Issue 15, 2024

https://doi.org/10.23939/sisn2024.15.469

УДК 004.9: 339.9.342

МЕТОДИ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ БЛОКЧЕЙН В СИСТЕМІ ОБЛІКУ ПРОДАЖУ ЗБРОЇ

Юрій Яримович, Наталія Кунанець

Національний університет "Львівська політехніка",
кафедра інформаційних систем та мереж, Львів, Україна
E-mail: Yurii.A.Yarymovych @lpnu.ua, ORCID: 0009-0006-1391-3214
E-mail: nataliia.e.kunanets@lpnu.ua, ORCID: 0000-0003-3007-2462

У статті досліджується застосування інформаційної технології блокчейн у сфері обліку продажу зброї. Автори розглядають основні методи формування такої технології, включаючи розподілену базу даних, хеш-функції, криптографічний захист, смарт-контракти, консенсус-протоколи, децентралізовану мережу, транзакції, генезис-блок, децентралізоване керування та публічний ключ. Автори аналізують потенціал цих методів у створенні ефективної та безпечної системи обліку продажу зброї. Висновки статті підкреслюють значення використання технології блокчейн у цій сфері та її потенціал у поліпшенні ефективності та безпеки обліку продажів зброї.

Ключові слова: блокчейн; розподілена база даних; хеш-функції; криптографічний захист; смарт-контракти; консенсус-протоколи; децентралізована мережа; транзакції; генезис-блок; децентралізоване керування та публічний ключ.

Introduction

In the modern world, information technologies are widely used in various spheres of activity. One of the most popular information technologies is blockchain – a distributed database that allows storing information in the form of a public chain of blocks. A distinctive feature of the blockchain is its use to protect information, the inaccessibility of the opportunity for change and manipulation, which makes this technology an ideal tool for ensuring reliability and openness in various spheres of activity.

One of these areas is accounting for the sale of weapons. Transparency and reliability of information storage in this area are critical, as careful attention to the accounting procedures of arms circulation has a direct impact on the security and stability of society. In this context, the use of blockchain information technology is of particular importance, ensuring transparency, security and integrity of data on the sale of weapons.

In this article, we will consider the possibilities of using blockchain information technology to build an information technology platform for accounting for the sale of weapons. Having analyzed the potential of this information technology, we will be able to ensure effective management of the processes of weapons sales, reduce the possibility of illegal circulation and increase the level of security in this area.

Formulation of the Issue

A detailed review of the current problems and challenges faced by the accounting systems for the sale of weapons allows us to state a lack of transparency, a large number of intermediaries, the risk of data falsification and ineffective control.

This allows us to hypothesize that the use of blockchain technology can solve these problems by ensuring transparency, security, automatization and efficient management of the accounting processes of arms sales. The construction of an information technology platform based on blockchain technology for the accounting of arms sales will include the structure of the database, the types of transactions and the roles of network participants.

Analysis of Recent Research and Publications

Researchers are paying more and more attention to the search for technological solutions to meet the need for accounting for military equipment, as well as providing documentary support for its transfer. At the same time, it is noted that the provision of documentary support and registration of all processes related to accounting for the movement of military weapons is a complex and time-consuming process. The authors of the article [1] suggested using a distributed registry for customs regulation of these processes, ensuring the safety of their participants, and achieving transparency in international arms supplies. At the same time, it is emphasized [2] the need to use modern information technologies to optimize data exchange and authenticate communications between numerous and diverse stakeholders and to facilitate the tracking of defense equipment trade procedures [3].

Some technologies, the authors of the article [4] note, can expand monitoring capabilities while simultaneously providing protection, including blockchain technology, which is successfully used to document information on the circulation of military weapons in some countries, since the security of the chain is achieved by algorithmic encryption of each hash and guarantees allowing only the addition of records and providing participants with information about the history of each transaction.

In recent years, blockchain technology has gained popularity, and many experts refer to the potential application of the technology in various spheres. The researchers analyzed the results of the conducted survey on the relationship between blockchain and information systems and noted that providing wide access to the possibilities of using blockchain information technology through public libraries and code generation tools will contribute to the disclosure of the potential of the technology and generated proposals on how to improve information systems using blockchain technology [5].

Formulation of the purpose of the article

The purpose of the article is to substantiate and investigate the possibilities of using blockchain technology in the field of accounting and control of arms sales. The article will consider the following aspects:

The object of the study: an information technology platform for accounting for the sale of weapons.

The subject of the study: the use of blockchain information technology in the construction of this platform.

Tasks of the study:

1. To analyze the current state of information systems for accounting for the sale of weapons and existing problems in their functioning.
2. To study the basic principles and working principles of blockchain technology and its application in various industries.
3. To develop the concept of an information technology platform for accounting for the sale of weapons based on blockchain technology.
4. To determine the key functional requirements and characteristics of the platform.

Presenting main material

Blockchain information technology

Blockchain information technology is a data storage and transmission technology based on the concept of a distributed database that is stored on different computers at the same time (nodes) in the form of blocks that are linked together using cryptographic methods, forming an immutable chain of blocks [6].

This technology is used to create secure transactions between network participants, track and verify them, and also ensures data confidentiality and the absence of the need to trust an intermediary. Each block contains the previous block's hash code, timestamp, and transaction data, and each network node has a copy of this database. This technology is based on the absence of centralized management and data storage, which makes it particularly reliable, since each block of data in the block chain contains a unique hash code that links it to the previous block, and also applies cryptographic methods to ensure the security and integrity of the data. Unlike traditional databases that rely on a central authority to verify transactions, a blockchain can contain protocols to provide information to participants according to their level of access.

