Ensuring Information Security of Web Resources Based on Blockchain Technologies

Barakova Aliya[1], Ussatova Olga[2], Begimbayeva Yenlik[3], Ibrahim Sogukpinar[4]
Al-Farabi Kazakh National University, Almaty, Kazakhstan[1]
KazNMU named after S.D. Asfendiyarov, Almaty, Kazakhstan[1]
AUPET named after Gumarbek Daukeyev, Almaty, Kazakhstan[2]
Institute of Information and Computational Technologies, Almaty, Kazakhstan[2]
Satbayev University, Almaty, Kazakhstan[3]
Kazakh-British Technical University, Almaty, Kazakhstan[3]
Computer Engineering, Gebze Technical University, Gebze, Kocaeli, Turkey[4]

***Abstract*—This project examines how blockchain technology can enhance data security and reliability for web applications. In this article, ways to improve data security on online course platforms that utilize blockchain technology are explored. To clarify, online course platforms are web-based applications that enable users to access course materials online. These platforms often deal with sensitive data which, if compromised, can cause significant harm to users. Unfortunately, this information is often the target of fraudulent operations and illegal actions aimed at stealing personal data that can be used for authentication on various platforms. This article identifies the weaknesses of these sites and discusses the importance of using complex technologies to safeguard web resources effectively. This research explores how blockchain technology can protect from common web application attacks, which are often aimed at the user authorization process involving the transmission of identification and authentication data from the user to the website database. The study outlines the key components of blockchain technology, including hash function, hash value, data structure, and blockchain classification. Additionally, the study presents a transaction block model for a web course developed using blockchain technology.**

Keywords*—Information security; data security; website protection; blockchain; network attacks; hash functions; web applications

I. Introduction

Websites store confidential information such as personal data like email addresses, names, birth dates, and credit card numbers [1]. Therefore, protecting information confidentiality is fundamental for most information compliance regulations today. It is concerning to know that hackers target at least 50,000 websites daily, especially since almost every business has an online presence. Small and medium-sized companies are not exempt as about 43% of attacks are directed towards them [2]. Although there are programs and firewalls available to prevent unauthorized access, there is no foolproof way to protect against hackers as they are always on the lookout for new vulnerabilities and once found, they launch an attack.

This article explores the use of blockchain technology to enhance the security and dependability of data in web applications, specifically the methods employed in online course platforms to safeguard data using blockchain technologies. Online course platforms are web applications that grant access to online course content. Therefore, a significant concern is preventing theft, unauthorized access, and duplication of online course content belonging to others. Unfortunately, scammers and plagiarists can be a common issue for creators of online training courses [3]. Providing expert knowledge in online courses can be a great way to earn a steady income, but protecting your content from theft is essential. Attackers use various methods to steal content from online course websites such as hacking the server or recording video from the screen to distribute online [4].

It is essential to ensure that your online course platform has top-notch security to prevent these unauthorized activities. Utilizing blockchain technology can effectively safeguard data and avoid unauthorized usage and copying of online course content. There are many ways to protect content from cyber-attacks and unauthorized access. However, with the development of information technology, it is necessary to use relevant methods and models for ensuring data protection, including blockchain technology. Blockchain is a data storage system that operates in a decentralized manner and guarantees the security and reliability of information. The technology creates a chain of blocks where data is stored, and each block is linked to the previous one, enabling easy verification and preventing unauthorized alterations.

By utilizing blockchain technology, it is possible to establish a decentralized registry for content rights, ensuring protection against infringements. In addition, the blockchain system enables users to manage access to information and establish usage guidelines safeguarding content from unauthorized use. With blockchain technology, it is developed to develop a register of content rights and a change control system, which protects against cyber threats. Another benefit of using blockchain technology for content protection is the potential for transparency and clarity in storing and transmitting information. This implies that every block, including information on content rights, will be visible to all users, allowing for monitoring of any changes in data and safeguarding content against potential violations.

One effective method of safeguarding content from cyber-attacks and remote access is using blockchain technology. This

technology provides a decentralized registry for storing information about content ownership and rules for appropriate use. With such measures in place, unauthorized content use is prevented, ensuring that content creators can confidently use their content online without fear of infringement.

The paper discussed various methods of information protection, their mechanisms and structures, and their weaknesses. Finally, the article demonstrated the efficacy of blockchain technology in safeguarding content against cyber-attacks and unauthorized access.

II. Related Work

We reviewed the work of scientists who conducted other studies before using blockchain technology. Sathya A. et al., in their research papers, conducted research on cryptography and blockchain technology and discussed how combining the two technologies could ensure data security. This article deals with various cryptographic attacks on the blockchain and the various security services offered on the blockchain. Blockchain security issues are also analyzed and briefly presented in this article [5]. Ahmed A. et al., in their research work, made a comprehensive analysis of the current new and large-scale level tasks based on the blockchain used in the Internet of Things domain. They have proposed a scalable assessment system in IAR environments, including essential criteria such as bandwidth, latency, and block size for information threats. They also evaluated and differentiated the Most Outstanding Large solutions, highlighting six complex scalability problems for blockchain-based solutions in IoT [6]. Sabri H. et al., in research work, analyzed SHA and MD5 and developed analytical work on the comparative analysis of algorithms and their velocities. SHA-2 and SHA-3 have become industry norms. In this paper, hash methods proposed by other scientists are considered. As a result of the study, it was decided that hash performance plays a vital role in the blockchain and IoT [7]. Naresh K. et al. provided a comprehensive overview of how Blockchain technology is used to ensure Internet security and counter current threats, as well as growing cybercrime and cyberattacks. During the review, they studied how blockchain affects cyber data and information over the Internet. In this paper, they first compiled blockchain architecture and cybersecurity models, classified and discussed the latest and most relevant anti-cybersecurity work, and identified the main challenges and barriers to blockchain technology in response to cybersecurity [8].

III. Website Protection Mechanisms and its Analysis

The World Wide Web is a collection of websites residing in various domains. A segment of the Internet comprises websites hosted within one or multiple domains. Therefore, the Internet can be seen as a compilation of these segments [9][10].

The average security of a segment of the Internet is defined as the ratio of the number of "protected" websites in the studied part to the total number of sites in the studied component.

$$W_i = \frac{s_i}{n_i} \quad (1)$$

where Wi - security indicator of the i-th segment of the Internet,

s - the number of secure websites in the i-th segment,

n - the total number of websites in the i-th segment,

i - segment number i=l,2,..C,

C - total number of Internet segments.

