd

Amount: 50

Figure 4.12. The last block (highlighted in green) and the penultimate block (highlighted in red) after mining the new block presented in the GUI

Figure 4.13 illustrates the replica of the database that is created after mining a new block by the blockchain. Please take note that the "previousHash" field of the bottom block and the "hash" field of the penultimate block are identical. This is something that should be taken into consideration. It is the application of this idea that makes it possible to organize the blockchain.



```
  _id: ObjectId("5e03874486cca122561efa1b")
  previousHash: "000996233e6bb78f52eb4b0423760f2805d2f5040d48affe825373d4cb0496b0"
  hash: "000c63f3203bac66159294fb253bed691009e2f7e7c3a0d27b4680b35de93b73"
  date: 2019-12-25T15:59:00.000+00:00
  nonce: 1675
> transactions: Array
> minerReward: Object
  __v: 0

  _id: ObjectId("5e08a248f214e1be51a41489")
  previousHash: "000c63f3203bac66159294fb253bed691009e2f7e7c3a0d27b4680b35de93b73"
  hash: "000ec6905f111bdd0e8ab9928af1cfa8f4c7e449e650b51ea5d604c177e2f4a2"
  date: 2019-12-29T12:55:36.000+00:00
  nonce: 1896
> transactions: Array
> minerReward: Object
  __v: 0

  _id: ObjectId("5e08b5cdf214e1be51a4148b")
  previousHash: "000ec6905f111bdd0e8ab9928af1cfa8f4c7e449e650b51ea5d604c177e2f4a2"
  hash: "00083c1a50ed676c66c76003163642305602 99d45824ccb66474127465a6b270"
  date: 2019-12-29T14:18:53.000+00:00
  nonce: 83
> transactions: Array
> minerReward: Object
  __v: 0

  _id: ObjectId("5e183a04ca61275348c66318")
  previousHash: "00083c1a50ed676c66c760031636423056029 9d45824ccb66474127465a6b270"
  hash: "000a68307e66399269fac502d380e0a9484ffe908f09e9f8f51028b966691249"
  date: 2020-01-10T08:46:59.000+00:00
  nonce: 4269
v transactions: Array
  v 0: Object
      _id: ObjectId("5e183a04ca61275348c66319")
    v data: Object
        from: "04b49c281f781435603ccc25074b378f7d4cc54ba41145da09576ff555fe9bd4f5a266..."
        to: "043f25ae65644072ebb546f069ecd61f5f452bf564ec8792cda3b43906d80b5db7d602..."
        amount: 85
        description: "10.01.20 test"
      signature: "304402204886f35963425488d68f5ec57b44bbe54429ab71b8085601db3bc328ef6a9f..."
      hash: "1fcf5fe532648a174d508a395cdb436389226995f3d4bcb24b89cee8674bcc7f"
> minerReward: Object
  __v: 0

> _id: ObjectId("5e1f7887996becd6df5c3a9d")
  previousHash: "000a68307e66399269fac502d380e0a9484ffe908f09e9f8f51028b966691249"
  hash: "000a644c95cf0bdbf0e9f8a1d4edd875bf671ced88daa1b8dee3ec9eb6cc5b78"
  date: 2020-01-15T20:39:34.000+00:00
  nonce: 2549
v transactions: Array
  v 0: Object
      _id: ObjectId("5e1f7887996becd6df5c3a9e")
    v data: Object
        from: "04b49c281f781435603ccc25074b378f7d4cc54ba41145da09576ff555fe9bd4f5a266..."
        to: "043f25ae65644072ebb546f069ecd61f5f452bf564ec8792cda3b43906d80b5db7d602..."
        amount: 140
        description: "for own purposes"
      signature: "30440220341eacfd6416cc60a9b06f7845542c08e6783ef90614021c56e346fe3b1e96..."
      hash: "a6121656eb2d5bdfce839258419b1cb9cab41f8af6cd52422560c03339ff8476"
> minerReward: Object
  __v: 0
```

Figure 4.13. The last block (highlighted in green) and the penultimate block (highlighted in red) after mining the new block presented in the database

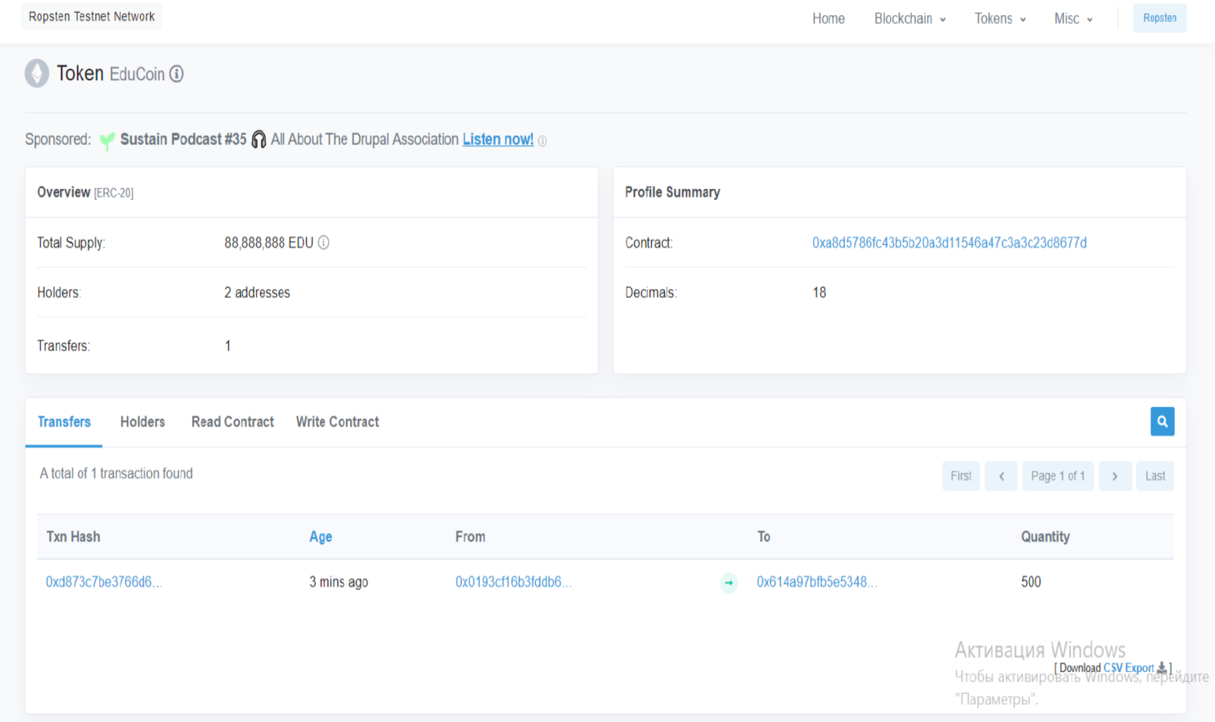
4.3.2.1 Token Creation

The EDUcoin cryptocurrency is a crypto asset that enables transactions in the same manner as a conventional cryptocurrency, such as having a defined emission volume and the ability to be divided.

In order to facilitate the implementation of smart contracts in an easy and expedient manner, the EduCoin token is generated by employing the Solidity programming language through the Truffle Framework.

Ethereum is the most well-known and largest open-type platform that has proved stability over a lengthy period of time. As a result, I decided to use Ethereum as the blockchain platform for my token. The development of smart contracts and decentralized applications (dapps) has been made possible by Ethereum, which eliminates the possibility of fraud, control, or interference from other parties.

To deploy the ERC20 standard token, I needed to create an Ethereum wallet (I used MetaMask) and obtain an INFURA API key through https://infura.io. INFURA is an Ethereum network access package that provides API access. After successfully deploying the smart contract, we obtain its key: 0xa9b5786fc46b6b20a3b11546a47c3a6c23d8677b, and the token appears on the website https://ropsten.etherscan.io/ (Figure 4.14).



Token EduCoin

Sponsored: Sustain Podcast #35 All About The Drupal Association Listen now!