The use of blockchain information technology to build an information technology platform for accounting for the sale of weapons should contribute to the security of all processes of this technological cycle. Blockchain information technology provides a high level of reliability and security. Since the data when using this information technology is distributed throughout the network, it becomes unavailable for modification or deletion. This helps to avoid the possibility of falsification of data on the sale of weapons and to prevent unreliability of information. Blockchain ensures transparency of operations, as any changes in data are recorded and available for viewing by all network participants. It allows buyers, sellers and regulatory authorities to verify the legitimacy and status of arms sales transactions in real time. Blockchain technology allows transactions to be carried out without intermediaries, which reduces costs and time for concluding agreements and confirming transactions. This is especially important for accounting for arms sales, where confidentiality and speed of transactions are critical. The use of smart contracts in sales accounting procedures allows to automatize operations, ensuring the automatic fulfillment of the terms of agreements and reducing the risk of errors or fraud. Blockchain technology allows different parties, such as manufacturers, distributors, regulators and customers, to share and access data in real time, which helps to improve the management, tracking and control of arms sales procedures.

Therefore, the use of blockchain information technology in the construction of an information technology platform for accounting for the sale of weapons contributes to a significant increase in the efficiency, security and reliability of operations, as well as to ensure greater transparency and automatization in this field.

The main characteristics of blockchain information technology that make it attractive for building an information technology platform for accounting for arms sales include: decentralization, transparency and integrity of data, security, irreversibility of transactions, speed and scalability.

In general, the use of blockchain information technology to build an information technology platform for accounting for arms sales can help ensure a high level of security, transparency and integrity of data, as well as facilitate the management and monitoring of arms circulation.

The main characteristics of the blockchain information technology for building an information technology platform for accounting for the sale of arms can be represented by the following tuple:

$$BC = (D, T, S, I, P),$$

where D – decentralization, which provides the ability to store data on different nodes of the network, which makes it decentralized and allows to avoid centralized control and provides greater resistance to attacks and failures; T – transparency and inviolability of data, which contributes to the storage of information, its availability for viewing by all network participants, which ensures the transparency of all transactions, and thanks to the use of cryptography, the data in the blockchain is inviolable and cannot be changed without appropriate confirmation; S – security, which is achieved through the use of cryptographic data protection methods, and each block contains the hash of the previous block, which makes data manipulation almost impossible; I – irreversibility of transactions, which ensures the impossibility of canceling or changing already saved transactions, and contributes to the reliability of accounting and preservation of the history of arms trade; P – speed and scalability that offer high transaction speed, making them suitable for processing the large volume of data often required in the field of accounting for arms sales.

When using blockchain information technology, it is expedient to create distributed registers when conducting accounting procedures for the sale of weapons, which has significant potential, especially for ensuring reliability, transparency and data security. Blockchain allows for the creation of distributed ledgers without central control. Each network node has a copy of all data, which makes the system more resistant to the exit of individual nodes and attacks on centralized data processing centers. Blockchain information technology ensures data reliability through cryptographic security and confirmation mechanisms. Each block of data is cryptographically signed and then linked to the previous block in a chain, making it impossible to change already recorded data. All transactions and actions that take place on the information technology platform are recorded in the blockchain and are viewable only by network participants. This ensures transparency and openness of data and financial management. The specified information technology allows for the automatization of many processes, which makes them more efficient and less costly in both time and other resources. Blockchain can be used to create "smart" contracts that are automatically executed when certain conditions are met, providing automatization and eliminating the possibility of third-party intervention. Blockchain is used to create cryptocurrencies and other financial instruments such as stable coins, tokens and decentralized financial services (DeFi). Blockchain can be used to track the supply of goods from suppliers to consumers, providing transparency and verification of the supply chain.

In general, the use of blockchain information technology to create distributed ledgers can significantly improve the reliability, transparency and efficiency of data management and business processes in various fields.

Methods of formation of blockchain information technology

The use of blockchain information technology involves the creation of distributed ledger technologies (Distributed Ledger Technologies, DLT), which are characterized by a number of key aspects. The main components of the blockchain information technology for the information technology platform for accounting for the sale of weapons, considering the need to create distributed registers, can be represented by the following tuple:

$BC_{ITP} = (DB_{ITP}, HF_{ITP}, CP_{ITP}, SC_{ITP}, CP_{ITP}, DN_{ITP}, TR_{ITP}, GB_{ITP}, DC_{ITP}, PK_{ITP})$, where

BC_{ITP} – blockchain information technology

DB_{ITP} – distributed database;

HF_{ITP} – hash functions;

CP_{ITP} – cryptographic protection;

SC_{ITP} – smart contracts;

CP_{ITP} – consensus protocols;

DN_{ITP} – decentralized network;

TR_{ITP} – transactions;

GB_{ITP} – genesis block;

DC_{ITP} – decentralized management;

PK_{ITP} – public key.

Let's consider each element in more detail. Blockchain uses ***a distributed database*** in which each network node contains a copy of the entire transaction history [7]. Using blockchain technology to create a distributed database has a number of advantages and opportunities. Blockchain allows each member of the network to have a copy of the database, which makes it more resistant to the failure of one or more nodes. To achieve decentralization, a distributed database is created, which is stored and updated on different network nodes without a central control body. Thus, information in distributed registers is distributed across all network nodes, which ensures reliability and data recovery in case of node failure. Information in the blockchain is protected by cryptography and distributed among many nodes. This makes it reliable and more resistant to hacking or manipulation. Although blockchain technology can be slow compared to traditional databases, developers are constantly working on improving protocols to increase the speed of transactions.