And the average security of the entire Internet W is defined as the average security of all its segments:

$$W = \frac{1}{c}\sum_{i=1}^{c} W_i \quad (2)$$

The security level of a website is evaluated based on a specific method. Websites face risks such as unauthorized access to locally stored information and unauthorized access or modification during data transmission over communication channels [10]. The classification of website protection mechanisms that prevent these types of threats is shown in Fig. 1.

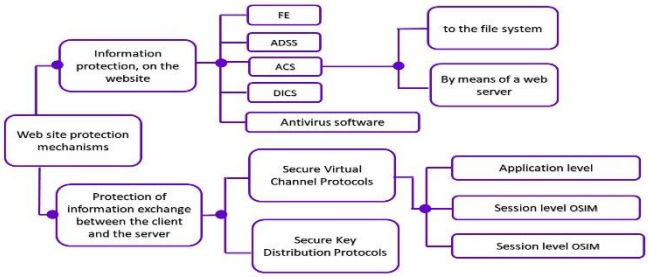

Fig. 1. Website protection mechanisms.

ACS (access control system).

DICS (Data Integrity Control System).

FE (firewall).

ADSS (attack detection system).

OSIM (Open Systems Interaction model).

Any commercial site is at risk of external influence by default – attackers use dozens of ways to hack web pages, regardless of the platform they are made on [11].

The list of "classic" types of attacks [12]:

- SQL injections;
- Cross-site Scripting (XSS);
- Remote Code Execution (RCE);
- Cross-site Request Forgery (CSRF);
- Local and remote inclusion (LFI, RFI);
- Authorization bypass options;
- Automated password selection (Bruteforce).

It is concerning that 85% of websites that use PHP (Hypertext Preprocessor) [13] are at a high risk of dangerous attacks. Even conventional technology websites can be vulnerable to hacking or "dropping" if they don't have enough protection. All websites are at risk of attacks unless they have special safeguards - but even those safeguards have limitations

[14]. Therefore, it's not surprising that attackers are continually improving their tactics and targeting both individuals and corporations.

This research work analyzed the website (www.aliyaschool.kz), which serves as the subject of the study. Due to the pandemic and self-isolation measures, traditional education shifted to online education, making it a crucial part of many fields. Unfortunately, there has been an increase in copyright infringement cases where content is used without permission. To prevent potential material and moral losses, it's essential to safeguard against plagiarism and fraud even before the online course is launched for sale. Therefore, it's necessary to prioritize the security of online course content to prevent theft, distortion, and unauthorized access.

A web course site review was conducted, and Webrate [15] presented statistics revealing a daily traffic volume of 219 unique visitors and 1228 page views. Fig. 2 displays general information about the site.

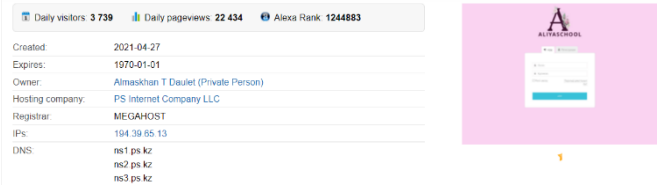

Fig. 2. General information of the studied web course.

Each visitor makes an average of about 3739 page views (Fig. 3). According to the Alexa Rank statistical ranking system [16], aliyaschool.kz traffic occupies 49,006 positions worldwide, while the most significant number of its visitors is from Kazakhstan (Fig. 4), which occupies 211th place. According to these data, there is a demand for web course resources. Therefore, there is a reason to attack it.

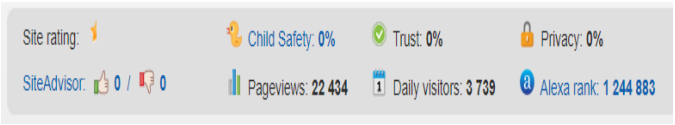

Fig. 3. Web course statistics information.

Fig. 5 shows how many visitors visited the website daily for the past 90 days. The last record was on Oct 4, 2022, and about 3,400 visitors visited this site.

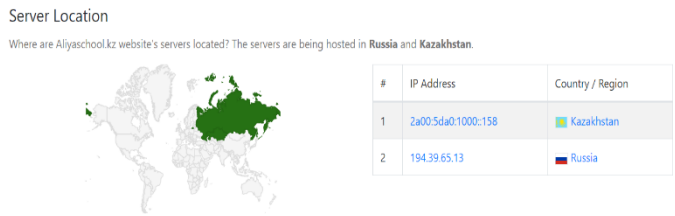

Fig. 4. Server location.

In Yandex.Metrica, a sharp surge in direct visits to the site was detected for the area under study, and mobile traffic also increased sharply - direct visits during the day are distributed evenly over time. Therefore, we analyzed the web browser and monitored the data, and concluded that the site was under attack (Fig. 6).

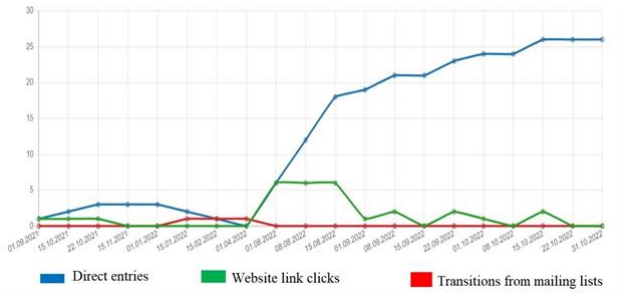

Fig. 5. Web course attendance information.

DDoS attacks (Distributed Denial of Service) are one of the most prevalent and damaging forms of cyberattacks on the internet today. Hundreds of thousands of websites, including government institutions, businesses, media outlets, and non-profit organizations, fall victim to these attacks daily. Unfortunately, attackers continue to develop sophisticated methods to disrupt and block access to internet resources and servers. While there are several effective methods for protecting against DDoS attacks, the increasing complexity of these attacks and the decreasing cost of computing resources means that more than basic protection is required.

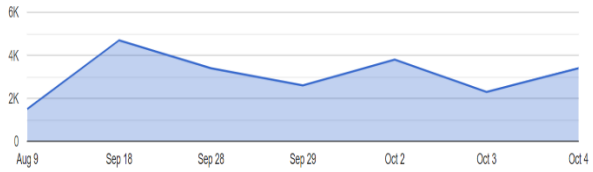

Fig. 6. Web course traffic analysis.