Overview [ERC-20]	
Total Supply:	88,888,888 EDU
Holders:	2 addresses
Transfers:	1

Profile Summary	
Contract:	0xa8d5786fc43b5b20a3d11546a47c3a3c23d8677d
Decimals:	18

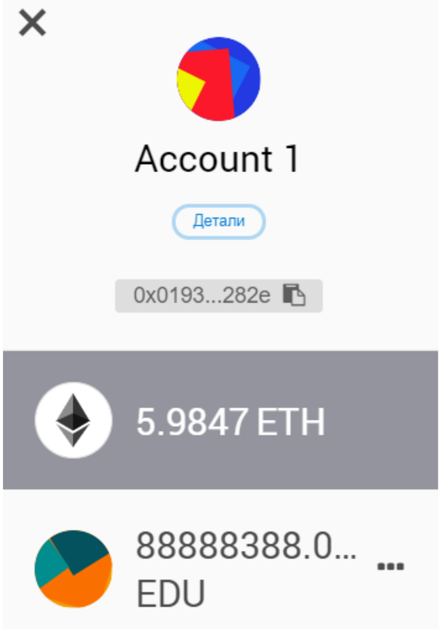
A total of 1 transaction found

Txn Hash	Age	From		To	Quantity
0xd873c7be3766d6...	3 mins ago	0x0193cf16b3fddb6...	→	0x614a97bfb5e5348...	500

[Download CSV Export]

Figure 4.14. Token Page

And the tokens appear in the wallet of the owner of this contract (Figure 4.15).



Account 1

Детали

0x0193...282e

5.9847 ETH

88888388.0... EDU

Figure 4.15. Cryptocurrency Owner's Balance

4.3.2.1 Web Application Creation

The Meteor framework, which is based on the MongoDB platform, is the one that I determined to use for my application. The fact that this framework comes with built-in packages for establishing authorization, in addition to a wealth of other helpful packages, makes it an extremely convenient framework.

Both user authentication (shown in Figure 4.16), as well as registration (shown in Figure 4.17), are included in the application. Figure 4.18 shows that the user profile includes all of the required information, as well as the ability to connect to the MetaMask wallet in order to get a public key for the purpose of conducting token withdrawals.

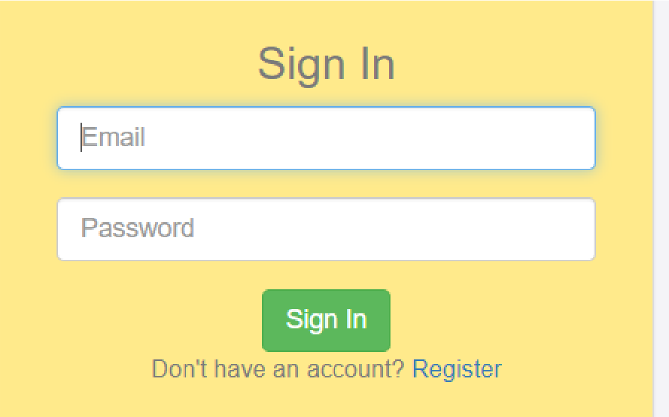


Figure 4.16. Authorization

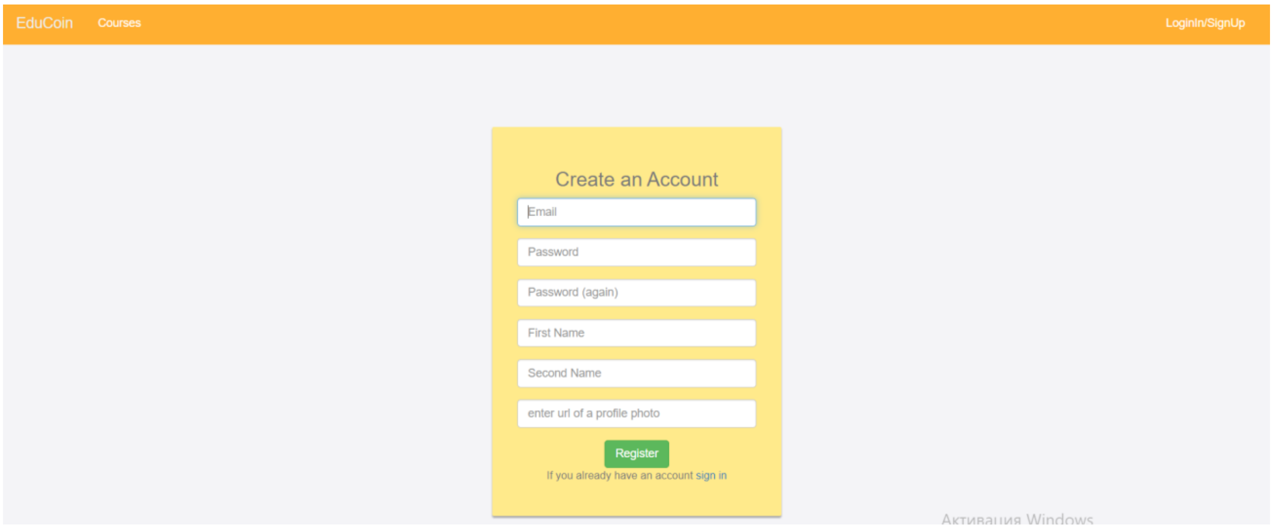
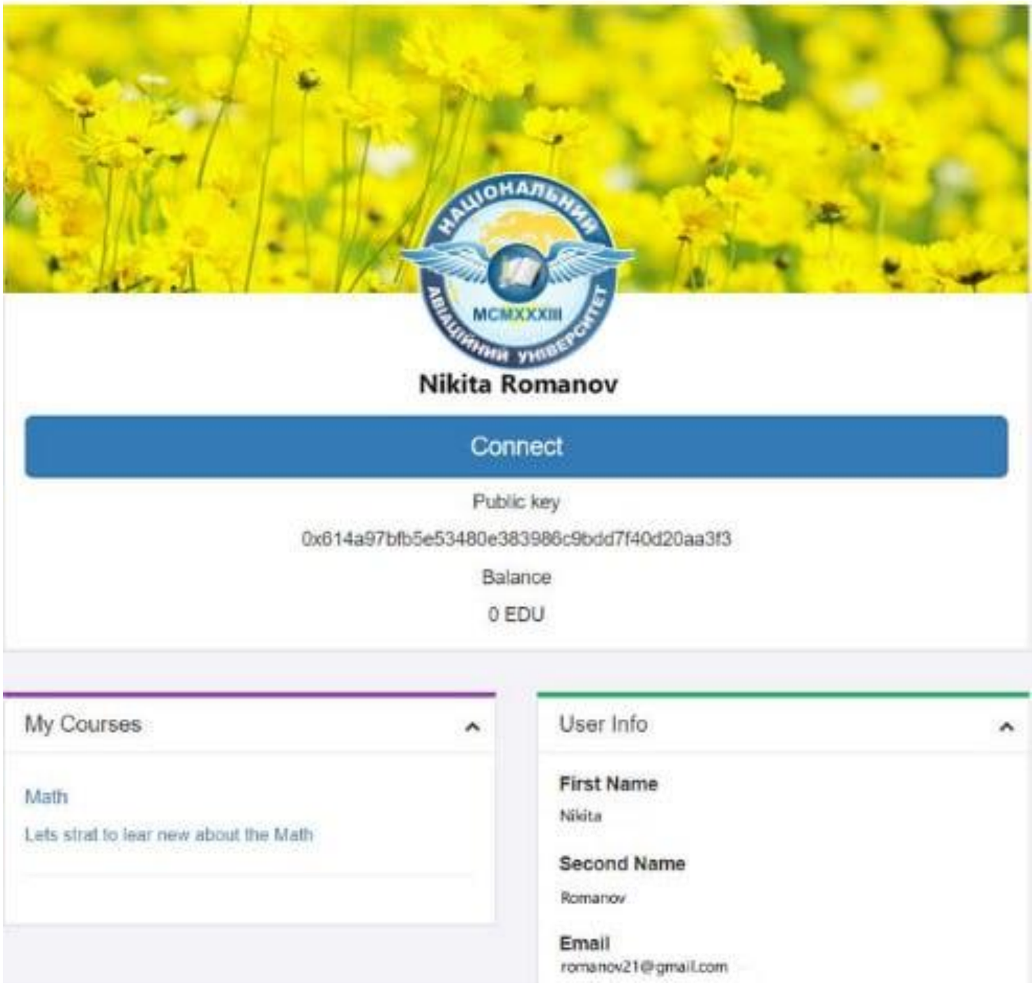