Information in the blockchain is cryptographically protected, making it difficult for unauthorized access and alteration. Each block contains the hash of the previous block, making it difficult to change the transaction history. Distributed databases use cryptographic techniques to secure and authenticate transactions and data. The use of blockchain technology allows to create a distributed database with high resistance to attacks, scalability and ensures a high level of security and trust for network participants.

Hash functions are used to create a unique signature for each block, which allows to check the integrity of the data [8]. The hash function in blockchain information technology can be expressed as follows:

Let H be a hash function that takes an input string of arbitrary length and returns a fixed-length hash value. That is, $H(x)$ will represent the hash of the input string $×$. Mathematically, it can be written as follows:

$$H:\{0,1\}^{*}\rightarrow\{0,1\}^{n},$$

where ${0, 1}^*$ is the set of all possible strings of arbitrary length, and ${0, 1}^n $ is the set of all possible hash values of fixed length n bits.

For example, if we have a string $×$ that represents some information about a transaction or a block in the blockchain, then its hash can be calculated as $H(x)$. This hash value can then be used to verify data integrity or track changes in the blockchain.

Let us give one example of the use of hash functions in the information technology of the blockchain for the accounting platform for the sale of weapons, which can be the creation of a hash for each transaction of the sale of weapons. When a transaction is executed, a block will be created in the system, which will contain data about the transaction, for example, information about the buyer, the seller, type and quantity of weapons, date and time of the transaction, and other metadata. Once a block is created for that transaction, the hash of that block will be calculated using a hash function.

For example, let us have the following transaction of selling weapons:

Byer: John Doe Seller: ABC Guns Inc. Arms type: gun Quantity: 2 Transaction date: 2024-03-25 15:30:00

This data will be used to create a block, and then the hash of that block will be calculated using a chosen hash function, such as SHA-256. Therefore, the hash value of this block will be unique and can be used to identify this transaction in the blockchain network.

Cryptographic protection ensures confidentiality and security of transactions, as well as users identification [9]. Cryptographic protection in blockchain information technology can be expressed as follows:

Let:

M be a message or data to be protected from unauthorized access;

K – the key used to encrypt and decrypt data;

$E_K(M)$ – encryption of message M using key K;

$D_K(M)$ – decrypting the encrypted message M using the key K.

Then cryptographic protection in blockchain information technology can be expressed by the following mathematical expression:

Encrypting data before recording it in the blockchain: $E_K(M.)$

Decrypting data while reading it from the blockchain: $D_K(M)$,

where $E_K(M)$ and $D_K(M)$ correspond to the use of a certain encryption and decryption algorithm using the key K.

Let us consider an example of a scenario of using cryptographic protection in blockchain information technology for an information technology platform for accounting for the sale of weapons. Before recording data on the sale of weapons in the blockchain, the data is encrypted during the transaction, they can be encrypted using a cryptographic key. For example, buyer, seller and transaction details can be encrypted to ensure privacy. Decryption of data when viewing information occurs when viewing information about weapon transactions from the blockchain, the data can only be decrypted by

authorized users using the appropriate cryptographic key. This will ensure data confidentiality. Before an arm sale transaction is added to the blockchain, it can be signed using the seller's cryptographic key. This will allow to verify the authenticity of the transaction and avoid possible falsifications. Cryptographic hash functions can be used to generate a unique hash for each block of data in the blockchain. When verifying the integrity of the blockchain, these hashes can be compared to detect any changes in the data.

One of the elements of blockchain information technology is ***a system of "smart" contracts***, which has significant potential for an information technology platform for accounting for arms sales, especially considering the various legal requirements and complexities in this area [10]. Smart contracts are software codes that automatically execute the terms of the agreement recorded in the blockchain. A "smart" contract system can automatize many processes related to the sale of weapons, such as checking licenses, verifying the identity of buyers, signing agreements, etc. This will speed up and simplify processes, reduce costs and increase efficiency. The use of "smart" contracts will allow the creation of a system that automatically checks licenses and permits before each weapon transaction. This will help reduce the risk of illegal arms sales and increase security. The blockchain, on which the system of "smart" contracts is based, ensures transparency and inaccessibility to change data. This can build trust between the parties and promote greater openness in arms sales processes. All operations performed through the system of "smart" contracts are recorded in the blockchain, which allows parties to check the history and details of transactions at any time. This can be useful for auditing and tracking purposes. The system of "smart" contracts ensures automatic fulfillment of the terms of the agreement. For example, the contract may be automatically canceled if the buyer does not have the appropriate license or permit to purchase weapons. A smart contract system can help reduce the risk of financial loss or legal issues by automatizing the fulfillment of contract terms and ensuring compliance with all requirements and regulations. The use of a system of "smart" contracts can significantly increase the efficiency and security of arms sales processes, ensuring transparency, automatization and inaccessibility to data modification. However, it is important to consider all the potential risks and challenges associated with the implementation of such system. The formalization of the system of "smart" contracts can be presented using formulas that describe various aspects of the functioning of this system. Below are some formulas that can be used for formalization:

The formula for checking the terms of the contract will be submitted as follows:

$$C_i \rightarrow P_i,$$

where C_i – contract terms; P_i – fulfillment of the contract terms.