IV. Blockchain Technologies

Initially, blockchain technology was only associated with cryptocurrency. However, over time, this method of data storage has found various applications since the blockchain can contain any digital information about transactions, legal documents, and media files, including photos, video, and audio.

Blockchain technology, as a decentralized environment for storing and executing programs, ensures the immutability of stored data, protecting web applications from unauthorized changes to site scripts and database contents [17]. The load is distributed over devices with identical data, protecting against DDoS attacks [18]. Special libraries track and automatically block malicious requests, protecting servers from unauthorized access [19]. Blockchain technology can protect web applications from cyber-attacks and data leaks. Blockchain technology can be used to build decentralized and distributed networks that can provide DDoS protection and high availability for web applications.

To begin, let's examine the process of constructing a blockchain. Blockchain technology is a decentralized, distributed database governed by many contributors and available to all [20]. It is not a collection of several large databases managed centrally. Data related to each batch of confirmed transactions is stored in a separate block. Each such block is connected to the previous one, as shown in Fig. 7. As information is added, new blocks are created. To include them

in the chain, it is necessary to confirm all participants of the entire network [21].

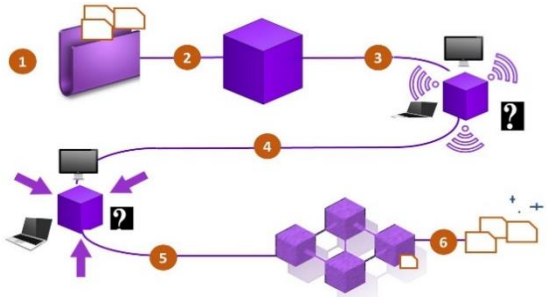

Fig. 7. Blockchain structure.

1) A wants to send money to B.

2) Transactions are transferred to the network and collected in a new "block".

3) Blocks are sent out for verification to all participants of the system

4) Each participant writes a block to their database instance.

5) The block falls into the "blockchain", which contains information about all transactions.

6) The transaction is completed.

2008 marked a significant turning point for the internet when an individual or group, using the pseudonym Satoshi Nakamoto, released a White Paper detailing a decentralized peer-to-peer electronic payment system called Bitcoin. Satoshi Nakamoto, the creator of blockchain technology, remains unidentified to this day. Recently, Bloomberg corroborated claims that Satoshi is Hal Finney. It's worth noting that Bitcoin is the first iteration of blockchain technology.

It works as a decentralized payment system with simple, smart contracts - conditions for a transaction. The problem is that they need more capabilities.

The second generation is Ethereum [22]. It began with the launch of the eponymous network in 2015. Then, for the first time, developers implemented the advanced functionality of smart contracts [23]. The history of development is shown in Fig. 8.

Blockchain today consists of various cryptocurrencies, NFT tokens [24], crypto exchanges and wallets, stock markets where virtual assets are traded, and much more [25] (see Fig. 8). It is easy to forge paper documents with a hand signature because the source code, a ballpoint pen, and a desire are enough. Electronic documents are stored centrally in one extensive archive, and people enter information into registers, causing them to be susceptible to changes [26]. Legal norms are not sufficient for ensuring document authenticity. The only viable solution is to develop a technical solution.

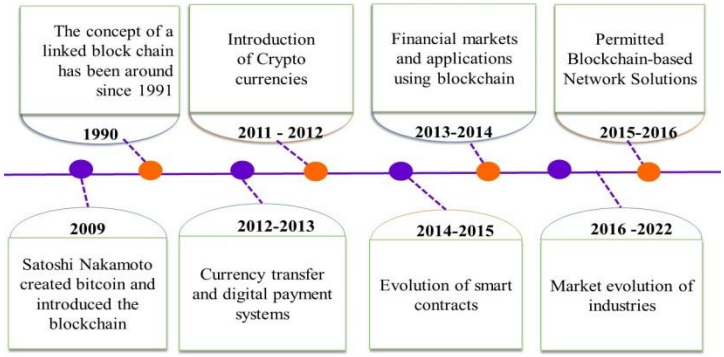

Fig. 8. Blockchain history.

In 1991, American cryptographers Stuart Haber and Scott Starnet came up with an idea to put time stamps on electronic documents, making them impossible to issue retroactively or forge [27]. The documents were sorted by the same marks and collected into one block, forming the prototype of the blockchain. A year later, the technology was improved, including Merkle trees, which made it possible to store more documents in one block.

Another technology that contributed to the emergence of blockchain is a decentralized peer-to-peer network [28]. In such a network, there are typically no dedicated servers, and each node performs the server and client functions. Based on the characteristics and functional features of the blockchain, three types of networks are distinguished: public, private, and consortium, as shown in Fig. 9 [29].

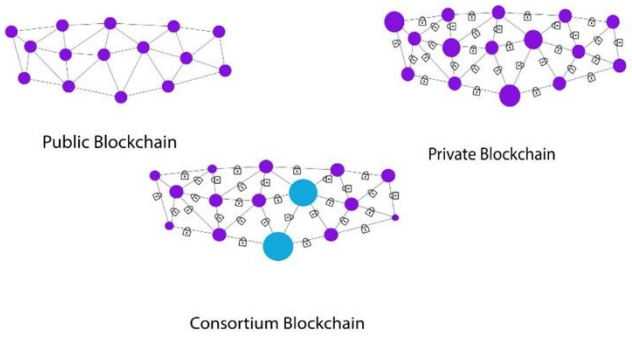

Fig. 9. Types of blockchain network.

According to the source [30], a public blockchain allows any internet user to join or leave the blockchain network without providing identification forms or seeking permission.

A private blockchain [31] assumes that all network participants are known and trustworthy; belong to a controlled community. Subjects can be individuals, such as employees, customers, and organizations (companies or departments within companies). Private network users can have certain types of access to write to the registry. Private Blockchain contains the majority of corporate, industrial, and government projects. Various other actors may have different personal read-only representations of the data (e.g., regulatory officials).

The consortium's blockchain combines elements of a public and private blockchain [32]. An authorized group functions as a validator; validators or authorized persons can limit the network's visibility or have no restrictions.

An essential innovation of the Blockchain protocol is the consensus matching algorithm, which allows you to build an open distributed network where all actors can agree [33]. This mechanism ensures overall reliability in a distributed network of registers. It is assumed that 51% coordinates the content stored in the registers network.

