Model of Using Blockchain Technology to Secure Digital Financial Transactions

Volodymyr Nakonechnyi[1,*,†], Volodymyr Saiko[1,†], Oleksandr Pliushch[1,†], Vladyslav Lutsenko[1,†] and Mykola Mordvyntsev[2,†]

[1] *Taras Shevchenko National University of Kyiv, 24 Bohdana Havrylyshyn str., 04116, Kyiv, Ukraine*
[2] *Kharkiv National University of Internal Affairs*

Abstract

One of the main reasons for data breaches is human mistake, which can be greatly reduced by enterprises to make their transactions more impenetrable and less vulnerable to eavesdropping. Blockchain is merging with essential company processes and is becoming synonymous with every vertical sector worldwide. Blockchain technology is entirely decentralized and records data and processes transactions utilizing several computers connected to a network using a ledger-based approach. The ability to add any digital asset to the chain and start a transaction is the finest thing about blockchain. In contrast to conventional banking systems, there won't be any middlemen and data will always be safe. Blockchain is a distributed ledger where data is gathered in "blocks" and transactions are broadcast to all participants who are working on their verification. This kind of distributed ledger, which is a network of blocks, is known as "blockchain" technology as the ledger is made up of discrete but linked blocks. Because every computer on the network has a copy of the blockchain, users can rapidly confirm transactions and stop fraud. This article analyzes the technical aspects of blockchain technology, as well as how it affects society and the financial system. On the basis of the research conducted in this work, the method of protecting payment data using blockchain technology was further developed.

Keywords

Blockchain, banking, database, online, transaction, financial institutions, cryptography.

1. Introduction

A more specific description of a blockchain is as follows: a type of data in a blockchain is a data block structure linked in a way that continuously combines time series, which, to some extent, prevents non-encrypted manipulation. The so-called blockchain technology, which employs the construction of blockchain data to verify and save data, is a novel distributed infrastructure and computing approach, according to a broad definition. Data is generated and changed using a distributed node consistency mechanism, while security is provided via cryptography [1].

The phrase "capital markets" describes the process of connecting investor capital demand with issuers that have the appropriate risk and return profiles. The process of acquiring capital can be difficult for issuers, whether they are business owners, startups, or major corporations.

SHA-256 is the main hash algorithm used by Bitcoin and several other cryptocurrencies. In Bitcoin, it is used for hashing of blocks, transactions and other data, as well as for Proof-of-Work (proof of work) algorithm, which requires solving a complex computational problem for miners [2].

Businesses must contend with more onerous rules, longer time to market, interest rate volatility, and liquidity risk. They must overcome the absence of strict oversight, extensive regulation, and

Information Technology and Implementation (IT&I-2024), November 20-21, 2024, Kyiv, Ukraine

[*] Corresponding author.

[†] These authors contributed equally.

nvc2006@i.ua (V. Nakonechnyi); vgsaiko@gmail.com (V. Saiko); oleksandr.pliushch@knu.ua (O. Pliushch); vladyslav.lutsenko99@gmail.com (V. Lutsenko); pestalocyj@gmail.com (M. Mordvyntsev)

0000-0002-0247-5400 (V. Nakonechnyi); 0000-0002-3059-6787 (V. Saiko); 0000-0001-5310-0660 (O. Pliushch); 0000-0002-2377-1858 (V. Lutsenko); 0000-0002-7674-3164 (M. Mordvyntsev)

adequate market infrastructure for issuance, settlement, clearing, and trading, particularly in emerging nations [3].

2. Asymmetric encryption technology

The key generation and digital signature algorithm of bitcoin is ECDSA, which comes from ECC. The elliptic curve calculation method satisfies the Weierstrass equation [1]:

$$y^2 + a_1xy + a_3y = x^3 + a_2x + a_4x + a_5$$

Formula 1: Weierstrass equation

F is defined on the finite field, and the points of an elliptic curve are continuous discrete points. F contains p elements. Where p is a particularly large prime, P can be obtained from the following figure:

$$P = P^{256} - P^{32} - P^9 - P^8 - P^7 - P^6 - P^4 - 1$$

Formula 2: Representation of P on the field F

Let K and G represent the discrete points that meet the requirements of the elliptic curve EP. K is an integer smaller than n, and N is the order of G. Given K and G, it's easy to calculate K. However, given K and G, it is very difficult to get K. Let G be the initial point on the ellipse, that is, the first discrete point. K is the public key and K is the private key. The following formula can be obtained:

$$K = k * G$$

Formula 3: Public key K

The public key is generated by the private key by the above method. Mechanism for Dealing with Block Chain Security Problems. I define such a group of components {g1(x), g2(x), . . . , gn(x)}, which is Out = {O1, O2, … , Om} with the external incentive set defined in the original isomorphic system logic, and Out' = {O'1, O'2 , … , O'3 }, which is not defined in the logic.

$$g_1(O_i) = g_2(O_i) = g_3(O_i)\ldots = g_n(O_i)$$

Formula 4: Original isomorphic system

The final output of the component set to stimulation is the multiple decision of all outputs. The isomerization transformation of the blockchain system can make the use of single vulnerability in the component be identified by the system, and the single vulnerability can not have a destructive impact on the system, thus greatly improving the security and stability of the blockchain system [1].

Every block is given a hash, or 256-bit number (Figure 1). Hashing is the cornerstone of cryptographic security; the blockchain ecosystem cannot operate without it. Hashing is performed according to a special algorithm and is a check of the integrity of numeric or alphabetic messages. In simple terms, in the blockchain, all messages are encrypted by senders.