Checking the status of the order according to the terms of the contract may look like this. The client plans to make a purchase through an online store that uses a system of "smart" contracts to process orders. Before making a purchase, the customer wants to check the status of his order according to the terms of the contract with the store using the following method:

Step 1. The client enters the personal account on the website of the online store.

Step 2. The client goes to the "My orders" section.

Step 3. The system executes the contract condition check formula for each customer order.

Step 4. If the terms of the contract are fulfilled (for example, the payment is made, the product is in stock, etc.), the system displays the status of the order as "Active".

Step 5. If the terms of the contract are not fulfilled (for example, insufficient quantity of goods in stock or payment arrears), the system displays the status of the order as "Inactive".

Step 6. The client reviews the status of each order and decides on further actions.

This is just one possible example of using the contract terms check formula.

Formula for automatic fulfilment of the contract:

$$P_i \rightarrow A_i,$$

where A_i – automatic fulfilment of the contract when conditions P_i are met.

Let us give an example of automatic fulfilment of a contract for an information technology platform for accounting for the sale of weapons. The arms seller and the buyer entered into a contract for the purchase and sale of arms through an information technology platform. The terms of the contract include details about the product, price, delivery terms and other important aspects. The method is implemented as follows:

Step 1. The buyer deposits the required amount of money into the account using an electronic payment service.

Step 2. The seller provides the platform with evidence that the product is ready for shipment.

Step 3. The platform automatically checks the fulfillment of the terms of the contract. For example, the presence of the necessary amount on the buyer's account and the readiness of the goods for shipment are checked.

Step 4. If all conditions of the contract are fulfilled, the platform automatically executes the transaction: transfers money from the buyer to the seller and initiates the process of delivering the goods.

Step 5. If any of the contract terms is not fulfilled (for example, insufficient amount on the buyer's account), the platform suspends the contract fulfilment process and informs the parties about it.

This method allows to automatize and simplify the contract fulfilment process, reducing the risk of errors and improving the efficiency of operations.

Transaction audit formula:

$$T_i = \{t_1, t_2, ..., t_n\},$$

where T_i – multiple transactions; t_i – a separate transaction.

Let us analyze the transaction audit scenario for accounting for the sale of weapons. This scenario describes the use of the transaction audit formula to verify the legality and legitimacy of all transactions that occur on the information technology platform for accounting for the sale of weapons and is carried out using the following method;

Step 1. Launching an audit. The system automatically runs the transaction audit process on a regular basis based on a set schedule or under certain conditions.

Step 2. Receiving transactions. The system receives data on all transactions taking place on the platform, including data on arms sales.

Step 3. Legitimacy check. Certain criteria and rules apply to verify the legitimacy of each transaction. For example, compliance of the transaction with legal regulations on the sale of weapons, availability of necessary licenses, etc. are checked.

Step 4. Recording the results. Audit results (positive or negative) are recorded in the system and are available for further analysis.

Step 5. Notification of detected violations. In case of detection of violations or inconsistencies with the rules, the system generates a notification about this and initiates appropriate measures, for example, suspending the transaction or notifying the relevant authorities.

Step 6. Reporting. The system provides the ability to generate reports on audit results for further analysis and monitoring of the legislation abiding.

This method allows to ensure a high level of control and security in the process of accounting for the sale of weapons with the help of automatized audit of transactions.

The formula for determining the owner of the contract:

$$O_i = f(C, P, T),$$

Where O_i – contract owner; f – function to determine the contract owner; C – characteristics of the contract; P – characteristics of the contract participants; T – contextual parameters.

Let us give an example of a scenario: the user makes a request to the system about the owner of a certain contract on the platform for accounting for the sale of weapons using the following method:

Step 1. Entering information. The user enters the contract identifier or other necessary information so that the system can find the appropriate contract.

Step 2. Contract search. The system searches for the contract based on the data entered by the user.

Step 3. Identifying the owner. After finding a contract, the system identifies the owner of the contract according to the established rules. For example, the owner can be the person who signed the contract or the organization for whose benefit the contract was concluded.

Step 4. Output of the results. The system returns information about the contract owner to the user, such as their name, contact details or other information that may be important.

Step 5. Completion. The user receives the necessary information and can use it for further actions, for example, to contact the owner of the contract or conduct an audit of transactions.

This method allows users to identify contract owners on the weapons sales accounting platform quickly and conveniently using developed methods and established rules.

We can present the access control formula as follows:

$$D_i \rightarrow A_i,$$

where D_i – access control; A_i – automatic fulfilment of the contract.

In this scenario, the system administrator configures users' rights to access the information on the arms sales accounting platform using the access control formula according to the following algorithm.

Step 1. Resource selection. The administrator selects the resource or the function to which access needs to be configured.

Step 2. Defining access rights. The administrator uses the access control formula to determine the access rights of users to the selected resource. For example, it can set the right to "read", "modify" or "delete" for different categories of users.

Step 3. Using the formula. The administrator enters into the formula the parameters that start the access conditions, for example, the user role, access time, territory restrictions, etc.

Step 4. Setup results. After setting access conditions using a formula, the system automatically grants or restricts user access to the selected resource in accordance with the defined rules.

Step 5. Testing. The administrator checks the access settings by checking how the system responds to the actions of different types of users.

Step 6. Completion. After successful setup and access verification, the administrator completes the setup process and ensures that users have appropriate access to information on the arms sales accounting platform.

This method allows administrators to manage user access to various functions and resources on the platform effectively, ensuring data security and privacy.

The formula for determining the status of the contract:

$$S_i = \{0, 1\},$$

where S_i – contract status (0 – inactive, 1 – active).