Public Blockchain agreement algorithms for "Proof of Work" (PoW) are shown in Fig. 10 [34].

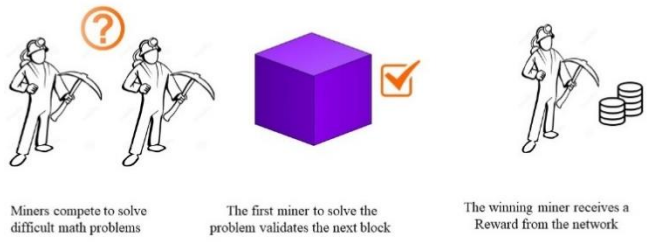

Fig. 10. Proof of work.

"Proof of Stake" is shown in Fig. 11 (Proof of Stake (PoS) is the most common and popular consensus algorithm.

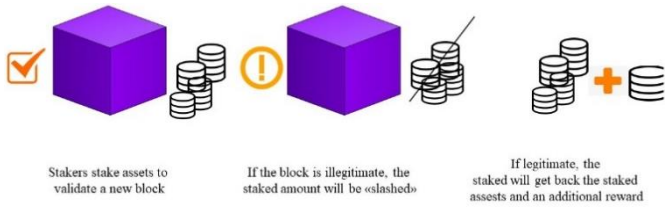

Fig. 11. Proof of stake.

The Proof-of-Work (PoW) algorithm is designed to require all nodes in the network to compete for a reward when adding a block of records to the end of the chain. This competition involves finding a one-time number using computing power [35].

This creates an incentive model in which the winning node that adds a block to the blockchain is rewarded with digital tokens – bitcoins. To hack the network, an attacker must fight for the right to add a block and compete to create the longest chain.

This undermines the economic incentives of attacks, making them financially costly (the type of attack is Sybil's attack). The Proof of Stake (PoS) algorithm assumes that the miner or validator who creates a new block is chosen deterministically depending on his wealth or share [36].

Open-type blockchains are suitable for a broad community and mainly for solving private tasks, such as exchanging cryptocurrency between users or concluding small transactions using smart contracts [37]. For corporate networks, it is advisable to use a closed type, which allows you to hide certain information. Consensus algorithms are vital for blockchains to remain fully decentralized. Due to the decentralized nature of the blockchain, there will never be a centralized authority that checks and updates the register with transactions and new data. Therefore, stakeholders in the network should decide on an equal basis which transactions should be added to the blockchain.

For corporate networks, it is advisable to use the closed type, which allows you to hide certain information. Consensus algorithms are vital for blockchains to remain fully decentralized. Due to the decentralized nature of the blockchain, there will never be a centralized authority to verify and update the ledger with transactions and new data. Therefore, the stakeholders in the network must decide on an equitable basis which transactions should be added to the blockchain.

A. Hashing is the Basis of Blockchain Functioning

Cryptographic hash functions are prevalent [38]. They store passwords during authentication, protect data in file verification systems, detect malicious software, and encode information in the blockchain (the block is the central primitive processed by Bitcoin and Ethereum). This article will review hashing algorithms: what is it, what types are there, and what properties they have.

A significant contribution to the development was made by Hashcash, the proof—of—work algorithm developed by Adam Back. It worked like this: each email user added a text stamp to the email header, indicating that the sender had spent some of his time and resources calculating this stamp. The algorithm significantly complicated spam and DDoS attacks on mail servers [39].

A hash function is called any function h:

X -> Y, easily computable and such that for any message, M is the value;

h (M) = H (convolution) has a fixed bit length;

X is the set of all messages;

Y is a set of binary vectors of fixed length.

As a rule, hash functions are built based on the so-called one—step compression functions $y = f(x_1, x_2)$ of two variables, where x_1, x_2, and y are binary vectors of length m, n, and n, respectively, and n is the convolution length, and m is the length of the message block.

To obtain the value of h(M), the message is first divided into blocks of length m (in this case, if the message length is not a multiple of m, then the last block is supplemented to the full in some unique way), and then the following sequential convolution calculation procedure is applied to the resulting blocks M_1, M_2,.., M_N:

$$H_o = v,$$

$$H_i = f(M_i, H_{i-1}),\ i = 1,.., N,$$

$$h(M) = H_N$$

Here v is some constant, it is often called an initializing vector. It is chosen for various reasons and can be a secret constant or a set of random data (for example, a date and time sample). With this approach, the properties of the hash function

are entirely determined by the properties of the one-step compression function [40].

There are many cryptographic algorithms out there these days. They vary in complexity, digit capacity, cryptographic reliability, and operation features. However, hashing algorithms are a familiar idea. They appeared more than half a century ago, and there have been little changes from a fundamental point of view for many years [41-42]. However, because of its development, data hashing has acquired many new properties, so its application in information technology has already become universal. In our study, we analyzed cryptographic hash functions.

Comparison of Cryptographic hash functions:

The Secure Hash algorithms are a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as the U.S. Federal Information Processing Standard (FIPS), including [43]:

- SHA-0: A retronym applied to the original version of the 160-bit hash function published in 1993 under the name "SHA". It was withdrawn shortly after publication due to an undisclosed "significant flaw" and replaced with a slightly modified version of SHA-1.
- SHA-1: 160-bit hash function, reminiscent of the earlier MD5 algorithm. This was developed by the National Security Agency (NSA) as part of a digital signature algorithm. Unfortunately, cryptography weaknesses were discovered in SHA1, and after 2010 the standard was no longer approved for most cryptographic applications.
- SHA-2: A family of two similar hash functions with different block sizes, known as SHA-256 and SHA-512. They differ in word size; SHA-256 uses 32-byte words, and SHA-512 - 64- byte words. There are also truncated versions of each standard known as SHA-224, SHA-384, SHA-512/224, and SHA-512/256. The NSA also developed them.
- SHA-3: A hash function, formerly Keccak, was selected in 2012 after an open competition among non-NSA designers. It supports the same hash length as SHA-2, and its internal structure differs significantly from the actors of the SHA family. Table I compares general and technical information for several cryptographic hash functions.

In blockchain technology, all blocks are interconnected by a complex cryptographic signature called a hash - it is created using complex mathematical algorithms, looks like a generator of letters and numbers, and contains 1024 characters. After the transaction is completed and written to the block, all network nodes receive data about it. In simple terms, a node is a separate computer where the complete and most up-to-date copy of the blockchain is stored [44]. Whenever a new block appears on the network, all nodes update their blockchain.