Figure 4.17. Registration



Nikita Romanov

Public key
0x614a97bfb5e53480e383986c9bdd7f40d20aa3f3

Balance
0 EDU

Math
Lets strat to lear new about the Math

First Name
Nikita

Second Name
Romanov

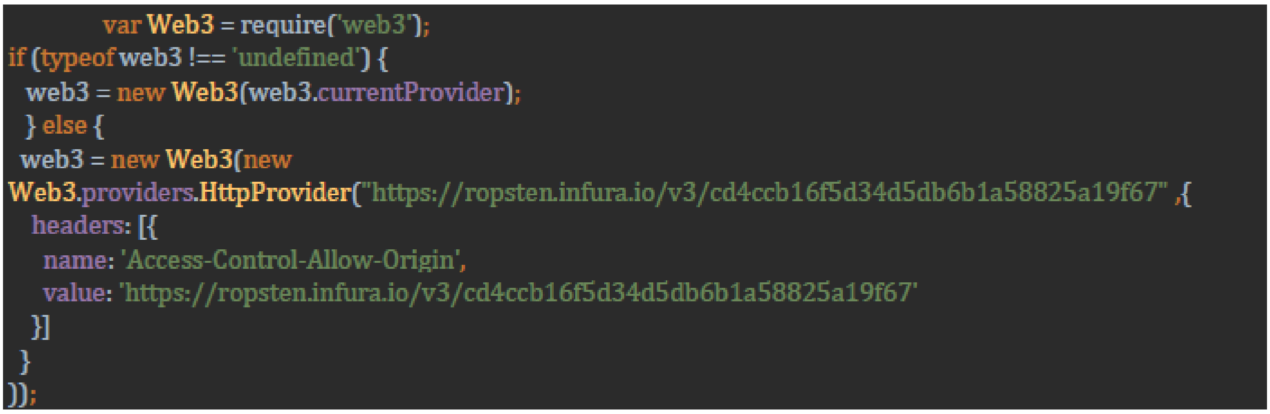
Email
romanov21@gmail.com

Figure 4.18. User Profile

Utilizing the Web3.js package is required in order to establish a connection to MetaMask and engage in interactions with Ethereum on the web page. Before you can incorporate this library into the Meteor project, you will first need to install the package by giving the following command:

- meteor add ethereum:web3

After that, you need to create an instance and configure the provider.



```
        var Web3 = require('web3');
if (typeof web3 !== 'undefined') {
  web3 = new Web3(web3.currentProvider);
  } else {
 web3 = new Web3(new
Web3.providers.HttpProvider("https://ropsten.infura.io/v3/cd4ccb16f5d34d5db6b1a58825a19f67" ,{
   headers: [{
     name: 'Access-Control-Allow-Origin',
     value: 'https://ropsten.infura.io/v3/cd4ccb16f5d34d5db6b1a58825a19f67'
   }]
  }
}));
```

Figure 4.19. Code Example

Every single user who successfully completes the course that was paid with cryptocurrency is eligible to get a prize. Additionally, in the not-too-distant future, a referral system will be implemented, which will result in the user generating additional cash from the activities of each participant who is invited to participate.

CONCLUSIONS FOR CHAPTER 4

The purpose of this chapter is to delve into the complexities involved in designing and effectively executing the proposed concepts in the Internet of Things (IoT) area by utilizing Blockchain technology. To lay the groundwork for the development of the software implementation, a comprehensive analysis of development tools, such as Mongo DB and the Java Programming Language, is required.

A comprehensive description of the Blockchain algorithm that is used in the automated resource accounting system is provided, which includes the particulars of the program architecture and algorithms. One of the most important components of the security system is the user permission and authentication method that makes use of JSON Web Tokens. This mechanism receives special careful attention.

Insights into the user's engagement with the software system are also supplied, together with the requirements for more software and program execution outcomes, with a special emphasis on the production of tokens and online applications.

The results of Chapter 4 define the practical aspect of the study by demonstrating the concrete capabilities of the algorithms and concepts that were developed in the context of real-world settings. The purpose of this chapter is to act as a significant step in improving Internet of Things systems by utilizing Blockchain technology. It also establishes the path that will be followed for further investigation and improvement.

CHAPTER 5
LABOR PROTECTION

The result of this thesis is a developed schematic diagram of switching equipment for optimizing traffic flows.

The subject of the thesis is an engineer-designer who develops and analyzes the schematic diagram of a cable digital television subscriber receiver.

The design engineer's workplace is located in the design department on the second floor.

5.1. Analysis of dangerous and harmful factors affecting the engineer

The design department is located on the second floor of a five-story building. The room has the following dimensions: length 8 m, width 4 m, height 4. The total area is 32 m^2, the total volume is 128 m^3. The department has 5 workstations for design engineers equipped with computers.

The working area of one employee is:

$$S_{\text{роб}} = \frac{S_{\text{заг.пл}}}{N} = \frac{32}{5} = 6{,}4\ \text{м}^2$$

The workload of one employee:

$$V_{\text{роб}} = \frac{V_{\text{заг.об}}}{N} = \frac{128}{5} = 25{,}6\ \text{м}^3$$

N is the number of employees in the department

$S_{\text{заг.пл}}$ - total area;

$V_{\text{заг.об}}$ - total volume.

According to [1], the area per workstation should be at least 6 m^2, and the volume should be at least 20 m^3. The workplace of the design engineer meets the requirements.

In the design department of a design engineer there are: computers, a printer. In this room, the air temperature in the warm season is 30°CCelsius, natural and artificial lighting is used. The artificial lighting is in the form of intermittent lines of LED lamps. The noise level in the room is 54 dB, and according to the State Sanitary Standards [2] it should not exceed 50 dB.

The workstation is located so that natural light falls from the left side, with a distance of 1 m with light to the workstation. The height of the work surface of the table above the floor is 750 mm, the depth of the table is 800 mm, and the width of the table is 1300 mm. The desk has a 650 mm high and 600 mm wide legroom.

List of harmful and dangerous production factors.

The creation of favorable working conditions in the work of a design engineer is of great importance both for facilitating and increasing labor productivity. According to [3], harmful production factors are:

1. Elevated temperature of the workspace
2. Insufficient illumination of the work surface
3. Production noise
4. Electromagnetic radiation of the radio frequency range
5. Ionizing radiation

According to [4], the work of a design engineer in a room with an energy consumption of 90-120 kcal/hour is classified as light physical work Ia (work performed while sitting and not requiring physical exertion).

Table 5.1

Optimal temperature values

Period of the year	Category of work	Air temperature,℃
Cold period of the year	Easy Ia	22-24
Warm period of the year		23-25

Permissible temperature values at permanent workplaces:

Period of the year	Category of work	Air temperature,℃	
		Upper limit	Lower limit
Cold period of the year	Easy Ia	25	21
Warm period of the year		28	22

In the design department, the air temperature is 30℃ C in the warm season, which exceeds the permissible temperature by 2 ℃. We provided a room temperature of 23 ℃, using mechanical ventilation with a VORTICE VARIO fan, the air exchange of which is $680\ \text{м}^3\ /\text{год}$.

Insufficient lighting. Personal computers are installed in the room, and there is natural and artificial lighting. According to [5], the value of the natural light coefficient should be at least 1.5%. In the design department, the requirements are violated, the illumination of the work surface is 370 lux, and the illumination factor is 1.2%. Natural light enters the room through the side skylights. The windows have blinds. The artificial lighting is made in the form of intermittent lines of LED lamps located parallel to the line of sight of the design engineer. For local lighting, halogen incandescent lamps are used

Industrial noise. Noise in the workplace is generated by: a computer and a peripheral device. Permissible sound pressure levels at the workplace must meet the requirements [6]:

Table 5.2

Sanitary standards for industrial noise, ultrasound and infrasound

Type of labor activity, workplace	Noise levels and equivalent noise levels, dBA, dBAeq
Design and engineering.	50

The actual noise level in the design department is 54 dB, which exceeds the permissible level.

To reduce noise levels, it is recommended to use local and general sound insulation, noise-absorbing screens, and absorbing filters.

5.2. Calculation of air exchange based on excess heat in the design department:

The room has dimensions of 4 ×8 × 4, which is located on the second floor of a five-story building on the south side. The area of the windows is F= 2.88 m^2. The windows have blinds. There are 5 design engineers in the room, N $_{пк}$= 5 personal computers and a printer. For artificial lighting, 4 office LED lamps with a power of 125 W are used.