From the sender to the receiver, the hash code is sent along the chain and validated by blockchain network nodes. Data transfer is irreversible, after the message is sent and confirmed, it cannot be canceled, information about completed transactions is forever recorded in the blockchain.

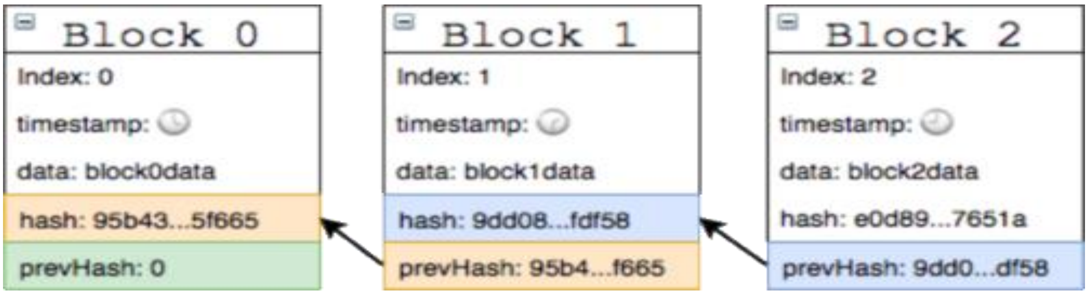


Figure 1: Working model for blockchain

An attempt to rewrite the information in one of the blocks will entail a domino effect, it will be necessary to make changes to all subsequent blocks of the chain. A protocol in blockchain technology requires confirmation of transactions by independent regulators. And if at least one of them rejects changes in the structure of blocks, the process will be blocked and the changes made will be rejected [4].

The blockchain does not store digital data, all transactions that have been verified for authenticity are recorded in its blocks in chronological order. Attempting to modify or delete records will destroy the blockchain. Based on cryptography, this technology is especially made to secure personal information.

After the transaction data is formed into blocks, they undergo cryptographic verification and are recorded in the database. All information related to blockchain technology is stored in a well-secured decentralized network. Access to it is opened with the help of special cryptographic keys. Due to this, it is impossible to forge information that is stored on the network.

Thus, blockchain is an information storage technology. Its main feature is that there can be many copies of the block chain, and they are stored simultaneously on different computers (the so-called nodes).

The data that is kept on the blockchain is immutable. One compromised node allows an attacker to alter the blockchain. If 51% of nodes reject these updates, then other nodes won't accept them either. Hundreds of thousands of nodes cannot be hacked at once. Attackers do, however, take use of further blockchain security flaws.

The unique structure of the technology, characterized by its transparency, immutability and decentralization, allows it to be widely used in various fields of activity. In addition, blockchain has great potential for development in the digital economy. Blockchain can be thought of as a huge database that has no center. It consists of an ever-increasing number of blocks.

A block can be created by anyone through a computer by entering certain information there. For example, you want to make a money transfer in a digital environment. The money transfer has been made! The operation is completely safe, since only you and the person to whom you transfer money have the keys to the block.

3. Blockchain implementers in the banking system

An attacker attempting to create a longer chain of blocks than a legal user may be used to illustrate how blockchain technology operates. Even if he succeeds, it will not lead to the point that it will be possible to create false transactions, appropriate someone else's data or make other arbitrary changes. Nodes will never accept an incorrect one transaction or block containing it. An attacker can only try to change one of their transactions to get something back.

A successful event, when the "good" chain is extended by one block, leads to an increase in the gap by one, and an unsuccessful event, when the next block is created by an attacker, leads to its reduction. The likelihood of an attacker creating a disparity of many blocks is equivalent to that of the "ruining the player" dilemma.

Let's say a player has unlimited credit, starts with some deficit, and has an infinite number of attempts to win back.

The probability that he will succeed, as well as the probability of an attacker catching up with honest participants, is calculated as follows [3]:

p - the probability that a block will occur in an honest chain

q - probability that the attacker will build the block

qz - probability that the attacker will use extra z-blocks to make up the difference

$$q_z = \left\{ \begin{array}{c} 1 \quad if\ p \le q \\ (\frac{q}{p})^z\ if\ p > q \end{array} \right\}$$

Formula 5: Probability of winning

In the event that p > y, the probability decreases exponentially as the number increases

blocks, by which the attacker lags behind. With all the odds stacked against him, without a good start, his chances of success become slim to none.

Consider now how long the payee should wait before he is completely sure that the former owner will not be able to reverse the transaction. We suppose that the malicious sender allows the recipient to believe for a while that the payment has been made, after which he returns the money to himself. The recipient will find out, but the scammer hopes it will be too late.

Despite its potential, the literature identifies several challenges to blockchain's adoption for secure data transmission. Scalability remains one of the most discussed issues, as blockchain networks—particularly those using Proof of Work (PoW)—experience delays and high transaction costs when processing large volumes of data [5].

The high energy consumption of PoW consensus mechanisms is also a notable concern [6].

Just before signing the transaction, the recipient creates a new key pair and sends the sender its public key. This prevents the sender from beginning work on the chain beforehand and from initiating a transaction when it is fortunate enough to progress. After sending the payment, the fraudster secretly starts working on a parallel version of the chain containing the alternative transaction.