Most of the current classes of attacks on websites fall on the stage of user authorization, namely the process of transferring identification and authentication data from the user to the website database [45].

In our study, we show login and password hashing using several algorithms and compare their parameters shown in Fig. 12.

Currently, only SHA2 and SHA-3 groups are considered secure. At the same time, it should be regarded that the more characters in the resulting hash in Fig. 12, the more difficult it is to select it. Results of algorithm security analysis hashing against attacks are shown in Fig. 13, which shows the speed of various hashing functions based on the experimental studies of the authors. For hash rate comparison, we use the Intel Iris Xe Graphics G7 96EUs laptop graphics system, which belongs to the Tiger Lake GT2 family and is currently the most powerful integrated graphics.

TABLE I. COMPARISON OF SHA FUNCTIONS

Algorithms	Output size (bits)	Internal state size (bits)	Block Size (bits)	Round	Operations	First published
MD5	128	128	512	64	And, Xor, Rot, Add (mod 2 32), or	1992
SHA-0	160	160	512	80	And, Xor, Rot, Add (mod 2 32), or	1993
SHA-1						1995
SHA-224 SHA-256	224 256	256	512	64	And, Xor, Rot, Add (mod 2 32), Or, Shr	2004 2001
SHA-384 SHA-512	384 512	512	1024	80	And, Xor, Rot, Add (mod 2 64), Or, Shr	2001
SHA-512/224 SHA-512/256	224 256					2012
SHA3-224 SHA3-256 SHA3-384 SHA3-512	224 256 384 512	1600	1152 1088 832 576	24	And, Xor, Rot, Not	2015
SHAKE 128 SHAKE 256	d (arbitrary) d (arbitrary)		1344 1088			

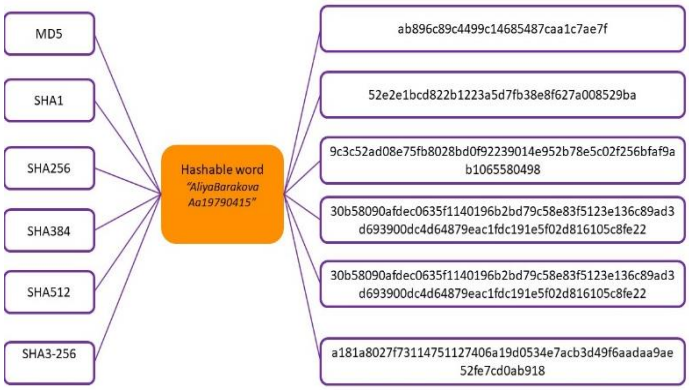

Fig. 12. The result of hashing the username and password.

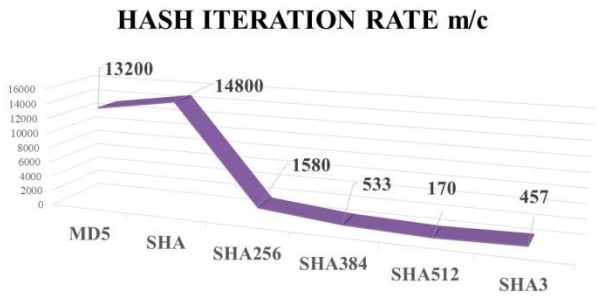

Fig. 13. Hash brute force values on a modern video card INTEL R IRIS R XE GRAPHICS.

As shown in Fig. 13, SHA512 and SHA3 algorithms and algorithms based on block encryption are the best among the given values regarding hashing speed. With different implementations, the absolute values of hashing rates may vary, but the ratio between their speeds will be maintained.

Hashing functions are widely used to verify data integrity [46]. For example, many software vendors publish their checksums together with the software. After downloading the file, you need to feed it to the hash function and then compare the produced hash with what the software developer published.

In the blockchain, a hash guarantees the block's integrity [47]. Unfortunately, the input data for the hashing algorithm contains the hash of the previous block, which makes it impossible (or at least very difficult) to change the block in the chain: you will have to recalculate the hash of the block itself, as well as the hashes of all the blocks following it.

B. Securing Web Course Transactions

Using blockchain technologies for online course transactions can significantly increase the trust and attractiveness of these courses in users' eyes. Blockchain technologies provide unique opportunities to ensure the security of web course transactions. They allow you to guarantee the integrity of data and their reliable protection against cyber-attacks and fraud. Furthermore, due to transparency and decentralization, the blockchain facilitates the payment process and is convenient for storing information about participants and their achievements.

The use of blockchain technology for web course transactions has many advantages. It allows you to ensure the security and transparency of buying and using courses, simplifies the payment process, and improves the ability to manage finances and monitor the use of the course.

Consider building a transaction block model based on blockchain technology for the web course under study. This article proposes to build a block model using lines of code in Node JS. Node (or, more formally, Node.js) is an open-source, cross-platform runtime that allows developers to create server-side tools and applications using JavaScript.

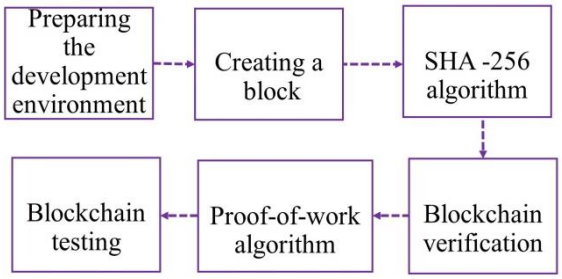

Fig. 14. The general structure of our blockchain.

Our blockchain (see Fig. 14) will be a chain of blocks, and every block will include the following:

- block number [index];
- timestamp [timestamp];
- the value of the hash sum of the previous block [previous hash];
- the value of the hash sum of the current block [hash].

We will include in the transaction content the sender of the funds [sender], the name of the recipient of these funds [recipient], and the amount of funds transferred [amount]. We will include information about only one transaction to the block for simplicity.