1. Calculate the total amount of heat:

$$Q_{над} = Q_{осв} + Q_{облад} + Qin\text{-}pr_{.} + Q_{рад,}\ \mathrm{W} \tag{5.1}$$

$Q_{над}$ - total amount of heat

$Q_{осв}$ - the amount of heat from artificial lighting sources

$Q_{equipment}$ - the amount of heat from the equipment

$Qin\text{-}p_{.}$- amount of heat from design engineers

$Q_{рад,}$ - the amount of heat from solar radiation

2. Calculate the amount of heat from artificial lighting sources:

$$Q_{\ осв}=N\cdot\eta\ , \tag{5.2}$$

where *N is the* total power of the lighting sources, W;

η is the coefficient of thermal losses (η = 0.55 for LED lamps).

$$Q_{\ осв.}=125\cdot4\cdot0.55=275\ \mathrm{W}$$

2. Calculate the amount of heat generated by the equipment: 5 computers and a printer (in print mode):

$$Q_{облад} =n\ \cdot P\ +P_{комп.пр.}, \tag{5.3}$$

where *n is the* number of computers (equipment);

$P_{комп}$ - installed power of computers, $P_{комп}$ = 400 W

$P_{пр.}$ - printer power in print mode, $P_{пр}$ =465 W

$$Q\ =5_{облад}\cdot\ 400+465\ =\ 2.5\ \mathrm{kW}$$

3. We calculate the amount of heat from design engineers:

$$Qin\text{-}pr_{.}=n\cdot q,\ \mathrm{W} \tag{5.4}$$

n - number of design engineers

q is the amount of heat generated by one design engineer

The amount of heat generated by one design engineer performing light physical work is 99 watts.

$$Q_{\ ін\text{-}пр}=\ 5\cdot 99=495\ \mathrm{W}$$

4. Calculate the amount of heat from solar radiation:

$$Q = m\ S\ k_{\text{рад}\cdot\text{скл}\ q} \tag{5.5}$$

where *m is the* number of windows; $S_{вікна}$ is the area of one window, $S_{вікна} = 2.88\ m^2$;

k - coefficient of window weave: *k* = 0.6 matte;

$q_{скл.}$ - heat gain through 1 m^2 of a window with different window orientation:

$q_{скл.} = 150$ - south;

$$Q = 1_{рад}\cdot 2.88\cdot 0.6\cdot 150 = 259.2\ \text{W}$$

5. The total amount of heat in the design department:

$$Q_{над} = Q_{осв} + Q_{облад} + Qin\text{-}pr_{.} + Q_{рад} = 275+2500+495+259.2 = 3.529\ \text{kW}$$

6. Air exchange is required for excess heat:

$$L = \frac{Q}{c\cdot\rho\cdot(t_{\text{вид}} - t_{\text{зовн}})}\ ,\text{м}^3/\text{год} \tag{5.6}$$

Q - is the amount of heat released into the room per hour, J:

$$Q{=}3600\text{-}Q_{надл} = 3600\text{-}3529 = 12704\ \text{W} = 5328\ \text{kJ};$$

s is the heat capacity of air, J/kg (in the temperature range from 0°C to 100°C, it is assumed to be 1.01-10^3 J/kg);

ρ is the air density, kg/m^3 (equal to $\rho_{\text{внт}} = 1.2$ kg/m^3);

$t_{вид}$ - temperature of the exhaust air, $t = 30_{вид}$℃

$t_{зовн.}$ - temperature of the air supplied to the working area, $t = 23_{зовн.}$℃

$$L = \frac{5328}{1{,}01\cdot 10^3\cdot 1{,}2\cdot(30-23)} = 628\ \text{м}^3\ /\text{год}$$

Since, in the design department, the air temperature is increased by 2 ℃ from the permissible value of 28℃, mechanical ventilation with a VORTICE VARIO fan was installed, which ensured that the air temperature in the room was 23 ℃this value is optimal.

5.3. Fire safety

According to [7], this room belongs to category B in terms of explosive and fire hazard due to the use of solid combustible materials with a flash point above 61℃.

The design department is equipped:

- Two wireless smoke detectors SD-02 (alerts in case of smoke in the room; service area: up to 20 m^2);

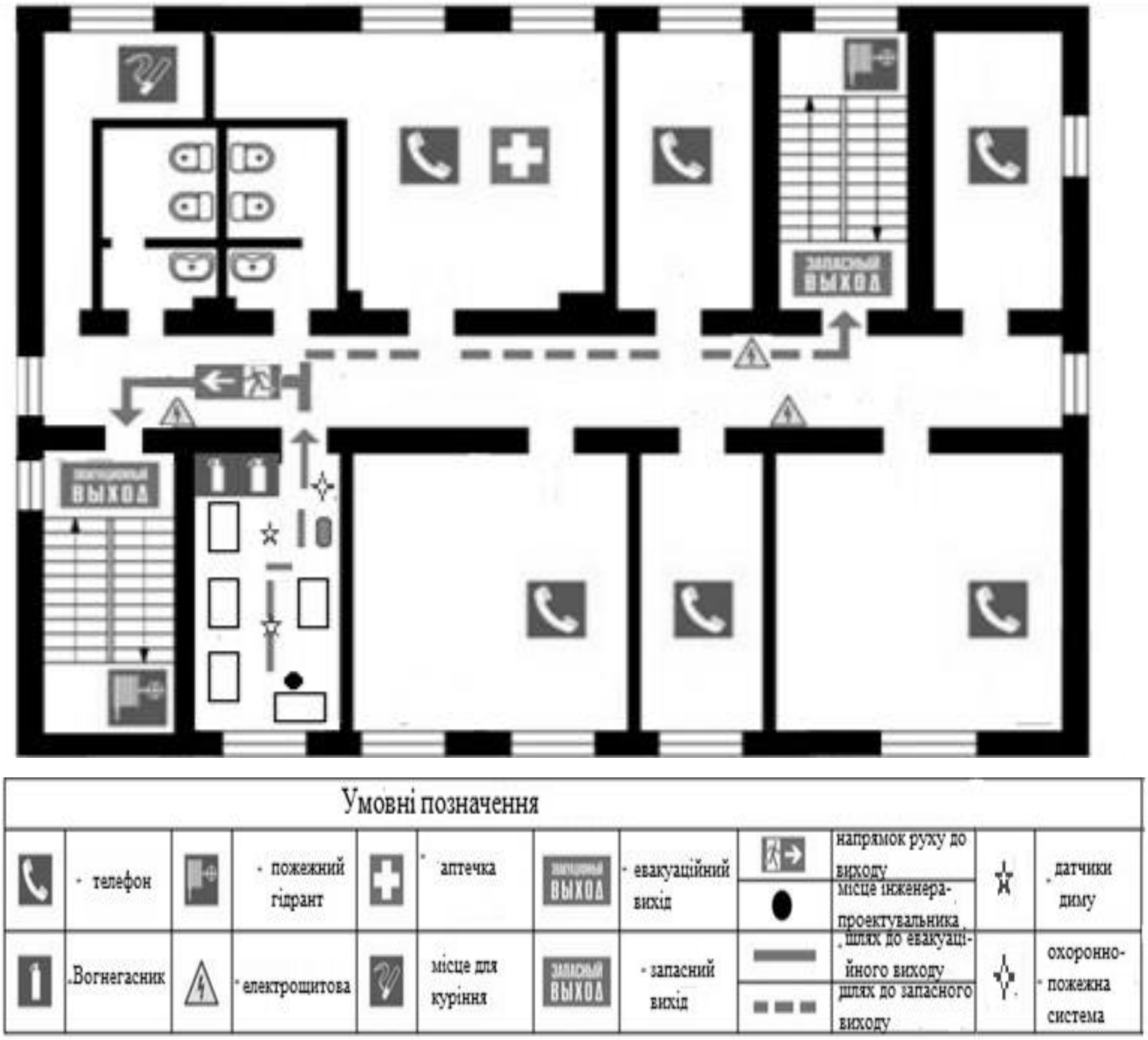
- two VP-5 powder fire extinguishers (for category B premises in the absence of combustible gases and liquids, with an area of up to 50 m^2 and an extinguishing agent weight of 5 kg, the minimum number of powder fire extinguishers is 2).

- LifeSOS LS-30LR wireless fire and security system (when an intrusion is detected, the detectors transmit an alarm signal to the central unit via a wireless radio channel. The central unit receives the signal from the detectors, activates the siren, sends information to the central monitoring station, calls the specified phone numbers, and sends SMS messages with alarm notifications).

To prevent fires, organizational and technical fire safety measures are taken, including:

- Inclusion of fire safety issues in all safety instructions;
- compliance with the established mode of operation of electrical networks and equipment;
- prohibition of smoking in the wrong place;
- issuing the necessary instructions and evacuation plans

The evacuation plan consists of graphic and textual parts. The graphic part is a schematic floor plan (Fig. 5.1), in which green solid arrows indicate the escape routes leading to the main exits, and dashed green arrows indicate the emergency exits. Doors on the escape route open outward in the direction of the building exit. The evacuation plan shows the location of fire extinguishers, fire hydrants, telephones, first aid kits, electrical panels, smoke detectors, and fire alarm systems with symbols.