The receiver waits until the transaction is added to the block and until it is continued with zblocks. He does not know the progress of the attacker, but if the average speed of generation of honest blocks is a known value, then the number of blocks of the attacker obeys the Poisson distribution and mathematical expectations [3]:

$$\lambda = z * \frac{q}{p}$$

Formula 6: Poisson distribution with mathematical expectation

From the results of research, it can be seen that the probability falls exponentially with the growth of Z.

4. Types of blockchain networks

Initially, public, private and hybrid types of blockchain networks were distinguished [4]. Evolution has led to the emergence of new types of blockchains, showed in table 1. They differ in structure, consensus mechanism and accessibility. These differences define unique application opportunities and potential for both business and society [7].

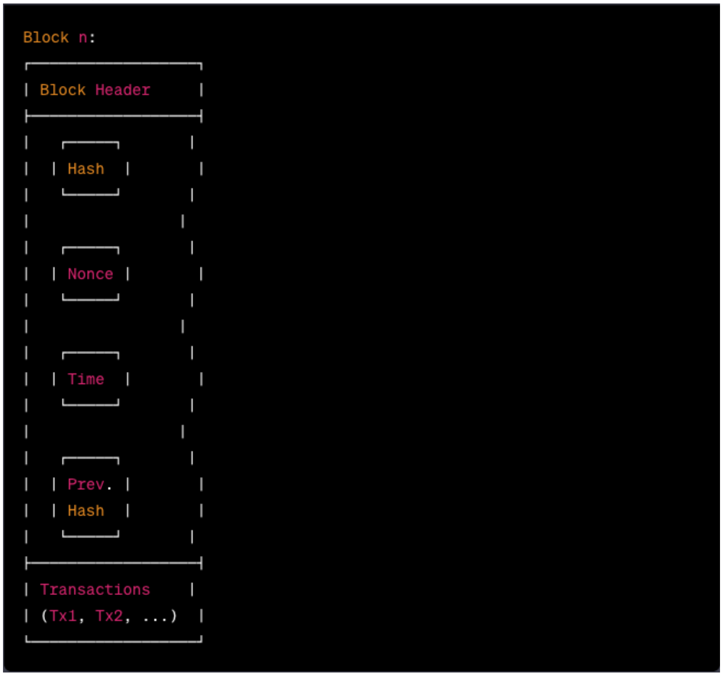
Table 1
Types of blockchain networks

Blockchain type	Description	Examples
Public blockchain	Open to all, accessible to everyone. Suitable for public networks and cryptocurrencies.	Bitcoin, Ethereum
Private Blockchain	Closed network for authorized participants. Provides a high level of privacy.	Hyperledger fabric
Blockchain Consortium	A hybrid of public and private blockchains used by multiple organizations to achieve consensus.	R3 Korda, Quorum
Permissioned blockchain	Limited access for authorized members. Ensures privacy.	Hyperledger Besu
Hybrid blockchain	Combines public and private attributes for different use cases.	Dragon Chain,QuarkChain

The public has access to the blockchain, which is the foundation for the issuance and distribution of bitcoin. The widespread use of distributed ledger technology may be attributed in large part to the Bitcoin blockchain. There is a high degree of decentralization and operational transparency in this kind of blockchain network. The advantages of a public blockchain include: resistance to cyber attacks, since this type of blockchain is not controlled by a single center, all transactions are visible to all users, as well as accessibility for all users [5].

A private blockchain is a closed network controlled by a limited number of individuals. This type of blockchain is mainly used as an internal platform within one or a number of affiliated organizations (organizations connected to each other through ownership). It is also referred to in a number of sources as a permissioned or enterprise type of blockchain. The advantages of a private blockchain include: confidentiality, speed, ease of implementation.

Let me provide simplified text-based representation of a block structure in a blockchain:



```
Block n:
┌──────────────────┐
| Block Header     |
├──────────────────┤
|    ┌─────┐      |
|   | Hash  |      |
|    └─────┘      |
|                |
|    ┌─────┐      |
|   | Nonce |      |
|    └─────┘      |
|                |
|    ┌─────┐      |
|   | Time  |      |
|    └─────┘      |
|                |
|    ┌─────┐      |
|   | Prev. |      |
|   | Hash  |      |
|    └─────┘      |
├──────────────────┤
| Transactions    |
| (Tx1, Tx2, ...)  |
└──────────────────┘
```

Figure 2: Blockchain block structure

Hybrid blockchain. Organizations frequently wish to benefit from both private and public blockchain varieties concurrently. In such cases, they develop a hybrid model that combines elements of both private and public blockchains. The organizers of the hybrid network control who can access certain data stored on the blockchain and what data can be public.

To mathematically represent the balance between public and private data, let P(x) represent the function for public access, where x is the type of data, and S(x) for private. The overall data management for a hybrid blockchain can be expressed as a weighted sum:

$$H(x) = \alpha P(x) + \beta S(x)$$

Here, α and β represent the weights for public and private data, respectively, ensuring their total impact sums to 1.

Organizations work together to administer blockchain consortia. Pre-selected organizations share responsibility for the functioning of the blockchain and the determination of data access rights. Blockchain consortia are frequently favored by similar businesses that gain from shared accountability.

One of the first examples of blockchain is cryptocurrency. Cryptocurrencies appeared at the intersection of economics, cryptography and ideology. The value of cryptocurrency can fluctuate based on various market conditions and can be represented as a stochastic process.