A new Blockchain.js file is used to create the block class, here, we create a blog class. This work uses the SHA 256 algorithm. First, a hash function is created. Next, to implement the hashing process, it is necessary to use the built-in crypto package from Node.js.

```
class Block {
   constructor(timestamp = " ", data=[]) {
      this.timestamp = timestamp;
      this.data = data;
      this.data = this.getHash();
      this.prevHash = "";    }
   getHash() {
        return SHA256(this.prevHash + this.timestamp +
JSON.stringify(this.data));  }}
   const crypto = require('crypto'), SHA256 = message =>
crypto.createHash("SHA256").
   update(message).digest('hex');
    class Blockchain{
   constructor () {
       this.chain = [new Block(Date.now().toString())];          }
         getlastblock() {
            return this.chain[this.chain.length - 1];}
   addBlock(block){
      block.prevHash = this.getlastblock().hash;
      block.hash=block.getHash();
```

```
        this.chain.push(Object.freeze(block));}
          isValid(blockchain = this) {
           for(let i = 1; i < blockchain.chain.length; i++) {
              const currentBlock = blockchain.chain[i];
              const prevBlock = blockchain.chain[i-1];
              if(currentBlock.hash !==currentBlock.getHash() ||
prevBlock.hash
                !==currentBlock.prevHash) {
                  return false;  }  }
            return true;}  }
        module.exports = {Block, Blockchain}
```

Timestamp is a sequence of symbols or encoded information showing when a particular event occurred. Usually indicates the date and time, respectively. With some data, we will get a hash, and we will also have the hash of the previous block. To do this, we will create a const crypto. If something changes every time, then SHA 256 will give us something completely different, and this can guarantee us immutability. In this case, the PrevHash property also plays a significant role in constancy. It ensures that the blocks will remain unchanged throughout the life of our blockchain. Accordingly, if the previous hash does not match, this block will not pass validation, respectively.

Next, let's move on to the next class, and we will create a blockchain class. The first thing we need is a genesis block. The Genesis block is our first block, and technically we have the main first block. Next, we also need to create a function with the last block. There are several functions here. Firstly, this function is for getting the previous block and also a process for adding a block to our blockchain. Finally, we need to know if our chain is valid and a method to check the validation.

Do we have a chain if the block's hash is equal to what its hashing method returns and the prevHash property of the block should be similar to the previous block? Accordingly, we check whether our blockchain is valid and coincides with our expectations. To do this, we export everything. Now let's go to another file stored in the same folder. Let's call it Index.js, and we need to add some data here. This is, firstly, the block, the blockchain that we exported, and the path to this file.

Next, we need to create the blockchain itself. Let's call it TEST. Then we will create an object of our blockchain. Next, we will create a block using this function.

```
        const test = new Blockchain();
        test.addBlock(new Block(Date.now().toString(), {from: "Alia", to:
"Olgaa", amount: 10}));
        test.addBlock(new Block(Date.now().toString(), {from: "Zhazira",
to: "Aliya", amount: 20}));
        test.addBlock(new Block(Date.now().toString(), {from: "Asel", to:
"Baglan", amount: 15}));
        test.addBlock(new Block(Date.now().toString(), {from: "Alma", to:
"Marat", amount: 25}));
```

Here we will indicate certain data. Here we will have from whom this or that transaction comes, for example, Aliya, then there is a value to whom this block goes, for example, "Olga". Next, write down the number of transactions. In this case, we have created four blocks. And further, we need to add a console to display everything from our block.

```
    console.log(test.chain)
    В данном случае мы видим на наш блокчейн
    PS C:\Blockchain> node index.js
    [
      Block {
        timestamp: '1666506048577',
        data:
'fd4b1de75b9fb1ac48ebeb12f3f306a2fd4c6227857b3f96deb2974e13974b86',
        prevHash: ''
      },
      Block {
        timestamp: '1666506048577',
        data:
'0013e76e5a7dc2a11c7caa2a0dff5e62e7557f831860f514581b8b8d616e2445',
        prevHash: undefined,
        hash:
'785d2b99afa9f2a13cf646a6a9e7d8366c523d39c0551bbd021a2e8b9e8d9d3a'
      },
      Block {
        timestamp: '1666506048577',
        data:
'eeae9571d9e0af0aa408ccfa5e94c495c3d66b8f7d80d273a47cad90f00e2884',
        prevHash:
'785d2b99afa9f2a13cf646a6a9e7d8366c523d39c0551bbd021a2e8b9e8d9d3a',
        hash:
'9170bfe54dc9b7bb70870edc403558f2f8f6222367ceb5a87790f91efd99777e'
      },
      Block {
        timestamp: '1666506048577',
        data:
'f3f9760c6f28dff8401da4003c3b7b2ccc8d26f62fb23b0b1036c3d3f3415959',
        prevHash:
'9170bfe54dc9b7bb70870edc403558f2f8f6222367ceb5a87790f91efd99777e',
        hash:
'661c470d5bc849d9d51cdeb41d73cb3d83fccc2a2a77ecde28f309114d1c0db4'
      },
      Block {
        timestamp: '1666506048577',
        data:
'f510198c0fc3ede70add6b98bf288dd4bba5584a9027a5eed94af73ec6e846df',
        prevHash:
'661c470d5bc849d9d51cdeb41d73cb3d83fccc2a2a77ecde28f309114d1c0db4'
,
        hash:
'700a5215a94fa8088cb061349c5605aa4616257c4c2e9d550852f61fbb863e38'
      }

    ]
```

V. Result and Discussion

As a result, there is a hash and a previous hash of the last block, respectively. We can compare it with the genesis block, which is shown in Fig. 15. The genesis block is the very first block in the blockchain. We can imagine a blockchain as a series of blocks where each block is connected to its previous block and replicated all over the blocks. The fundamental benefit of this replication is that, in case one of the replicated blocks becomes corrupted, other copies are available to ensure the integrity of the information contained in the data structure. Furthermore, replication provides assurance of the reliability of the data, conveyed as a guarantee that the different computers involved in the blockchain [48,49] platform are running appropriate calculations to ensure the consistency and reliability of the data. In general, our blockchain will look like this. Therefore, blockchain is one of the ways to store data and protect it by making it immutable.

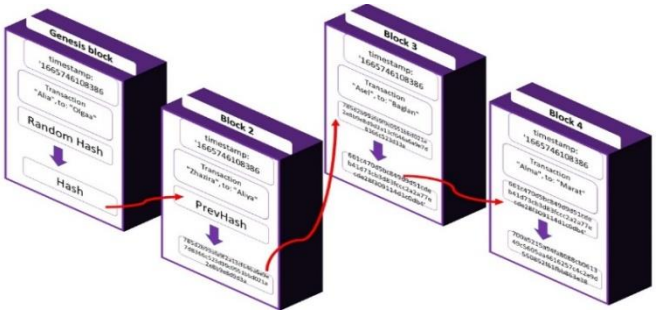

Fig. 15. Type of created blockchain.