Умовні позначення

☎	телефон		пожежний гідрант	✚	аптечка	ЭВАКУАЦИОННЫЙ ВЫХОД	евакуаційний вихід	→ ●	напрямок руху до виходу місце інженера-проектувальника	☆	датчики диму
	Вогнегасник	⚠	електрощитова		місце для куріння	ЗАПАСНЫЙ ВЫХОД	запасний вихід	▬ ▬ ▬ ▬	шлях до евакуаційного виходу шлях до запасного виходу	✧	охоронно-пожежна система

Figure 5.1. Evacuation plan for the 2nd floor

5.4. Instruction on labor protection when working with a personal computer

General requirements for the equipment of a workstation with a PC.

- The workstation for video terminal users must be located in such a way that the user's field of vision does not include windows, lighting fixtures, or reflective surfaces. The surface of the desktop must not be polished. To prevent glare on the video monitor screen, especially in summer and on sunny days, the video monitor screen should be placed so that the light from the window falls from the side, preferably from the left.

- The PC video monitor screen should be located at a distance of at least 500 - 700 mm from the user's (hereinafter referred to as the operator's) eyes. The viewing angle should be within 10-40 degrees. The most rational is to position the screen perpendicular to the operator's line of sight.
- The PC should be located at least 1 meter away from the heat source.
- The keyboard should be placed on a table surface or a special stand at a distance of 100-300 mm from the edge facing the user. The angle of inclination of the keyboard panel to the horizontal surface should be within 5 to 15 degrees.
- The height of the working surface of the table should be between 680-800 mm.
- The chair must provide the operator with comfortable working conditions and physiologically rational working posture during work. The chair must provide the ability to adjust the height of the seat surface, the angle of the backrest and the height of the backrest.
- To protect against direct sunlight, which creates glare on the video monitor screen, sun protection devices should be installed on the windows. The video monitor screen should be positioned so that the light from the window falls on the workstation from the side, preferably from the left.
- It is advisable to use fluorescent lamps as a source of artificial lighting in rooms where the PC is installed. Incandescent lamps may be used in local lighting fixtures. The illumination of the workstation in the horizontal plane at a height of 0.8 m from the floor level should be at least 400 lux. Vertical illumination in the plane of the screen should not exceed 200 lux. To reduce eyestrain, it is necessary to ensure a sufficiently uniform distribution of the brightness of the working surface of the video monitor and the surrounding space.
- The rooms where the PC is used should be damp-cleaned daily and regularly ventilated during the working day. Dust the screen at least once a day.
- To protect the operator from electromagnetic radiation and electrostatic fields generated by the video monitor, it is necessary to use protective screens.
- PC users should wear clothing made of natural materials or a combination of natural and artificial fibers.

Safety requirements before starting work.

- Before starting work, the employee must visually check the integrity of the cases of the system unit, video monitor, printer, and keyboard.
- Check the integrity of the power cables and their connection points (power outlets, power strips, junction boxes, plugs).
- Prepare your workplace by removing things that may interfere with your work.
- Turn on the power of the PC.
- If, after turning on the PC, the computer fails to boot or does not enter the operating mode, the employee must notify the manager or a specialist of the Information Technology Department.
- Notify your immediate supervisor if you find any damage or other defects. Do not start work without his/her instructions.

Safety requirements during work

- All components of the device must be placed stably on the table, including the keyboard. At the same time, it should be possible to move the keyboard. Its location and angle of inclination must meet the wishes of the PC user. If the keyboard design does not provide space for palm support, then it should be located at a distance of at least 100 mm from the edge of the table in the optimal area of the monitor field. When working on the keyboard, sit up straight and do not strain.
- To reduce the adverse effects on the user of devices such as "mouse" (forced posture, the need for constant monitoring of the quality of actions), it is necessary to provide a large area of the table surface for moving the "mouse" and a comfortable elbow rest.
- Extraneous conversations, annoying noises, etc. are not allowed.
- Periodically, when the PC is turned off, remove dust from the surfaces of the equipment with a cotton-paper cloth slightly moistened with soap and water. Wipe the screen and screen protector with cotton moistened with alcohol.
- Do not use liquid or aerosol cleaners to clean the PC surfaces.

Prohibited:

- independently repair equipment in which the kinescope and other elements may be under high voltage (up to 25 kV0.)

- place anything on the PC hardware, sandwiches, or drinks on or near the keyboard. Doing so may damage the keyboard;
- Do not cover the ventilation holes in the equipment, as this may cause it to overheat and malfunction.

- To reduce the negative impact on the health of employees of various risk factors associated with working on a PC, additional regulated breaks for resting PC users are provided:
  - 10 minutes after each hour of continuous operation;
  - every 2 hours - 15 minutes.
- Whenever possible, you should alternate between changing activities and other activities that are not related to working on a PC.
- In order to reduce the negative impact of monotony, it is advisable to use alternating text entry and data entry operations (changing the content and pace of work), etc.
- When working with laser printers:
- Place the printer next to the system unit so that the connecting cords are not stretched. Do not place the printer on top of the system unit.
- Before you program the printer, make sure that it is in communication mode with the system unit.
- To achieve a high-quality, clear, high-resolution image and avoid damaging the device, you should use paper whose brand is specified in the printer manual (most often paper weighing 60-135 g/m^2 , such as Canon or Xerox 4024).
- Trim the edges of the paper with a sharp knife blade, without burrs, to reduce the possibility of paper creasing.
- When performing work (more than 20 minutes), when user intervention in the program is not required, it is advisable to turn off the power of the video monitor.
- To maintain overall muscle tone, prevent musculoskeletal disorders, visual discomfort and other unfavorable subjective feelings, you should perform sets of recommended exercises for the eyes, spine, and arms during regulated breaks.

- The number of micro-pauses up to 1-2 minutes should be determined individually. The form and content of the breaks may vary: performing auxiliary work not related to PC operation, eating, performing recommended exercises.
- Exercise during the day is recommended individually, depending on the feeling of fatigue. Gymnastics should be aimed at correcting the forced posture, improving blood circulation, partially compensating for the lack of motor activity.
- Immediately stop working, disconnect all equipment from the power supply, and immediately notify your immediate supervisor or a PC repair specialist of any malfunctions (sparking, breakdowns, burning odor, signs of burning, etc.).

Safety requirements when ending work on a PC.

- Close and save the files that were in progress in the PC memory. Perform all the steps to correctly shut down the operating system.
- Turn off the printer and other peripherals, and turn off the system unit. If you have an uninterruptible power supply (UPS), turn off the power.
- Turn off the PC by pressing the "POWER" button and unplug the power cable from the power outlet
- Cover the keyboard to prevent dust from entering it.
- Clean up the workplace.

Safety requirements in emergency situations.

- If, after turning on the PC, you smell a burning odor or feel an electric shock when you touch the metal parts of the PC, you must immediately disconnect the PC from the power supply and report it to your supervisor.
- In the event of a fire, immediately begin extinguishing the fire with available fire extinguishing equipment and report it by calling 101 (city fire department) and the head of the company's fire department. Remember that electrical installations should be extinguished with carbon dioxide fire extinguishers and dry sand to avoid electric shock.
- In case of injury, stop working, provide first aid, call an ambulance by calling 103, and, if necessary, take to a hospital.
- The sequence of first aid:

- Eliminate exposure to dangerous and harmful factors that threaten the victim's health and life (remove the victim from the effects of electric current, remove him or her from the contaminated atmosphere, extinguish burning clothing, etc;)
- Determine the nature and severity of the injury, the greatest threat to the victim's life, and the measures to be taken to save him or her;
- Take the necessary measures to rescue the victim in order of urgency (restore airway patency, perform artificial respiration, external cardiac massage, stop bleeding, immobilize the fracture site, apply a bandage, etc;)
- Support the victim's basic vital functions until the arrival of a medical professional;
- call an ambulance or doctor, or take measures to transport the victim to the nearest medical facility.
- Assistance to the victim provided by non-medical personnel should not replace assistance from medical personnel and should be provided only until a doctor arrives.
- Specific actions to provide first aid to victims of various injuries are described in Instruction No. 03-OP "On Providing First (Premedical) Medical Aid in Accidents," which is studied by employees of the enterprise during initial and subsequent occupational safety and health briefings.

In the event of other emergencies, stop working and notify the work supervisor.