Suppose the price of a cryptocurrency C(t) follows a geometric Brownian motion (GBM), which is commonly used to model financial assets:

$$dC(t) = \mu C(t)dt + \sigma C(t)dW(t)$$

Here, μ represents the drift (expected return),   represents the volatility, and W(t) is a Wiener process (used to model the randomness).

Moreover, the first cryptocurrency – bitcoin – was an innovation "from below", not "from above", that is, not an initiative of states, but a decision from the people. Bitcoin was the first practical proof of the successful operation of blockchain systems. Although Bitcoin is starting to become more and more popular as a digital currency, the blockchain technology that powers it could end up being far more important.

Moving away from the topic of cryptocurrencies based on any agreements, it is important to note the importance of smart contracts – this is automatically executable computer code, which is also based on blockchain technology.

Smart contracts are triggered when certain conditions are met. Let f(x) represent the set of conditions that must be met for execution. If we treat the conditions as a set of Boolean functions, the execution of the smart contract can be defined as:

$$SC(x) = \prod_{i=1}^{n} (f_i(x))^{b_i}$$

Where:

$f\ i\ (\ x\ )$ f i (x) is the i i-th condition,

bi is a binary value (either 0 or 1) representing whether the condition is met (1 if true, 0 if false),

SC(x) represents the execution of the smart contract, which will only trigger if all required conditions fi(x) are satisfied.

The peculiarity of smart contracts is to automate the execution of operations, subject to the prescribed rules. In addition, they are self-sufficient, therefore, they have predetermined conditions. Smart contracts minimize the chance of mistake and save time [8].

5. Advantages of blockchain over the traditional financial system

It is possible to highlight three significant disadvantages of centralized bank transfers [9]:

- High commission costs;

- Unjustified time costs;
- vulnerability to hacker attacks and fraud.

The nature of blockchain technology, which was originally designed as a peer-to-peer electronic network designed for direct online payments from one party to another without going through financial institutions, allows it to take modern payment systems to a whole new level. The main advantages of using blockchain technology for money transfers and payments include the following [9]:

Low cost of translations. The use of blockchain technology will make it possible to confirm and carry out transactions, including international ones, between persons without the participation of a centralized intermediary. This will lead to minimization of the cost of such transactions due to the reduction of commission costs.

High transaction speed. The nature of blockchain technology, as well as the exclusion of intermediaries from the translation process, will allow transfers to be made in near real time.

Financial inclusion. Findex reports that 1.7 billion adults worldwide, or one-third of the global population, have little to no access to financial services, according to a World Bank research. Many people in Asia, Africa and South America do not have access to banks and traditional financial services, but they do have smartphones. Financial inclusion will be achieved globally by developing and making such a blockchain-based transfer system accessible.

Enhanced security. The blockchain is decentralized, and therefore it is almost impossible to hack it or rewrite transactions in the system.

Automation of processes. Complete payment automation will be aided by the usage of smart contracts.

The financial sector of the economy is characterized by a high speed of adaptation to innovative technologies. Thus, by maximizing expenses, the use of cutting-edge and inventive goods and services contributes to the strengthening of competitive advantages in the marketplace. Specialists in the financial sector were among the first to turn their attention to blockchain technology, since simplifying and speeding up transactions, as well as reducing transaction costs for participants in this market are very important. The use of blockchain technology is relevant, popular and promising in many areas of the financial sector: banking products and services, microcredit, project financing, insurance, exchange operations, etc.

With the use of cloud services, mobile banking, and interconnected systems, the financial sector's digital transformation has brought forth new vulnerabilities. This shift has increased the attack surface, creating multiple entry points for cybercriminals and emphasising the need for strong security frameworks to protect against emerging threats [10].

Implementation of transactions based on blockchain technology eliminates the problem of the "human factor", excludes intermediaries and increases the level of security of such operations. That is why the study of the application of blockchain technology in the financial sector is an extremely urgent issue.

Public and private key pairs govern EOA, which are primarily utilized for ether management and contract interaction through transaction transmission. While contract accounts are controlled by keyless codes and are mainly used to implement various functional requirements and record changes in contract status, such as executed transactions and balance modifications.

Unlike EOA, contract accounts cannot send transactions, but they can send messages to call other contracts [10]. Additionally, contract accounts cannot proactively interact with EOAs, but they can use some "radical" mechanisms such as self-destruction.

Thus, according to a report by the International Data Corporation, in 2018, European companies spent a total of about 400 million US dollars on blockchain solutions, and almost half of the investments fell on the financial sector. These data are presented in the form of a diagram in Figure 2. European banks, insurance, leasing and investment companies spent more than 172 million US dollars on the development and implementation of blockchain products, which corresponds to 43% of the total market.

This spread of interest in the various applications of blockchain technology makes sense given that the integration of blockchain technology into the established banking system has the potential to fundamentally alter it, improve its accessibility and efficiency, and result in large financial savings for the banks themselves. So, according to a study published by the consulting company Accenture, the introduction of blockchain technology will save banks up to 38% of annual costs [9].

6. The use of blockchain in the banking sector

The financial industry is becoming more exposed to various cyberattacks, which are increasing due to its dependence on advancing digital technology and global connectivity. With the increasing frequency and complexity of cyberattacks, traditional security frameworks that heavily depend on perimeter defences are proving ineffective [9].

The banking sector is one of the most important elements of the financial system, the role of which in the economy can hardly be overestimated. Banks serve as the backbone of all economies, acting as a "circulatory system" of different economic activities by gathering up short-term free capital and then putting them into active operations.