Let us give an example of a scenario for determining the status of a contract on the information technology platform for accounting for the sale of weapons using the following method:

Step 1. Data entry. The user enters the necessary data about the contract, such as the contract identifier, the date of conclusion, the validity period, the amount, etc.

Step 2. Using the formula. The system uses a formula that evaluates the entered data and determines the status of the contract based on certain conditions. For example, if the contract amount exceeds a certain threshold, or if the end date of the contract has already passed, then the status of the contract can be defined as "active" or "inactive".

Step 3. Analysis of results. The system analyzes the results of the formula and determines the status of the contract, which can be displayed to the user.

Step 4. Status display. The status of the contract (for example, "active" or "inactive") is displayed in the user interface of the weapon sales accounting portal.

Step 5. Contract management. Depending on the defined status, the user can decide on further steps with the contract, such as updating the data, extending the term or terminating the contract.

This method allows the system to determine the status of the contract efficiently based on the entered data and established conditions, which contributes to better contract management on the arms sales accounting platform.

There are given only a few formulas that can be used to formalize the system of "smart" contracts, the information technology platform will include more aspects and details, depending on the specific needs and requirements of the project.

Let us consider the method of using smart contracts in blockchain information technology for the information technology platform for accounting for the sale of weapons:

Step 1. Conclusion of an agreement on the sale of arms. The buyer and the seller enter into an agreement on the sale of weapons using a smart contract that is recorded in the blockchain. The agreement contains all the necessary information about the transaction, such as product details, price, delivery terms, etc.

Step 2. Automatic execution of the agreement. Once the agreement is concluded, the smart contract automatically executes the agreement when all terms specified in the contract are fulfilled. For example, when the buyer pays for the product, or when the product is delivered to the destination.

Step 3. Delivery status check. The smart contract may contain terms related to the delivery of the weapon, such as confirmation of receipt of the goods. The buyer can access the delivery status via the blockchain, which will allow him to be sure that the product has been successfully delivered.

Step 4. Automatic payment. The smart contract can automatically make payments to the seller after the buyer confirms receipt of the goods. This avoids payment delays and ensures a fast and efficient transaction.

Step 5. Automatic dispute resolution. In the event of a dispute between the parties, the smart contract can automatically initiate the dispute settlement process according to certain rules specified in the contract. For example, an arbitration procedure or the return of goods may be provided.

Consensus protocols are mechanisms that determine the rules of agreement between network participants for accepting new blocks [11]. The consensus protocol in blockchain information technology can be expressed as follows:

Let N be the number of network participants, t be the maximum number of participants that can detect abuse.

Then the consensus protocol can be expressed as (N, t)-resistant, where t is the security parameter. This means that the system can withstand an attack by no more than t attackers from the total number of N participants. In mathematical terms, a consensus protocol can be defined as:

$$N-t > 3t,$$

where N – total number of participants, t – maximum number of abusive members.

This expression shows that the number of honest participants ($N-t$) must be three times the number of attackers t to ensure the security of the system. Let us give an example of a scenario of using a consensus protocol in blockchain information technology for an information technology platform for accounting for the sale of weapons using the following method.

Step 1. Registration of transactions. Each arm sale is a separate transaction on the blockchain. The buyer and the seller complete a transaction where they specify the details of the sale (e. g. type of weapon, quantity, price, etc.).

Step 2. Transaction verification. After the transaction is registered, it is verified by network participants. The consensus protocol is used to confirm the correctness of the transaction and its inclusion in the block.

Step 3. Signing and processing of the block. When a transaction receives confirmation from all network participants, it is combined with other confirmed transactions to form a new block. Each block contains the hash signature of the previous block, which provides the chain structure of the blockchain.

Step 4. Block storage and distribution. After the block is formed, it is stored on each network member who confirmed the transaction. This ensures that every participant has the same copy of the blockchain.

Step 5. System status update. After a new block is added to the blockchain, the state of the system is updated. This means that arms sales data is now available for inspection and use by all members of the network.

This method is used to ensure the security and reliability of the information technology platform for accounting for arms sales using blockchain technology.

Decentralized network. Blockchain has a decentralized architecture that avoids single-threaded control and ensures distributed ownership. The following notations can be used to represent the procedure for using a decentralized network in blockchain information technology:

N – number of nodes (network members).

$P(x)$ – the probability of a block of data being successfully included in the block chain.

T – the average time for a node to process and confirm a block of data.

H – the number of blocks in the chain.

The formalized procedure for using a decentralized network in blockchain information technology can be expressed as follows:

$$P(x)=NN-H+1,$$

where $P(x)$ – the probability of a block of data being successfully included in the block chain. This expression shows how the probability depends on the number of active nodes in the network and the number of blocks in the chain.

The method of using a decentralized network in the information technology of the blockchain for the accounting platform for the sale of weapons can be as follows:

Step 1. Product registration. The seller enters data about the weapon into the blockchain network, where each block contains information about the product, its characteristics, certificates and other important information. Each block has a unique identifier and a reference to the previous block.

Step 2. Data validation. Other network participants (nodes) check and confirm the correctness of the information, taking into account all previous blocks. After successful validation, the data becomes permanent and immutable.

Step 3. Product search. The buyer can quickly find the required product in the blockchain registry using unique identifiers or filters.

Step 4. Automatized accounting and tracking. Each transfer of ownership or change in the status of goods is registered in the blockchain network, which provides automatized accounting and tracking of each stage of the sale of weapons.