Based on the calculation of air exchange for excess heat, the value of which is 628 m^3 /h, mechanical ventilation with a VORTICE VARIO fan was installed, since the use of natural ventilation is inefficient. Mechanical ventilation is capable of removing a temperature of 30°C and maintain the air temperature at an acceptable and even optimal value.

List of references in chapter five

1. NPAPP 0.00-1.28-10 Rules of labor protection during the operation of electronic computers

2. DSTU 3.3.6.037-99 "Sanitary norms of industrial noise, ultrasound and infrasound"

3. State Sanitary Norms and Rules "Hygienic Classification of Labor by Indicators of Hazardousness and Danger of Factors of the Production Environment, Severity and Intensity of the Labor Process"

4. "DSTU 3.3.6.042-99 Sanitary norms of microclimate of industrial premises"

5. DBN 13.2.5-28-2006 "Natural and artificial lighting"

6. DSTU 3.3.6.037-99 "Sanitary norms of industrial noise, ultrasound and infrasound"

7. NAPB B.03.002-2007 "Norms for determining the categories of premises, buildings and outdoor installations by explosion and fire hazard"

CHAPTER 6
ENVIRONMENTAL PROTECTION

Today, radio and electronic production is highly developed and society cannot imagine its life without it. The electronic and radio engineering industry plays a leading role in the scientific and technological revolution. The introduction of electronic devices in various spheres of human activity contributes significantly to the successful development of complex scientific and technical problems, increased productivity of physical and mental labor, and improved economic performance.

In the thesis project, a cable digital television subscriber receiver was designed, which can have a negative impact on the environment.

6.1 Analysis of the impact of man-made factors

The widespread use of electrical and electronic equipment has not only improved the quality of life, but also led to negative consequences for the environment and human health. The main harmful and dangerous factors that affect the environment can be identified:

- *noise pollution;*
- *Vibration pollution;*
- *electromagnetic pollution*
- *thermal pollution*
- *radiation contamination*

6.1.1. Noise pollution

In today's world, due to scientific and technological progress, noise has become a form of physical (wave) pollution of the environment. Noise is generally considered to be all unpleasant and unwanted sounds or their combination that interfere with normal work, perception of necessary sound information and rest.

Adaptation to it is almost impossible. The background noise level of the environment is 30-60 decibels. Under modern conditions, this natural background is supplemented by industrial and traffic noise, which often exceeds 100 decibels. Sources of noise include industrial facilities, vehicles, loudspeakers, televisions, radios, musical instruments, crowds, etc. Noise in the workplace has a negative impact on employees: it weakens attention, increases fatigue, and slows down the reaction to danger. As a result, performance decreases and the likelihood of accidents increases. Permissible sound pressure levels in octave frequency bands at workplaces in industrial premises are shown in Table 6.1[1]:

Table 6.1

Permissible sound pressure levels in octave frequency bands

Sound pressure levels in dB, in octave frequency bands, Hz								
31,5	63	125	250	500	1000	2000	4000	8000
107	95	87	82	78	75	73	71	69

It has been established that plants under the influence of noise reduce their energy for growth, they have excessive (even complete, leading to death) moisture release through the leaves, and cellular disorders are possible. Leaves and flowers of plants located close to the source of intense noise (sound) die. The absence of noise is especially necessary for animals that exchange sound information and analyze environmental sounds to improve information, including alarms. Noise has a similar effect on animals. The noise of a jet airplane kills bee larvae, the

They lose their ability to navigate, and eggshells crack in bird nests. Beetles, bumblebees, and other insects cannot take to the air due to air vibrations caused by the sounds of portable radio equipment.

6.1.2. Vibration pollution

Vibration is a mechanical oscillation of a solid body. Vibration is divided into natural and artificial. Sources of natural vibration are earthquakes caused by natural factors. Sources of artificial vibration include industry and transportation. Prolonged vibrations cause great harm to human health - from severe fatigue to changes in many body functions: cardiac disorders, nervous system, vascular spasms, muscle deformities, concussions, etc. Vibration with a frequency that resonates with the frequency of oscillation of individual organs or parts of the human body is especially dangerous, which can lead to their damage. Prolonged exposure to vibration can cause an occupational disease - vibration sickness.

6.1.3. Electromagnetic pollution

In the course of evolution, the biosphere has been and is constantly under the influence of electromagnetic fields (EMFs) of natural origin (natural background): the Earth's electric and magnetic fields, space electromagnetic radiation, primarily that generated by the Sun. In the period of scientific and technological progress, humanity has created and increasingly used artificial (anthropogenic) sources of EMF. Nowadays, EMFs of anthropogenic origin significantly exceed the natural background and are an unfavorable factor whose impact on humans and the environment is growing year by year. The degree of EMF exposure to the human body depends on the frequency range, intensity and duration of exposure, the nature of the radiation (continuous or modulated), the exposure mode, the size of the body surface exposed to the radiation, and individual characteristics of the body. Electromagnetic fields can cause biological and functional disorders in the body. Functional effects are manifested in premature fatigue, frequent headaches, sleep disturbances, and impaired cardiovascular and central nervous system functions. Prolonged and intense exposure to EMFs leads to persistent disorders and diseases. Biological negative effects of EMF exposure are manifested in thermal and non-thermal effects. Thermal effects lead to an increase in body temperature and local selective heating of organs and tissues due to the conversion of electromagnetic energy into heat. Such heating is especially dangerous for organs with poor thermoregulation (brain, eyes, kidneys, stomach, etc.). For example, radiation in the centimeter range leads to cataracts, i.e., gradual loss of vision.

6.1.4. Thermal pollution

Thermal pollution is the result of heat dissipation into the environment, which is released in numerous thermal processes, primarily related to fuel combustion. Fuel combustion annually consumes up to 23% of the oxygen generated by photosynthesis on Earth over the course of a year. It is estimated that during coal combustion, more radioactive components are released into the environment than during the same time at all nuclear power plants in case of accident-free operation. Thermal pollution of the hydrosphere occurs mainly as a result of discharges of heated water from thermal power plants, nuclear power plants and other energy facilities into water bodies. Warm water changes the thermal and biological regimes of water bodies and has a harmful effect on their inhabitants.

6.1.5. Radiation contamination

The main sources of radiation pollution include:

- the uranium industry, which is engaged in the extraction, processing, enrichment and production of nuclear fuel;

- Nuclear reactors of various types with a large amount of radioactive material in their cores, which are atomic bombs whose processes have been slowed down to a steady state;

- the radiochemical industry, whose enterprises process and renew spent material;

- radioactive waste treatment and disposal sites that, due to the inability to ensure absolute isolation of the radiation source, release radionuclides into the environment;

- use of radionuclides in the form of sealed low-power radioactive sources in industry, medicine, geology, and agriculture.

The main threat to the environment is posed by man-made radionuclides that arise during nuclear weapons testing.

6.2 Environmental impact of receiving devices

Subscriber receiver is a television receiver (set-top box), a device that receives a digital television signal, decodes it and converts it into an analog signal for output via RCA or SCART connectors or converts it into a digital signal for output via HDMI connector, and transmits it further to the TV.

The receiver produces weak electric and magnetic alternating fields in a wide range of frequencies. However, the problem of exposure to electromagnetic radiation deserves special attention. Scientific studies have shown that EMFs include a factor that affects users when they have modern EMF shields. Ukrainian scientists have identified this factor as torsion fields, which accompany any electromagnetic radiation and are its information component. The World Health Organization's Working Group on Hygienic Aspects of the Use of Monitors and Radio Terminals has identified health disorders when using devices that emit electromagnetic radiation, the most serious of which are:

- visual impairment;
- immune system disorders;
- psycho-emotional disorders (stress syndrome, aggressiveness)

To ensure the safety of users' health, the State Sanitary Norms and Rules for Working with Sources of Electromagnetic Fields "DSanPiN 3.3.6.096-2002" [2] are in force in Ukraine. The values of the GDRs for the intensity of electric ($E_{гд}$) and magnetic ($H_{гд}$) components depending on the duration of their exposure are given in Table 6.2.

As a result of exposure of the human body to electromagnetic radiation in the range of 30 kHz - 300 MHz (LF), the following symptoms are observed: general weakness, increased fatigue, drowsiness, sleep disturbance, headache and pain in the heart area. Irritability appears, attention is lost, motor and speech reactions slow down. There are a number of symptoms that indicate a malfunction of certain organs - the stomach, liver, and pancreas.