The rising complexity of cyber threats presents considerable concern, particularly for financial institutions that are highly vulnerable to various complex attacks like advanced persistent threats (APTs), phishing, ransomware, and insider threats [12].

As a result, the banking industry must act swiftly and effectively to respond to the emergence of new technologies and find ways to integrate them to meet the demands of contemporary society. The country's economic growth and overall economic efficiency are significantly influenced by the banking system's performance.

Nevertheless, despite the centuries-old history of banks and the banking sector as a whole, the current level of informatization and the degree of automation of many processes, there are a number of urgent problems, some of which are related to the human factor and the presence of a number of intermediary links in the services provided and operations carried out. In particular, these include high commission costs and time costs in the implementation of money transfers and transactions, the presence of internal and external fraud, personnel errors, leakage of personal data of customers and much more.

Consequently, it is clear and appropriate that the financial industry is becoming more interested in blockchain technology. Thus, blockchain is a new type of database organization system that allows a wide group of participants to receive almost simultaneous joint access to shared data with an unprecedented level of confidentiality.

The blockchain architecture allows you to collect information from various service providers into a single cryptographically secure and immutable database that does not need a third party to verify the authenticity of information. Thanks to this, it is possible to create a system where the user will only need to go through the KYC procedure once, and then use this platform to confirm his identity. At the same time, the use of smart contracts could automate many processes.

The banking industry now spends billions of US dollars defending itself against hackers; nevertheless, standard measures to avert hacker assaults, such as updating hardware and software, may not always have the desired outcome. Obviously, the financial sector needs a more reliable tool that will not only work to prevent attacks, but also reduce the theft of any information to zero, which is why more and more banks are investing in developments related to the introduction of blockchain technology. This is justified by the fact that the technology has already proven its effectiveness in the field of data management and ensuring their integrity through the use of cryptographic methods of protection and distributed storage of information.

As a result, the application of blockchain technology in the banking industry is spreading like wildfire, covering areas such as securities transactions, lending, issuing bank guarantees, and automating settlements in addition to transfers, authentication systems, and banking security [9].

7. Functional features of blockchain technology implementation in the financial sector

The disadvantages of using blockchain technology in the financial sector include [12]:

1. Limited scaling and throughput — modern blockchain technologies find it difficult to cope with large transactions, there is enough capacity at the level of an individual bank or other financial institution, but if we talk about the national or international level, then there are problems with throughput, which are still unresolved and impose certain limits on the volume of transaction transactions.

2. High cost of development — blockchain technologies are very expensive and resource-intensive projects, so only financial companies that have significant budgets for scientific and technical developments can implement them or buy ready-made solutions from startup companies.

3. High cost of use — despite significant savings on use, the use of blockchain technologies has its own high cost, as it requires a lot of computing power and storage space for an array of data. That is why many blockchain projects, despite their prospects, are not implemented or their term of use is very short.

4. Uncertainty of state regulation — many issues related to the deep implementation of blockchain in the financial sector and not only require additional regulation. For example, blockchain technology is closely related to cryptocurrencies, the regulation and status of which in Ukraine is completely uncertain and devoid of legality.

However, many interesting and potentially effective projects in the financial sector can be implemented by combining blockchain and cryptocurrencies. For the full-scale implementation of blockchain, it is necessary for state regulators to confirm the reliability, stability and efficiency of the latter and develop updated regulatory procedures.

5. Lack of highly qualified specialists — unfortunately, the demand for qualified specialists in the field of blockchain far outweighs their supply in the market. And it's not just the situation in Ukraine, the world's financial giants are also experiencing a significant shortage of skilled labor. McLagan, based on data from eight of the world's largest investment banks, conducted a study of the effectiveness of the implementation of blockchain technology in their work.

The conservative nature of the domestic financial sector, which is unwilling to adopt drastically new technologies and replace outdated but debugged work algorithms, is the main reason behind the low adoption of blockchain projects among Ukrainian financial companies, rather than the expense of their development and implementation.

Global trends, however, will have a greater impact on the direction that Ukrainian industry moves, therefore we should anticipate a rise in interest in blockchain technology soon. Especially as the financial industry stands to gain greatly from and save money on the application of blockchain technology.

At the same time, it is necessary to understand that the use of blockchain technology is not possible for all financial transactions and will not always bring economic benefits. And although the range of its use in the financial sector is extremely wide, it will still be impossible to optimize all operations in this way.

That is why it is important to conduct further research in this direction in order to provide the Ukrainian financial sector with effective recommendations on the possibility of wider use of innovative technologies in their work and analysis of their prospective effectiveness and efficiency [13].

8. 6 Ways to Use Blockchain to Improve Security

Blockchain security can be viewed in terms of the benefits it can provide to protect data and systems. The most significant examples are described below [11]:

1. Fraud prevention: Blockchain provides security by verifying and confirming transactions before adding them to the blockchain, ensuring that only legitimate transactions are recorded and preventing fraud.

2. Protection of personal data: Blockchain protects personal data by encrypting and storing it in a decentralized manner. This guarantees that personal information is safe from data breaches and cyberattacks.

3. Ensuring transparency: Blockchain provides transparency by providing a reliable record of all transactions. This means that all participants can access the same information, ensuring transparency and accountability.

4. Prevention of cyberattacks: Blockchain prevents cyberattacks with modern encryption methods to protect data. This prevents hackers from accessing and manipulating data on the blockchain.