Step 5. Decentralized security. Due to the decentralized nature of the blockchain, data on the sale of weapons is stored in distributed network nodes, which makes the system less vulnerable to malicious attacks and provides a high level of security.

The method demonstrates how blockchain information technology can be used to build a decentralized accounting system for the sale of weapons, ensuring reliability, security and automatization of the management of this process.

Blockchain provides an opportunity to make secure and irreversible transactions between network participants [12]. A secure transaction in blockchain information technology can be expressed as follows:

Let T = (sender, receiver, amount) – a transaction, where:

sender – the sender of the transaction;

receiver – the receiver of the transaction;

amount – the amount being transferred.

A secure transaction can then be expressed as a signature verification function:

$$verify\text{Signature}(T, publicKey_{sender}, signature)$$

where T – transaction; $publicKey_{sender}$ – the public key of the sender of the transaction; signature – a signature that was created by the sender's private key and is intended for authentication.

This function verifies that the signature created by the sender's private key matches the signature that can be verified using the sender's public key. If the signatures match, then the transaction is considered secure and can be added to the blockchain. The method of using transactions in the blockchain information technology for the accounting platform for the sale of weapons can be the process of confirming and registering the sale of weapons and is as follows:

Step 1. Placing an order for the purchase of weapons by the client.

Step 2. Creation of a transaction by the customer, in which he specifies the details of the order: type of weapon, number of units, cost, delivery address, etc.

Step 3. Signing the transaction with the client's private key.

Step 4. Sending a transaction to the blockchain network. The client sends the generated transaction to the blockchain network.

Step 5. Distribution of the transaction on the network and its arrival to the miners for further processing.

Step 6. Blocks mining. Miners collect transactions from the transaction pool memory and create a new block.

Step 7. Including the client's transaction in a new block.

Step 8. Confirmation and registration. After the client's transaction block has received enough confirmations, the arm purchase order is considered confirmed and is being registered in the system.

Step 9. Providing access to weapon order information (type, quantity, cost, delivery address) to all members of the blockchain network.

This method allows for security, unrivaled authenticity and reliability of the arm purchase process using blockchain technology.

Formation of the ***genesis block***, which is the first block in the chain of blocks (blockchain), which has a unique identifier and establishes the initial state of the system, starting the initial block when creating a blockchain network [13]. The use of the genesis block in blockchain information technology can be formalized as follows:

Let:

G be a genesis block.

H(G) – hash value of the genesis block.

Then, in blockchain information technology, a genesis block *G* with a certain hash value *H(G)* is used as the first block in the block chain.

This can be written as: G=(H(G),data)

where *G* – genesis block; *H(G)* – hash value of the genesis block; data – data that can be included in the genesis block (for example, the date of creation of the blockchain, the version of the protocol, etc).

This expression reflects the use of the genesis block in the blockchain structure as the first block in the sequence.

The method of using the genesis block in blockchain information technology for the weapons sales accounting platform may look as follows:

Step 1. Creating a blockchain. A team of developers creates a new blockchain network to record arms sales. The first step is to create a genesis block.

Step 2. Creating a genesis block. Developers determine the data that will be included in the genesis block. For example, it can be the date of creation of the blockchain, the version of the protocol, initial agreements, or decisions on the distribution of rights of network participants. Then they calculate the hash value of this data and create the first block – the genesis block.

Step 3. Adding a genesis block to the blockchain. A genesis block is added to the blockchain as the first block. This sets the initial state of the blockchain.

Step 4. Starting the network. After the genesis block is created and added to the blockchain, the network is launched. Network participants can start interacting with the system, adding new blocks and transactions.

Step 5. Transfer of network control. After the network is launched, management can be transferred from the project initiators to the community or a decentralized organization. The genesis block serves as the starting point for all future transactions and blocks that make up the network.

Decentralized management is considered as a network management mechanism without centralized power structures [14]. Decentralized management in blockchain information technology can be expressed as follows:

$$C = f(D,P,T),$$

where C – decision or state of the decentralized control system; D – data including transactions, blocks, and the current state of the network; P – parameters defining the rules of the blockchain protocol; T – the time interval during which the system status is updated.

The function f determines the method of processing the input data D, taking into account the parameters P and the time interval T, which leads to the determination of the new state C of the decentralized control system.

Let us give an example of the use of decentralized management in blockchain information technology for an information technology platform for accounting for the sale of weapons, it can be a logistics management system in the supply chain of the arms industry. If the information technology platform is used by manufacturers, suppliers, distributors and customers, each of these participants may have different roles and responsibilities, and they have different levels of access to information and management capabilities. The use of blockchain technology allows to ensure security, transparency and ensures the unavailability of modification of data stored in the system.

The method of using decentralized management can be as follows:

Step 1. Confirmation by the manufacturer of sending a batch of weapons to the distributor by entering the corresponding transaction into the blockchain system.

Step 2. Receipt by the supplier of information about the arrival of a batch of weapons and confirmation of its receipt.

Step 3. Ensuring the delivery of weapons to the client by the distributor and entering relevant data about this operation into the system.

Step 4. Confirmation of receipt of goods by the client.

Step 5. Recording each transaction in the blockchain, entering information about the status of the arms consignments and providing access to all network participants.

This method is aimed at decentralized management in the blockchain system to ensure transparency and reliability of the management of the processes of accounting for the sale of weapons.

A public key is a cryptographic key used to sign transactions and identify users [15].