Table 6.2

GDR values of the electric ($E_{\text{гд}}$) and magnetic ($H_{\text{гд}}$) components

Staff overstay, hours	$E_{\text{гд}}$, V/m					$H_{\text{гд}}$, A/m			
	1-10 kHz	10-60 kHz	0.063 MHz	3-30 MHz	30-300 MHz	1-10 kHz	10-60 kHz	0.06-3 MHz	30-50 MHz
8	120	70	50	30	10	9	7	5	0,3
7	130	75	53	32	11	9,8	7,5	5,3	0,32
6	140	82	58	34	12	10,6	8,1	5,8	0,34
5	155	90	63	37	13	11,6	8,8	6,3	0,38
4	175	110	71	42	14	13	9,9	7,1	0,42
3	200	115	82	48	16	15	11,4	8,2	0,49
2	250	140	100	59	20	18,4	14	10	0,6
1	350	200	141	84	28	26	19,7	14,2	0,85
0,5	500	280	200	118	40	37,6	27,9	20	1,2

In order to reduce the level of electromagnetic radiation, it is necessary to limit the continuous operation time of the subscriber receiver.

In Ukraine, electromagnetic safety standards are regulated by the State Sanitary Norms and Rules for the Protection of the Population from the Effects of Electromagnetic Radiation, according to which the permissible levels of electromagnetic radiation intensity for the civilian population are 2.5 $\mu W/cm^2$.

The subscriber receiver generates noise with a level of 54 dB during operation. The permissible sound pressure level must comply with "DSN 3.3.6.037-99 Sanitary norms of industrial noise, ultrasound and infrasound"[1], namely 50 dB.

A large number of sound signals entering the cerebral cortex cause anxiety, fear, and premature fatigue. The impact of noise on humans is expressed in a wide range - from subjective irritation to objective changes in the central nervous system, hearing organs, cardiovascular and endocrine systems, digestive tract and other organs and systems. The first indicator of the harmful effects of noise is complaints of irritation, anxiety, and sleep disturbance.

6.3 Means of protection against electromagnetic radiation and noise, the problem of e-waste.

6.3.1 Protection against electromagnetic radiation

To reduce the impact of EMFs on personnel and the public in the area of radio electronic equipment, a number of protective measures should be taken. These may include organizational, engineering, technical, and medical and preventive measures.

Measures to reduce exposure of workers to EMFs include organizational, engineering, technical, and medical and preventive measures.

Organizational measures are carried out by sanitary supervision authorities. They conduct sanitary supervision of facilities that use sources of electromagnetic radiation.

Engineering and technical measures provide for the location of EMF sources that would minimize their impact on workers, the use of remote control of equipment that is a source of radiation, shielding of radiation sources, and the use of personal protective equipment (gowns, overalls made of metallized fabric, with a lead to a grounding device). To protect the eyes, it is advisable to use protective goggles ZP5-90. The glasses are coated with semiconducting tin, which reduces the intensity of electromagnetic energy with a light transmission of at least 75%.

In general, personal protective equipment should be used only when other protective equipment is impossible or insufficiently effective: when passing through areas of high intensity exposure, during repair and adjustment work in emergency situations, during short-term monitoring and when the intensity of exposure changes. Such means are inconvenient to use, limit the ability to perform labor operations, and worsen hygienic conditions.

In the radio frequency range, personal protective equipment works on the principle of shielding a person using reflection and absorption of EMFs. Clothing made of metallized fabrics and liquid-absorbing materials is used to protect the body. Metallized fabric is made of cotton threads with a thin wire placed inside them, or of cotton or nylon threads spirally wrapped with metal wire. This fabric, like a metal mesh, significantly reduces the effect of radiation at a distance of up to 0.5 mm between the threads. When sewing parts of protective clothing, it is necessary to ensure contact of insulated wires. Therefore, seams are electrically sealed with conductive masses or adhesives that provide galvanic contact or increase the capacitive coupling of non-contact wires. Medical and preventive measures include systematic medical examinations of employees exposed to EMFs, time limits for people to stay in areas of high intensity electromagnetic radiation, free medical and preventive nutrition, and sanitary and health breaks.

6.3.2. Protection against noise

To reduce and eliminate noise, a whole range of measures called noise protection is used. This includes the use of sound-absorbing materials, rational placement of construction facilities, creation of screens along the streets in the form of earthen berms, walls of various structures, noise-reflecting, usually non-residential buildings such as shops, warehouses, and garages.

6.3.3 The problem of e-waste

According to the Law of Ukraine "On Waste", in order to prevent or reduce waste generation, systems for the collection and utilization of electrical and electronic equipment must be implemented [3]. The solution to the problem of e-waste in Ukraine should be provided by the “Technical Regulations on Waste Electrical and Electronic Equipment Management”, which has been developed in Ukraine since 2008. According to the drafts of these legislative acts, importers and manufacturers can either dispose of e-waste themselves or sign contracts with authorized companies to organize the collection, procurement and disposal of the relevant types of equipment. A draft Resolution of the Cabinet of Ministers of Ukraine “On Approval of the Technical Regulations for Waste Electronic and Electrical Equipment Management” has also been developed.

However, in general, the problem of e-waste in Ukraine needs to be solved both in the organizational and legal aspect – the creation of producer funds, state support for waste disposal companies – and in the social and informational aspect: Ukrainians need to be convinced that it is not allowed to take a broken electronic device to a regular trash can.

Conclusion to Chapter Six

Subscriber receivers have a negative impact on the environment. They are sources of electromagnetic radiation and noise pollution. To minimize the risk of disease, engineering and technical measures that reduce the impact of harmful factors are effective. The problem of electronic waste was also discussed, one of the ways to solve which is to create collection points for electronic and electrical equipment.

CONCLUSIONS

This work is the outcome of an in-depth examination of the relationship between Blockchain technology and the Internet of Things. The investigation was conducted with the intention of improving the safety, effectiveness, and dependability of information systems.

Throughout the course of this investigation, the most important components of Blockchain technology and its relationship with the Internet of Things were thoroughly investigated. Following an analysis of the structure and classification of Blockchain, the most important component of smart contract functionality was brought to the forefront as a focal point. After conducting an in-depth investigation, the research then moved on to analyze the general characteristics of the Internet of Things (IoT) and the impact those characteristics have on the functionality of the system.

The classification of testing methods, as well as a study of testing methodologies and characteristics using Blockchain, were both required in order to evaluate the quality of Internet of Things (IoT) systems. Taking into consideration the significance of smart contracts and token issuance concepts for the purpose of achieving successful integration into scientific research, a comprehensive grasp of how these concepts operate was obtained.

The scope of the examination was expanded to include the investigation of models for the implementation of Blockchain technology in situations requiring the placement of scientific research. The importance of this facet was emphasized for the purpose of further development and use in the real world.

Additionally, a comprehensive investigation was conducted into the various sorts of assaults and security concerns, with a special focus on Proof-of-Stake methods. As part of the investigation, the probability of an attack being successful was calculated, methods were determined, and attacks were modified in order to guarantee the safety of Internet of Things networks.

When it comes to the practical application of the concepts that were investigated, a Blockchain algorithm was characterized as being implemented in an automated resource accounting system. The implementation of a mechanism for user permission and authentication through the utilization of JSON Web Tokens secured the safety of an essential component of the system. Additionally, an algorithm was developed for the purpose of authenticating a new block and maintaining the integrity of the contents.

The criteria for extra software were created in order to make it easier for users to engage with the software system. The practical embodiment of the topics that were presented was proven by the presentation of program execution results, which included the production of tokens and the software development of web applications.

In conclusion, our research explored a wide range of topics, ranging from theoretical analysis to practical application, with the goal of uncovering new opportunities for implementing Blockchain technology in Internet of Things (IoT) systems. The concepts that were established and the algorithms that were implemented offer great practical significance for the purpose of improving the speed, reliability, and security of Internet of Things (IoT) systems through the utilization of Blockchain. In order to further improve and execute the gained knowledge in the actual world, developers, engineers, and researchers can make use of the information that they have acquired.

This paper provides an overview of potential avenues for future research in the use of Blockchain technology to enhance and optimize Internet of Things (IoT) systems. For the growth of this sector, new vistas are opened up by the possibilities of expanding the application of the technology in actual settings and investigating the impact that it has on other contemporary technologies.

It is clear that the findings of this study represent a significant contribution to the understanding of the capabilities and applications of Blockchain technology for the purpose of improving the functionality and security of Internet of Things (IoT) systems, hence highlighting the promise of these technologies in the contemporary information environment.