5. Facilitation of secure transactions: The blockchain provides secure transactions by verifying and confirming all transactions before adding them to the blockchain. This guarantees the security of transactions and prevents counterfeiting.

6. Improving Supply Chain Security: Blockchain enhances supply chain security by providing a transparent and secure record of all transactions in the supply chain. By guaranteeing that every participant in the supply chain has access to the same data, this promotes accountability and openness.

At the same time, new technologies create new security challenges.

One of the key issues related to blockchain security is the 51% attack. In a 51% attack, a single person or group controls more than 50% of the network's computing power. They can now control the blockchain and influence transactions as a result.

An attacker can reverse transactions, spend coins twice, and prevent other users from participating in the network. This type of attack is especially dangerous in public blockchains, which anyone can join.

Many companies has partnered with industry-leading blockchain and cryptocurrency partners to provide enterprise-grade solutions for securing transactions. Together with partners such as IBM, R3, Ethereum, Hyperledger, Ledger, BitGo, Symbiont and ConsenSys Quorum, many companies are protecting the way industries are conducting business, bringing efficiency and establishing trust. There are also supports multiple blockchain applications including Bitcoin, Hyperledger, Ethereum, Altcoins, Monero, and more [14].

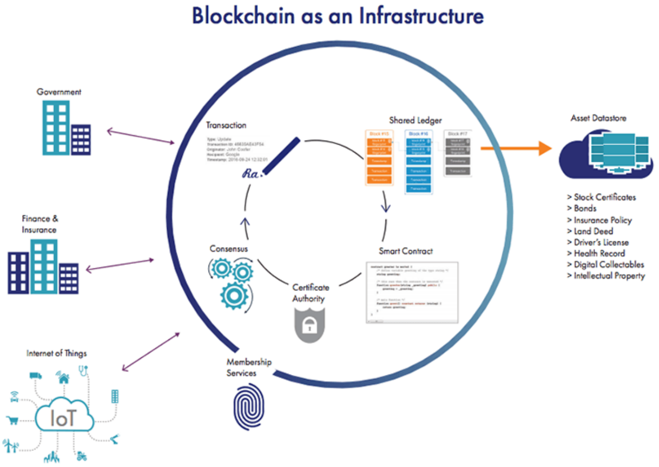


Figure 3: Blockchain as an infrastructure

Another issue related to blockchain security is smart contract vulnerabilities. These contracts may be open to assault if they are not drafted appropriately. Attackers can exploit these vulnerabilities to steal funds or disrupt the network.

In addition to the above-mentioned aspects, the blockchain security field also faces a number of other challenges. Scammers use social engineering tactics to trick users into accessing their personal information or cryptocurrency wallets. These tactics may include phishing emails, fake support calls, and other techniques aimed at deceiving users and revealing sensitive information.

Fraudsters often employ phishing attacks as a means of obtaining users' private keys and other personal information.

These attacks often involve the creation of fake websites that mimic official ones, with the aim of enticing users to reveal their sensitive data. Once fraudsters gain access to this information, they will not only be able to steal cryptocurrency from users' wallets, but also create serious threats and breaches in the field of blockchain security.

Users can purchase, trade, and store bitcoins on websites known as cryptocurrency exchanges. However, these exchanges are often subject to hacker attacks trying to gain access to users' funds. Attacks on exchanges can lead to significant losses of cryptocurrency and damage the reputation of the affected exchange.

Mining botnets are networks of computers that have been hijacked by cybercriminals and used to mine cryptocurrency without the knowledge of their owners. These botnets can be used to mine large amounts of cryptocurrency at the expense of unsuspecting users whose computers have been compromised.

This kind of attack puts the network's security at risk when a user transfers the same money again in an attempt to obtain more bitcoin. On public blockchains, where anybody is able to join the network and take part in consensus, this assault may be more damaging.

9. Solutions to blockchain security problems

There are key measures that contribute to ensuring the protection of blockchain systems [15].

A Sybil attack creates a variety of fictitious network nodes. using those nodes, the hacker will acquire majority consensus and disrupt the chain's transactions. Therefore, a large-scale Sybil attack is not nearly as effective as a 51% strike.

To prevent Sybil attacks [16]:

- Acceptable consensus algorithms are used.
- The behavior of alternate nodes is monitored and nodes that send blocks from a single user are checked exclusively.

While these algorithms can't completely prevent these attacks, they pose many obstacles and it's almost impossible for hackers to carry out attacks.

Blockchain endpoint vulnerability is another important blockchain security issue.

The ultimate goal of a blockchain network is wherever users interact with the blockchain: on electronic devices such as computers and mobile phones. Hackers will pick devices based on user behavior and take advantage of the user's key. This may be one of the most notable blockchain security issues.

To prevent end vulnerabilities:

- Don't save blockchain keys on your laptop or mobile phone as text files.
- Transfer and install antivirus software packages for your electronic devices.
- Check the system frequently, tracking time, location, and device access.

A 51% assault happens when a single person or group (malicious hackers) obtains more than half of the hash rate and takes over the whole system, which might have catastrophic consequences. Transactions can be changed out of sequence and prevented from being verified by hackers. They will even go back and undo earlier transactions, which would result in double spending.

To prevent a 51% attack:

- Ensure that the hash rate is higher.
- Improve your mining pool monitoring.

Take a look on phishing attack. The goal of a hacker in a phishing attack is to steal the user's credentials. They will send legitimate emails to the owner of the wallet key.