In blockchain information technology, the public key is used to sign transactions and authenticate users. It can be expressed mathematically as follows:

Let *Kpub* be the public key used to sign transactions in the blockchain. Let us suppose that M is a message and S is a digital signature created using a private key.

Then the expression for signature S by using the public key *Kpub* can be expressed as:

$$S=Sign(K_{pub},M).$$

This expression shows that the signature S is created using the public key *Kpub* and the message M.

The method of using the public key in the blockchain information technology for the weapon sales accounting platform can be presented as follows:

Step 1. User registration. The user registers on the platform, specifying his personal data and receiving a unique identifier. A pair of keys is generated for each user: a public key (for signing and verifying the signature) and a private key (for creating a signature).

Step 2. Signing transactions. The user wants to make a transaction on the platform, for example, to sell or buy a weapon. He creates a digital signature of the transaction using its private key. The signed transaction along with its public key is sent to the blockchain network for further verification.

Step 3. Authenticity check. Other network participants (such as miners) receive the signed transaction and the user's public key. They use the public key to verify the signature of the transaction: if the signature is correct, then the transaction is authentic and can be added to the blockchain.

Step 4. Adding a transaction to the blockchain. After successful verification, the transaction is added to the blockchain and becomes an integral part of the transaction history. All members of the network can view and verify this transaction using the user's public key.

The method contributes to the efficient use of public key in the blockchain information technology for the weapons sales accounting platform.

Formation of requirements for the information technology platform

The conducted analysis makes it possible to form technical requirements for the information technology platform for accounting for the sale of weapons using blockchain technology:

1. Formation of decentralized architecture. Implementation of a system based on a distributed architecture to ensure the decentralization of accounting and management of arms sales.

2. Data encryption. Application of cryptographic protection to ensure confidentiality and security of information on weapons transactions.

3. Creation of smart contracts. Implementation of smart contracts to automatize transactions and ensure fulfillment of terms without the intermediation of third parties.

4. Expanding authentication capabilities. Using a public key to identify and authenticate users with support for two-factor authentication mechanisms.

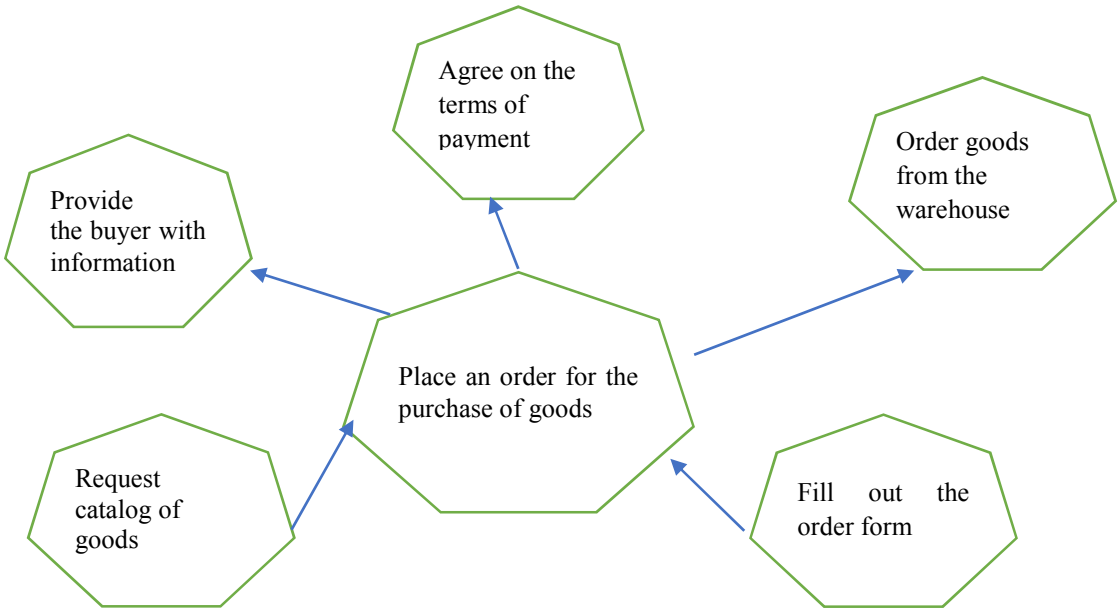

Diagram of options for using the information technology platform

5. Scalability. Ensuring the platform is scalable to handle a large volume of arms transactions while ensuring high performance and system reliability.

6. Ensuring transaction security. Application of transaction confirmation mechanisms and consensus control to prevent double spending and ensure data integrity.

7. Audit and reporting. Ability to audit and generate reports on all arms transactions to ensure compliance with the legislation requirements.

8. Possibility of integration with existing systems. Provision of prerequisites for integration with existing accounting, management and reporting systems to ensure compatibility and interoperability.

These requirements create the basis for the development of an information technology platform using blockchain technology for efficient and secure accounting of arms sales.

Conclusions

The article analyzes the main methods of forming blockchain information technology in the accounting system for the sale of weapons. The conducted analysis showed that the blockchain can be effectively used to create decentralized and reliable weapons accounting systems. The use of hash functions

and cryptographic protection are key elements to ensure security and verification of the integrity of data in the blockchain system. Smart contracts prove to be a powerful tool for automatizing transactions and managing processes in the accounting system for the sale of weapons, helping to avoid conflicts and ensure the accuracy of accounting. Consensus protocols play an important role in ensuring data consistency and solving the problem of double spending in the blockchain network. Decentralized management allows to ensure the adaptability and stability of the system to the influence of external factors. Considering the above methods, blockchain information technology can become a powerful tool for building an efficient and secure accounting system for arms sales. The article provides examples of real cases of the use of blockchain information technology in the field of accounting for the sale of weapons, and a set of methods for obtaining positive results is formed. The study formulated recommendations for the implementation of blockchain technology in the accounting systems for the sale of weapons in order to increase their efficiency and reliability. These findings highlight the importance of using blockchain technology in the field of accounting for the sale of weapons and its potential to improve the efficiency, security and reliability of these systems.