REFERENCES

1. Yuan, Y., & Wang, F. Y. (2020). Blockchain and internet of things: integration and security issues, challenges, and opportunities. IET Cyber-Physical Systems: Theory & Applications, 1(1), 13-35.

2. Anagnostopoulos, I., & Zeadally, S. (2021). Decentralized autonomous organizations and the internet of things: a comprehensive review. IEEE Internet of Things Journal, 8(4), 2316-2332.

3. Yao, H., Wu, J., & Zhang, W. (2020). A blockchain-based secure internet of things system for intelligent transportation systems. IEEE Internet of Things Journal, 7(9), 8254-8264.

4. Noor, A. K., Bashir, A. K., Elragal, A., & Ahmed, R. (2020). Blockchain in internet of things: Challenges and solutions. Measurement, 167, 108288.

5. Zeng, J., & Xiong, H. (2021). Blockchain for decentralized trust management in ambient assisted living. Journal of Network and Computer Applications, 170, 102841.

6. Sun, Y., Li, J., & Ren, Y. (2020). Blockchain-based secure firmware update framework in the internet of things. IEEE Internet of Things Journal, 7(6), 4981-4990.

7. Ma, J., Xiao, Y., Wang, H., Sun, L., Wang, F., & Lai, C. F. (2021). A survey on blockchain technology for the Internet of Things: Security and privacy. IEEE Access, 9, 45217-45232.

8. Wang, X., & Guo, S. (2020). Research on blockchain technology and its application in internet of things. IEEE Access, 8, 144060-144072.

9. Khezr, S., Moniruzzaman, M., & Yassine, A. (2020). Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied Sciences, 10(11), 3820.

10. Liao, C., Li, W., & Yang, D. (2020). Blockchain technology for internet of things: A survey. IEEE Internet of Things Journal, 7(10), 9319-9334.

11. Naudé, W., & Rubin, B. (2020). Decentralized autonomous organizations: blockchain governance structures for the internet of everything. Technology in Society, 60, 101234.

12. Luo, Z., Xu, L., & Guan, D. (2021). Blockchain technology and its applications in the internet of things. In Advances in internet of things (pp. 261-278). Springer.

13. Salman, O. H., Kiah, M. L. M., Zaidan, A. A., Sali, A., & Ismail, N. (2021). The internet of things in healthcare: an overview. Sensors, 21(14), 4700.

14. Jia, K., Xie, H., & Xue, Y. (2020). A survey on blockchain-based internet of things. Journal of Ambient Intelligence and Humanized Computing, 11(2), 1071-1090.

15. Tanwar, S., Kumar, N., Tyagi, S., & Obaidat, M. S. (2021). Blockchain-based IoT for secure communication in healthcare: A review, taxonomy, and future directions. Journal of Network and Computer Applications, 178, 102983.

16. Alsamhi, S. H., Jiang, M., Han, G., & Song, H. (2020). Blockchain-based secure and privacy-preserving data sharing in vehicular edge computing and networks. Journal of Network and Computer Applications, 177, 102886.

17. Taneja, A., Mehta, S., & Verma, V. (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future directions. Computers, Materials & Continua, 64(1), 337-362.

18. Maesa, D. D., & Ricci, L. (2021). A survey on blockchain-based smart contracts for the internet of things. Computers, Materials & Continua, 68(3), 3733-3755.

19. Hammoudi, S., & Baina, A. (2020). Blockchain-based decentralized storage system for internet of things data. Future Generation Computer Systems, 111, 114-124.

20. Wang, S., Zhang, L., Wang, X., & Chen, Y. (2020). Blockchain-based remote healthcare monitoring: A survey. Journal of Network and Computer Applications, 175, 102873.

21. Conoscenti, M., Vetro, A., & De Martin, J. C. (2020). Blockchain for the Internet of Things: A Systematic Literature Review. IEEE Access, 8, 198776-198809.

22. Alsamhi, S. H., Zhou, D., Cheng, J., Alsamhi, S. H., & Hussain, A. (2021). Blockchain-Empowered Secure and Efficient IoT-Based Smart City Framework. Future Generation Computer Systems, 114, 632-647.

23. Li, X., Li, X., & Shen, J. (2021). Blockchain-Based Trustworthy Framework for Data Privacy Preservation in IoT Environments. Journal of Network and Computer Applications, 177, 102986.

24. Yao, H., Wu, J., & Zhang, W. (2020). A Blockchain-Based Secure Internet of Things Model with Trust Management in Precision Agriculture. Computers, Materials & Continua, 65(2), 1665-1685.

25. Han, G., Li, W., & Khan, M. K. (2021). Security and Privacy Preservation in Blockchain-Enabled Internet of Things: A Survey. IEEE Internet of Things Journal, 8(3), 2100-2121.

26. Wang, K., Cao, X., Liang, X., & Cao, J. (2020). A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. Journal of Network and Computer Applications, 171, 102878.

27. Wang, S., Zhang, L., & Wang, X. (2020). Blockchain-Based Remote Healthcare Monitoring: A Survey. Journal of Network and Computer Applications, 175, 102873.

28. Salman, O. H., Kiah, M. L. M., Zaidan, A. A., Almuktar, S., Sali, A., & Chiroma, H. (2021). A Survey of Consensus Algorithms in Blockchain. Journal of King Saud University-Computer and Information Sciences.

29. Malik, S. U. R., Batool, A., Abbas, H., Rho, S., & Song, H. (2021). A Survey of Consensus Algorithms in Blockchain. Journal of King Saud University-Computer and Information Sciences.

30. Han, G., Li, W., & Khan, M. K. (2021). Security and Privacy Preservation in Blockchain-Enabled Internet of Things: A Survey. IEEE Internet of Things Journal, 8(3), 2100-2121.

31. Wang, K., Cao, X., Liang, X., & Cao, J. (2020). A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. Journal of Network and Computer Applications, 171, 102878.

32. Wang, S., Zhang, L., & Wang, X. (2020). Blockchain-Based Remote Healthcare Monitoring: A Survey. Journal of Network and Computer Applications, 175, 102873.

33. Salman, O. H., Kiah, M. L. M., Zaidan, A. A., Almuktar, S., Sali, A., & Chiroma, H. (2021). A Survey of Consensus Algorithms in Blockchain. Journal of King Saud University-Computer and Information Sciences.

34. Malik, S. U. R., Batool, A., Abbas, H., Rho, S., & Song, H. (2021). A Review of the Security of Blockchain Technology: Applications, Solutions, and Challenges. Symmetry, 13(4), 628.
35. Khalid, A., Ghazal, A., & Khan, S. U. (2021). Leveraging Blockchain for Secure and Efficient Data Sharing in IoT-Enabled Smart Cities. IEEE Internet of Things Journal, 9(17), 13835-13844.
36. Liao, J., Cao, J., Wang, Q., & Wang, X. (2021). BNSC: A Blockchain-Based Non-Repudiable Secure Communication Scheme for Vehicular Ad Hoc Networks. IEEE Transactions on Network and Service Management, 18(3), 2134-2147.
37. Nafea, M. I., Alsayed, A., Elkordy, A., & Zahran, A. H. (2021). Secure Data Sharing in IoT-Based Healthcare Systems Using a Consortium Blockchain. IEEE Access, 9, 27264-27273.
38. Zhang, W., Feng, Z., Zhang, Y., Guan, Y., & Chang, W. (2021). A Blockchain-Based Data Provenance System for the Internet of Things. IEEE Internet of Things Journal, 8(9), 6787-6797.
39. Li, X., Jiang, P., Wang, Y., Xie, Y., & Xiong, H. (2021). Blockchain-Enabled Self-Sovereign Identity for Internet of Things Devices in Cloud Computing. IEEE Transactions on Cloud Computing.
40. Chen, C., Zhang, L., Guo, S., & Yang, Y. (2021). On the Application of Blockchain Technology in Edge Computing. IEEE Transactions on Industrial Informatics.
41. Li, X., Liu, Q., Li, Q., & Zhu, J. (2021). Blockchain-Enabled Multiagent System for Smart Grid: A Comprehensive Review. IEEE Transactions on Industrial Informatics.
42. Khezr, S., Montrone, F., Sapkota, B., Baidar, B., Misra, S., & Mohanty, S. P. (2021). A Secure and Efficient Blockchain-Based Framework for Edge Computing in Industrial IoT. IEEE Transactions on Industrial Informatics.
43. Li, X., Jiang, P., & Shi, W. (2021). Blockchain-Enhanced Authentication and Security Mechanisms in Industrial Internet of Things: A Review. IEEE Transactions on Industrial Informatics.