The immutability of blockchain ledgers is a critical factor in ensuring data security, as once data is recorded on the blockchain, it cannot be altered or deleted without leaving an audit trail. This property is especially beneficial in sectors like finance, where transaction records must be immutable to prevent fraud. The empirical evidence from cross-border payment systems using blockchain showed that immutability increased trust and reduced fraud, as every transaction could be traced and verified by all network participants [15].

The user needs to enter their login details via the attached fake hyperlink. Access to the user's credentials and other sensitive information can cause damage to both the user and, therefore, the blockchain network. they are also susceptible to subsequent attacks.

To prevent phishing attacks:

- Improve browser security by installing a trusted add-on or extension that will notify you of unsafe websites.
- Improve device security by installing malicious link detection software in the same way as reputable antivirus software.
- If you receive an email requesting your login details, contact support or the partner again to resolve the issue.
- Do not click on links until you have thoroughly reviewed them. Enter the address in a private tab of your browser rather than visiting links.
- Avoid Wi-Fi networks in outdoor or public cafes.
- Make sure your system and software are up to date.

Another problem is a routing attacks. The blockchain network and applications rely on the movement of vast amounts of knowledge in real time. Account anonymity allows hackers to intercept data being transferred between users and ISPs.

When a routing attack occurs, data transfer and activities continue as usual, therefore blockchain participants are typically oblivious to the danger. The risk is that these assaults may often reveal private information or take money without the victim's awareness.

To prevent routing attacks:

- Use encryption.
- Implement secure routing protocols (with certificates).
- Change passwords regularly; use strong passwords.
- Educate yourself and your workers about the risks associated with information security.

Private Key or seed phrase is the main key to your funds. It may be simple for a hacker to figure out your private key if it is weak. This means that they could gain access to your funds. Private keys should be kept secret and strong enough that they can’t be easily guessed.

Due to its continued immaturity, blockchain technology faces issues with quantifiability. This implies that the network will solely handle a restricted variety of transactions at any given time. You can utilize a variety of sidechains and offline solutions (L2s) to prevent scaling problems.

The threat posed by malevolent nodes is one of the additional security issues that blockchain technology faces. This will occur when a bad actor attempts to disrupt the network by joining it. They'll try this by flooding the network with transactions or making an attempt to reverse valid transactions.

The blockchain network, managed via Ethereum Ganache and smart contracts, is assumed to provide a secure and immutable ledger for recording authentication events, access decisions, and other critical logs. This mirrors similar logging mechanisms in blockchain platforms like Hyperledger Fabric and Ethereum, which are commonly used for creating secure, decentralised applications and maintaining immutable records [16].

Blockchain contains a lot of security flaws, however experts in cyber security will work hard to fix or lessen these issues. Blockchain may be deployed in the most stable and safe way by IT professionals that possess the necessary analytical and technical abilities. However, it's always beneficial to be aware of the many threats and how to defend your assets by taking preventative measures [18].

Additionally, despite the fact that the banking industry is already investing billions of dollars to thwart hacker attacks (Unicredit alone plans to invest roughly $2.7 billion in bolstering security), traditional countermeasures such as updating hardware and software components do not have the desired impact. The financial industry requires a more dependable instrument that can not only stop assaults but also completely eliminate information theft.

As blockchain technology evolves, new theories and models are emerging to address its limitations. Hybrid blockchain models, which combine elements of both public and private blockchains, are gaining attention as a potential solution to scalability and privacy concerns. Kaur et al. (2020) proposed a hybrid model that allows organizations to maintain control over private data while benefiting from the security of public blockchains. Empirical studies on hybrid models are still in their early stages, but initial results suggest that they offer a promising balance between security, scalability, and privacy [19].

That is why the financial sector is increasingly in need of the introduction of blockchain technology when working with large information fields. And this is not surprising: blockchain in practice has proven its worth in the field of data management and ensuring their integrity through the use of cryptographic methods of information protection.

Thus, the Civic platform provides identification and verification of users based on the blockchain, which eliminates the theft of their personal data. An additional project that provides a safe blockchain identity alternative is UniquID Wallet. In fact, UniquID Wallet replaces the standard password identification system, being integrated with a variety of biometric personal devices, which, as a result, gives the highest possible level of user recognition [20].

10.Conclusions

This work's study findings served as the foundation for future development of the blockchain-based payment data protection technique.

The blockchain industry is actively developing. Startups are creating blockchain-based solutions for managing digital finances, investing, and impacting the financial system. It can definitely be argued that the financial sector is waiting for changes, but in order for cryptocurrencies and blockchain to become a familiar means of payment, it is necessary to continue to explore the technology.

The Society for Worldwide Interbank Financial Telecommunications (SWIFT) works with banks around the world on global payment initiatives and tries to improve the quality of cross-border payments. SWIFT implements blockchain technologies by working with active vendors and allowing banks to allow customers to pay with fiat currencies and cryptocurrency. Blockchain technology is being used to significantly reduce the number of participants needed to deal with banking issues and ensure compliance, which means that we are already seeing some significant improvements [21].

The growth of blockchain-based payment solutions will continue to grow, and businesses will witness large-scale adoption of this technology. Several companies are experimenting with "tokenization" to encrypt digital assets for secure transactions, although this is still in the early stages of development. Banks use blockchain for digital fingerprinting and universal customer identification due to its decentralized nature. They will continue to disseminate information as it is updated and reduce the information load during authentication and verification processes. The blockchain will be used to verify firmware updates and patches, as well as to prevent unauthorized access or malware installation attempts.