VI. CONCLUSIONS

This research paper provides statistical data from analyzing the studied web course as an experiment. In addition to the standard methods of protecting websites, blockchain technology was studied, and a comparative analysis of hashing algorithms was given for further use when modifying an authentication system. Finally, a model of the transaction block of the analyzed web course based on blockchain technology was built.

In conclusion, it can be noted that most of the current classes of attacks on websites occur during the user authorization stage, namely the process of transferring identification and authentication data from the user to the website database. Although blockchain technology has great potential in authentication systems and provides high security against fraud and forgery, making it especially attractive to provide web resources, it is essential to address technical and organizational issues such as scalability, standardization, and regulation to enable widespread use of blockchain technology in authentication systems. Nevertheless, blockchain technology in authentication systems promises significant benefits for all stakeholders and may become one of the essential cybersecurity trends in the near future.

Further research should focus on developing an authentication system based on blockchain technology using a modified hashing algorithm.

REFERENCES

[1] Bugliesi M., Calzavara S., Focardi R. Formal methods for Web security // Journal of Logical and Algebraic Methods in Programming. 2017. Vol. 87. P. 110–126.

[2] Mercer D. Creation of reliable and fully functional websites, blogs, forums, portals, and community sites. Williams - M., 2018. 272 p.

[3] Bugliesi M., Calzavara S., Focardi R. Formal methods for Web security // Journal of Logical and Algebraic Methods in Programming. 2017. Vol. 87. P. 110–126.

[4] Choo K.-K. R., Ashman H. Web application protection techniques: A taxonomy // Journal of Network and Computer Applications. 2016. Vol. 60. P. 95–112.

[5] Sathya AR and Barnali Gupta Banik, "A Comprehensive Study of Blockchain Services: Future of Cryptography" International Journal of Advanced Computer Science and Applications(IJACSA), 11(10), 2020. http://dx.doi.org/10.14569/IJACSA.2020.0111037.

[6] Ahmed Alrehaili, Abdallah Namoun and Ali Tufail, "A Comparative Analysis of Scalability Issues within Blockchain-based Solutions in the Internet of Things" International Journal of Advanced Computer Science and Applications(IJACSA), 12(9), 2021. http://dx.doi.org/10.14569/IJACSA.2021.0120955.

[7] Sabri Hisham, Mokhairi Makhtar and Azwa Abdul Aziz, "Combining Multiple Classifiers using Ensemble Method for Anomaly Detection in Blockchain Networks: A Comprehensive Review" International Journal of Advanced Computer Science and Applications(IJACSA), 13(8), 2022. http://dx.doi.org/10.14569/IJACSA.2022.0130848.

[8] Naresh Kshetri, Chandra Sekhar Bhushal, Purnendu Shekhar Pandey and Vasudha, "BCT-CS: Blockchain Technology Applications for Cyber Defense and Cybersecurity: A Survey and Solutions" International Journal of Advanced Computer Science and Applications(ijacsa), 13(11), 2022. http://dx.doi.org/10.14569/IJACSA.2022.0131140.

[9] Moh M., Pininti S., Doddapaneni S., Moh T.-S. Detecting Web Attacks Using Multi-stage Log Analysis // IEEE 6th International Conference on Advanced Computing 2016 (IACC). — 2016. P. 733–738.

[10] Z. Shahbazi and Y.-C. Byun, "A framework of vehicular security and demand service prediction based on data analysis integrated with blockchain approach", Sensors, vol. 21, no. 10, p. 3314, May 2021.

[11] Khanna S., Verma A. K. Classification of SQL injection attacks using fuzzy tainting // Advances in Intelligent Systems and Computing. 2018. Vol. 518. P. 463–469.

[12] Sonewar P. A., Thosar S. D. Detection of SQL injection and XSS attacks in three-tier web applications // International Conference on Computing Communication Control and automation 2016 (ICCUBEA). — 2017.

[13] Palchevsky, E.V. Development of a system for analyzing and blocking requests to a web server in the PHP programming language / E.V. Palchevsky, A.R. Khalikov // Innovative scientific research: theory, methodology, practice. Publishing house: "World of Science", Chisinau, 2017. - P. 80-83.

[14] S. Nyssanbayeva, W. Wojcik, O. Ussatova «Algorithm for generating temporary password based on the two-factor authentication model» // Przegląd Elektrotechniczny, Poland, № 5, 2019., ISSN 0033-2097, R. 95, P. 101 – 106.

[15] WEBrate // https://webrate.org/site/aliyaschool.kz/.

[16] Alexa rate // https://metrika.yandex.ru/list?search=aliyaschool.kz&type=all&sortField=counter&sortDirection=asc.

[17] O. Ussatova, S. Nyssanbayeva, W. Wojcik «Modeling of the user's identification security system on the 2fa base» // Intl Journal Of Electronics And Telecommunications, 2021, VOL. 67, NO. 2, PP. 235-240.

[18] Santos R., Souza D., Santo W., Ribeiro A. & Moreno E. Machine learning algorithms to detect DDoS at № 3, 2020 information management systems 69 information protection tacks in SDN. Concurrency and Computation: Practice and Experience, 2019, e5402. DOI:10.1002/cpe.5402.

[19] Olga Ussatova, Aidana Zhumabekova, Yenlik Begimbayeva, Eric T. Matson and Nikita Ussatov, «Comprehensive DDoS Attack Classification Using Machine Learning Algorithms»//CMC-Computer, Materials & Continua. Tech Science Press. Volume 73, Number 1, 2022, PP.577-594.

[20] Ussatova O.A., Barakova A.Sh. "Analysis of modern systems for protecting web resources" // Proceedings of the National Academy of Sciences of the Republic of Kazakhstan No. 1 (341), Almaty, 2022. p. 88-95.

[21] S. Mambetov, Y. Begimbayeva, S. Joldasbayev, and G. Kazbekova, "Internet threats and ways to protect against them: A brief review," 2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2023, pp. 195-198, doi: 10.1109/Confluence56041.2023.10048858.