References

1. Yousif, E., & Marshall, W. (2023). Distributed Ledger Technology for Arms Control and Management. Retrieved from https://www.stimson.org/2023/issue-brief-distributed-ledger-technology-for-arms-control-and-management/

2. Wang, X.-Y., Chen, B., & Song, Y. (2023). Dynamic change of international arms trade network structure and its influence mechanism. *International Journal of Emerging Markets*. Advance online publication. https://doi.org/10.1108/IJOEM-07-2022-1058

3. W. S. Arus (1994). Military Technology and the Arms Trade: Changes and their Impact. *The ANNALS of the American Academy of Political and Social Science*, 535(1), 163-174. https://doi.org/10.1177/0002716294535001013

4. Jane Vaynman (2021). Better Monitoring and Better Spying: The Implications of Emerging Technology for Arms Control *Texas National Security Reviev* Vol. 4, Iss 4 l, 33–56. URL: http://dx.doi.org/10.26153/tsw/17498 https://tnsr.org/2021/09/better-monitoring-and-better-spying-the-implications-of-emerging-technology-for-arms-control/

5. David Berdik, Safa Otoum, Nikolas Schmidt, Dylan Porter, and Yaser Jararweh (2021). "A Survey on Blockchain for Information Systems Management and Security". *Information Processing & Management*, 58 (1), 102397. https://doi.org/10.1016/j.ipm.2020.102397.

6. What Is a Blockchain? URL: https://www.ibm.com/topics/blockchain

7. Charles D. Tupper (2011) Distributed Databases. *Data Architecture, Berlin: Morgan Kaufmann*, 385–400. https://www.sciencedirect.com/science/article/pii/B978012385126000022X. doi.org/10.1016/B978-0-12-385126-0.00022-X.

8. Poston Howard (2020). Hash functions in blockchain. URL: https://www.infosecinstitute.com/resources/blockchain-security-overview/hash-functions-in-blockchain/

9. Anurag Singh Choudhary (2023). Concept of Cryptography in Blockchain. URL: https://www.analyticsvidhya.com/blog/2022/09/concept-of-cryptography-in-blockchain/

10. M. Abdelhamid et al. (2019). Blockchain and smart contracts. *Proceedings of the 2019 8th international conference on software and information engineering*. URL: https://kruschecompany.com/smart-contracts-in-blockchain/

11. Guru, B. K. Mohanta, H. Mohapatra, F. Al-Turjman, C. Altrjman, A. Yadav (2023). A Survey on Consensus Protocols and Attacks on Blockchain Technology. *Applied Sciences*. 13(4):2604. https://doi.org/10.3390/app13042604

12. Sultan, Karim & Ruhi, Umar & Lakhani, Rubina. (2018). Conceptualizing Blockchains: Characteristics & Applications. *Conference: 11th IADIS International Conference on Information*

Systems At: Lisbon, Portugal. URL: https://www.researchgate.net/publication/325464908_ Conceptualizing_Blockchains_Characteristics_Applications

13. Shyamasundar, R. & Patil, Vishwas (2018). Blockchain: Revolution in TRUST. *Proceedings of the Indian National Science Academy*. 96. DOI:10.16943/ptinsa/2018/49340.

14. Mohammad Basheer, Faris Elghaish, Tara Brooks, Farzad Pour Rahimian, Chansik Park (2024). Blockchain-based decentralised material management system for construction projects. *Journal of Building Engineering*, Vol. 82,108263. https://doi.org/10.1016/j.jobe.2023.108263. (https://www.sciencedirect.com/science/article /pii/S2352710223024464).

15. Y. Zhang, C. Xu, J. Ni, H. Li and X. Shen (2021). Blockchain-Assisted Public-Key Encryption with Keyword Search Against Keyword Guessing Attacks for Cloud Storage *IEEE Transactions on Cloud Computing*, Vol. 9, No. 04, 1335–1348. DOI: 10.1109/TCC.2019.2923222

METHODS OF BLOCKCHAIN TECHNOLOGY FORMATION IN THE ARMS SALES ACCOUNTING SYSTEM

Yurii Yarymovych, Nataliia Kunanets

Lviv Polytechnic National University,
Information Systems and Networks Department, Lviv, Ukraine
E-mail: Yurii.A.Yarymovych @lpnu.ua, ORCID: 0009-0006-1391-3214
E-mail: nataliia.e.kunanets@lpnu.ua, ORCID: 0000-0003-3007-2462

The article explores the application of blockchain technology in the field of arms sales accounting. The authors examine the main methods of forming such technology, including distributed ledger, hash functions, cryptographic protection, smart contracts, consensus protocols, decentralized network, transactions, genesis block, decentralized governance, and public key. The authors analyze the potential of these methods in creating an efficient and secure arms sales accounting system. The conclusions of the article underscore the importance of using blockchain technology in this field and its potential to enhance the efficiency and security of arms sales accounting.

Key words: blockchain; distributed ledger; hash functions; cryptographic protection; smart contracts; consensus protocols; decentralized network; transactions; genesis block; decentralized governance; public key.