The results of this study confirm that blockchain technology has the potential to significantly enhance the security of data transmission across various industries. Its decentralized architecture, cryptographic protections, and immutability offer robust security advantages, while newer consensus mechanisms such as PoS and PoA show promise in overcoming scalability and energy challenges [22].

Smart contracts demonstrate to users the ability to automate payments through the use of predefined conditions and automatically reduce fraud by reducing human intervention. The technology manages complex reconciliation activities such as creating invoices, making financial decisions, approving a loan, and processing applications. A significant benefit of using blockchain is the expansion of access to banking services and the opening of new economic flows for the world's unbanked population. The future of blockchain in the cybersecurity of the banking industry is uncertain, but one thing is clear: it will continue to improve asset security and payment outcomes for organizations [23].

In today's technology environment, the introduction of novel technologies like business blockchains, digital assets, and quantum computing in their respective fields can be revolutionary.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Huitong Song, Yansheng Chen. Digital Financial Transaction Security Based on Blockchain Technology, 2021. URL: https://iopscience.iop.org/article/10.1088/1742-6596/1744/3/032029/pdf

[2] Wood J. Custodial Wallets vs. Non-Custodial Crypto Wallets, 2022. URL: https://www.coindesk.com/learn/custodial-wallets-vs-non-custodial-crypto-wallets/

[3] W. Feller, An introduction ot probability theory and its applications, 1957.

[4] Blockchain in Financial Services. URL: https://consensys.net/blockchain-use-cases/finance/

[5] Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 2019, 13-24.

[6] Zhang, L., Zhang, L., & Du, B. Deep learning for remote sensing data: A technical tutorial on the state of the art. IEEE Geoscience and remote sensing magazine, 4(2), 2016, 22-40.

[7] Oleksandr Leusenko, What is Blockchain - In Simple Language, 2023. URL: https://shorturl.at/afpX3

[8] Raptunovich O.M. Blockchain technology as an accelerator for the development of digitalization in the financial sector of the economy.

[9] Oleksandr Kud, Mykola Kucheryavenko, Yevhen Smychok. Digital assets and their economic and legal regulation in the light of the development of blockchain technology. Monograph Kharkiv "Law", 2019.

[10] C. Le´ on, J. Migu´ elez, Securities cross-holding in the Colombian financial system: a topological approach, Stud. Econ. Finance 38, 2021, 786–806, doi: 10.1108/sef-10-2020-0398

[11] S.H. Bakry, Development of security policies for private networks, Int. J. Network Manage. 13, 2003, 203–210, doi: 10.1002/nem.472X7 Clement Daah, Amna Qureshi, Irfan Awan, Savas Konur. Simulation-based evaluation of advanced threat detection and response in financial industry networks using zero trust and blockchain technology, Simulation Modelling Practice and Theory, 2024, doi: 10.1016/j.simpat.2024.103027

[12] What is a smart contract, and how does it work? URL: https://cointelegraph.com/learn/what-are-smart-contracts-a-beginners-guide-to-automated-agreements

[13] Bondarenko, L., Moroz, N. and Lashchyk, I., Functional features of blockchaine technology implementation in the financial sector, 2019.

[14] Blockchain Security Solutions, 2022 URL: https://cpl.thalesgroup.com/encryption/blockchain

[15] Priyadharshini, S. L., Al Mamun, M. A., Khandakar, S., Prince, N. N. U., Shnain, A. H., Abdelghafour, Z. A., & Brahim, S. M. Unlocking Cybersecurity Value through Advance Technology and Analytics from Data to Insight. Nanotechnology Perceptions, 2024, 202-210.

[16] S. Pancari, A. Rashid, J. Zheng, S. Patel, Y. Wang, J. Fu, A systematic comparison between the Ethereum and Hyperledger Fabric blockchain platforms for attribute-based access control in smart home IoT environments, Sensors 23, 2023) doi: 10.3390/s23167046

[17] G. Rathee, C.A. Kerrache, M.A. Ferrag, A blockchain-based intrusion detection system using Viterbi algorithm and indirect trust for IIoT systems, Journal of Sensor and Actuator Networks, 2022, doi: 10.3390/jsan11040071

[18] Danyal Zafar, 8 blockchain security issues you are likely to encounter, 2022. URL: https://cybersecurity.att.com/blogs/security-essentials/8-blockchain-security-issues-you-are-likely-to-encounter

[19] Axel Egon, Lucas Doris. Investigating blockchain technology for secure data transmission. November 2024. Journal of Cybersecurity

[20] Vladislav Kravets, Blockchain and banking security management system, 2018. URL: https://lb.ua/blog/vladiskav_kravets/403097_blokcheyn_sistema_upravleniya.html

[21] Mariya Ouaissa, Mariyam Ouaissa, Zakaria Boulouard, Abhishek Kumar, Vandana Sharma, Keshav Kaushik. Artificial Intelligence for Blockchain and Cybersecurity Powered IoT Applications, 2024, doi: 10.1201/9781003497585.

[22] Florackis, C., Louca, C., Michaely, R., & Weber, M. Cybersecurity risk. The Review of Financial Studies, 36, 2023, 351-407.

[23] Pappu Manadal, Securing the Future of Banking – Exploring the Synergy of Blockchain and Cybersecurity, 2023. URL: https://www.eccouncil.org/cybersecurity-exchange/network-security/securing-the-future-of-banking-with-blockchain-based-cybersecuritya/