[22] Roy Lai, David Lee, Kuo Chuen. Blockchain – From Public to Private. Handbook of Blockchain, Digital Finance, and Inclusion. Vol. 2 (2018). Elsevier, pp. 146–177. DOI:10.1016/B978-0-12-812282-2.00007-3.

[23] Liu, Z.; Yin, X. LSTM-CGAN: Towards Generating Low-Rate DDoS Adversarial Samples for Blockchain-Based Wireless Network Detection Models. IEEE Access 2021, 9, 22616–22625.

[24] Genkin, A. Blockchain. How it works and what awaits us tomorrow / A. Genkin. - Moscow: Alpina Publisher, 2018. - 804 p.

[25] Rondelet, A.; Zajac, M. ZETH: On integrating Zerocash on Ethereum. arXiv 2019, doi.org/10.48550/arXiv.1904.00905.

[26] Chang, S.E.; Chen, Y.; Lu, M.; Luo, H.L. Development and Evaluation of a Smart Contract–Enabled Blockchain System for Home Care Service Innovation: Mixed Methods Study. JMIR Med. Inform. 2020, 8, e15472.

[27] Cong, X.; Zi, L. DTNB: A blockchain transaction framework with discrete token negotiation for the delay tolerant network. IEEE Trans. Netw. Sci. Eng. 2021.

[28] Bonneau, J.; Miller, A.; Clark, J.; Narayanan, A.; Kroll, J.A.; Felten, E.W. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 18–20 May 2015; pp. 104–121.

[29] Puthal, D.; Mohanty, S.; Kougianos, E.; Das, G. When Do We Need the Blockchain? IEEE Consum. Electron. Mag. 2021, 10, 53–56.

[30] Liu, Z.; Yin, X. LSTM-CGAN: Towards Generating Low-Rate DDoS Adversarial Samples for Blockchain-Based Wireless Network Detection Models. IEEE Access 2021, 9, 22616–22625.

[31] Abdella, J.; Tari, Z.; Anwar, A.; Mahmood, A.; Han, F. An Architecture and Performance Evaluation of Blockchain-based Peer-to-Peer Energy Trading. IEEE Trans. Smart Grid 2021.

[32] Leksieva, V.; Valchanov, H.; Huliyan, A. Smart Contracts based on Private and Public Blockchains for Insurance Services. In Proceedings of the 2020 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 1–3 October 2020; pp. 1–4.

[33] Cagigas, D.; Clifton, J.; Diaz-Fuentes, D.; Fernández-Gutiérrez, M. Blockchain for Public Services: A Systematic Literature Review. IEEE Access 2021, 9, 13904–13921.

[34] Cagigas, D.; Clifton, J.; Diaz-Fuentes, D.; Fernández-Gutiérrez, M. Blockchain for Public Services: A Systematic Literature Review. IEEE Access 2021, 9, 13904–13921.

[35] Sun, G.; Dai, M.; Sun, J.; Yu, H. Voting-based Decentralized Consensus Design for Improving the Efficiency and Security of Consortium Blockchain. IEEE Internet Things 2020, 8, 6257–6272.

[36] Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Heal. Inform. J. 2019, 25, 1398–1411.

[37] Nair, P.R.; Dorai, D.R. Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain. In Proceedings of the 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 4–6 February 2021; pp. 279–283.

[38] Machacek, T.; Biswal, M.; Misra, S. Proof of X: Experimental Insights on Blockchain Consensus Algorithms in Energy Markets. In Proceedings of the 2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 15–19 September 2021; pp. 1–5.

[39] Omar, I.A.; Jayaraman, R.; Debe, M.S.; Salah, K.; Yaqoob, I.; Omar, M. Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts. IEEE Access 2021, 9, 37397–37409.

[40] Emmanuel, A.; Adeniyi; Peace Busola Falola; Mashael, S; Maashi; Mohammed, Aljebreen; Salil Bharany. Secure Sensitive Data Sharing Using RSA and ElGamal Cryptographic Algorithms with Hash Functions. Information 2022, 13(10), 442; https://doi.org/10.3390/info13100442.

[41] Balasundaram, P.; Muralidharan, S.; Bijoy, S. An mproved Content Based Image Retrieval System using Unsupervised Deep Neural Network and Locality Sensitive Hashing. In Proceedings of the 2021 5th International Conference on Computer, Communication, and Signal Processing, ICCCSP 2021, Chennai, India, 24–25 May 2021; pp. 65–71.

[42] Lai, H.; Pan, Y.; Ye, L.; Yan, S. Simultaneous Feature Learning and Hash Coding with Deep Neural Networks. In Proceedings of the IEEE International Conference on Pattern Recognition and Computer Vision, Boston, MA, USA, 7–12 June 2015; pp. 3270–3278.

[43] Emmanuel, A.A.; Okeyinka, A.E.; Adebiyi, M.O.; Asani, E.O. A Note on Time and Space Complexity of RSA and ElGamal Cryptographic Algorithms. Int. J. Adv. Comput. Sci. Appl. 2021, 12, 143–147.

[44] Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. BEdgeHealth: A Decentralized Architecture for Edge-based IoMT Networks Using Blockchain. IEEE Internet Things J. 2021.

[45] Haque, E.; Zobaed, S.; Islam, M.U.; Areef, F.M. Performance Analysis of Cryptographic Algorithms for Selecting Better Utilization on Resource Constraint Devices. In Proceedings of the 2018 21st International Conference of Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 21–23 December 2018; pp. 1–6.

[46] Zhang, L.; Ge, Y. Identity Authentication Based on Domestic Commercial Cryptography with Blockchain in the Heterogeneous Alliance Network. In Proceedings of the 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China, 15–17 January 2021; pp. 191–195.

[47] Intel® Iris® Xe Graphics Available online: https://ark.intel.com/content/www/us/en/ark/products/graphics/205778/intel-iris-xe-graphics.html.

[48] Steichen, M.; Fiz Pontiveros, B.; Norvill, R.; Shbair, W. Blockchain-Based, Decentralized Access Control for IPFS. In Proceedings of the 2018 IEEE International Conference on Blockchain (Blockchain-2018), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1499–1506.

[49] Piyush Panta, Anand Singh Rajawatb, S.B.Goyalc, Pradeep Bedid, Chaman Vermae, Maria Simona Raboacaf, Florentina Magda Enescug. Authentication and Authorization in Modern Web Apps for Data Security Using Nodejs and Role of Dark Web. DOI:10.1016/j.procs.2022.12.080.