UDC 004.056.55:004.89 **doi:** https://doi.org/10.20998/3083-6298.2025.03.04

Oleksandr Iegrashyn[1], Serhii Pohasii[1], Marharyta Melnyk[2]

[1] National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
[2] Science Entrepreneurship Technology University, Kyiv, Ukraine

# EVOLUTION OF ACCOUNTING SYSTEMS AND CRYPTOGRAPHIC MEANS OF THEIR PROTECTION IN THE CONDITIONS OF DECENTRALIZATION

**Abstract. The relevance of the study**. The article is devoted to an overview of the evolution of accounting systems, which are formed under the influence of the development of blockchain technologies and cryptographic protection tools. The relevance of the topic is due to the growing requirements for transparency, stability and trust in the conditions of digitalization, when centralized models increasingly demonstrate vulnerability to compromise, monopolization of control and cyber threats. **The subject of research** is cryptographic mechanisms: digital signatures, hash functions, commitment schemes, zero-disclosure protocols, smart contracts, and selective data disclosure models that ensure authenticity, integrity, and access control in decentralized accounting systems. **The purpose of the article** is to conduct a theoretical and analytical review of the evolution of accounting systems: from centralized models to decentralized architectures, with a focus on the role of cryptographic mechanisms to ensure the integrity, authenticity and protection of information accounting data. **Results.** Key trends in the development of decentralized registries are identified, in particular the integration of SSI approaches, the optimization of consensus algorithms, the combination of on-chain and off-chain infrastructures and the increasing role of regulatory mechanisms. It is shown that modern cryptographic tools are at different stages of technological maturity and require further improvement to meet the requirements of performance, scalability and confidentiality. **Conclusions.** It is substantiated that cryptography is becoming a key driver of the transition to a new accounting paradigm, in which trust is provided not by centralized control, but by mathematical guarantees, transparent rules, and the possibility of open verification. Directions for further research are identified, including improving the performance of ZKP in practical applications, standardizing confidential access models, and developing adaptive architectures of decentralized systems for real business environments.

**Keywords:** decentralized accounting systems, cryptographic mechanisms, data integrity, access control, zero-knowledge proof, blockchain.

## Introduction

**Problem relevance.** The current state of the digital economy demonstrates that classic accounting systems built on a centralized architecture are gradually losing their ability to meet the needs of organizations with a high level of interaction, distributed business processes and increased transparency requirements. In traditional models, all primary data was concentrated in one information center: a central database or corporate ERP platform. Such an architecture was effective in conditions of stable organizational structures: it simplified administration, unified regulations and allowed for centralized control of the reliability of information.

With the development of digital ecosystems and an increase in the number of interacting entities, key limitations of the centralized model have become apparent. These include: insufficient level of inter-organizational trust, risks of data manipulation on local nodes, weak resistance to internal threats and significant difficulties with synchronization of large volumes of transactions in real time. These factors are the ones that make it necessary to find new approaches that would ensure transparency, stability and shared responsibility for data.

The traditional foundation of information systems has long been the principle of double entry, which ensured the internal consistency of operations. However, the increase in the complexity of business logic and the growth in the number of transactions between independent organizations have demonstrated the limitations of this approach outside the boundaries of a separate institution. The evolutionary continuation was the concept of triple entry, that is, the creation of a common, immutable transaction log that serves as an independent source of verification for all participants in the interaction.

It was this idea that laid the foundations for the formation of decentralized accounting systems that use cryptographic mechanisms to ensure the integrity, authenticity and ownership of data. In combination with distributed ledger technologies, it became the answer to the requests of modern digital platforms, where the level of trust should be ensured not by organizational structures, but mathematically and algorithmically.

Thus, the relevance of studying the evolution of accounting systems today is directly related to the transition of global information infrastructures to decentralized models, in which cryptographic protection tools, consensus protocols, and mechanisms for record immutability play a key role. Analysis of these trends allows not only to understand the nature of transformations, but also to identify promising directions for the development of accounting systems capable of functioning in conditions of high interaction, cyber threats, and the growing need for transparency.

**Literature review.** To gain a deeper understanding of these trends, it is necessary to analyze scientific sources in which researchers highlight the evolution of accounting models and mechanisms for ensuring trust in decentralized environments. The search for mechanisms to increase trust, transparency, and auditability in various

 

sectors has stimulated the development of alternatives to traditional centralized accounting models [1]. In this context, a new concept has emerged – decentralized accounting systems (DARS), which combine the capabilities of blockchain with distributed ledger procedures. They allow for transactions without intermediaries and automate control processes using smart contracts.

As researchers noted back in 2016 [2], the basis of DARS is the blockchain, which ensures the immutability of records, cryptographic protection and transparency of transactions. Such properties create a technical prerequisite for the formation of a trust environment without a single administrator, which is critically important for accounting and auditing systems. An additional role is played by the tokenization of digital assets, which allows building flexible mechanisms for managing access rights and ownership in distributed environments.

The use of blockchain has provided the technical means to create shared, immutable transaction logs. In DARS, such a log becomes the only reliable source of records for all network nodes, and the consensus mechanism guarantees data consistency without a central regulator. Analysis of sources [1, 3] demonstrates the potential of blockchain to transform audit processes: smart contracts allow for the automation of control, verification, and logging of events. However, this imposes new requirements on system design, from the choice of a consensus protocol to the organization of key management.

In modern literature, there are different interpretations of DARS. In [1], attention is focused on the impact of blockchain on accounting and auditing procedures; smart contracts are considered as a tool for automating checks and reducing the human factor. In [4], their role in ensuring reliable fulfillment of accounting conditions and automatic updating of registers is emphasized. This simplifies the procedures for entering and confirming records and makes the system less dependent on administrative intervention.

At the same time, the authors [5] focus on tokens as universal units of account, means of access or confirmation of trust. In DARS, tokenization allows you to create a unified verification model, where each object has a unique cryptographic representation. Of particular importance are stablecoins and other stable tokens that provide a stable value for settlements.

Along with the advantages of DARS, there are also significant challenges. In particular, research [6] indicates problems of scalability, vulnerability of smart contracts, the possibility of consensus attacks and difficulties with data coordination between nodes. Additionally, the decentralized nature of the systems complicates legal liability and regulatory mechanisms. In [7], key barriers to the implementation of DARS are identified, related to regulatory requirements, confidentiality and integration with existing information systems. Studies [8, 9] focus on identity management, comparing current frameworks in which the user controls their own digital attributes and cryptographic evidence. [10] analyzes the prospects for blockchain applications in authentication and key exchange protocols.

Some authors [11] emphasize that along with increasing inclusivity and decreasing transaction costs, DARS creates new risks related to cybersecurity and the regulatory environment. In [12], an integrative definition of DARS is proposed as a system that combines financial principles with technological innovations – blockchain, tokenization and algorithmic control mechanisms.

Along with fully public blockchains, hybrid models that combine private registries with off-chain storages are attracting increasing attention. In such architectures, confidential data is placed off-chain, while only hashes or commitments are recorded in the blockchain, which guarantee integrity and provide auditability. This approach allows you to balance security, transparency and confidentiality requirements, which is especially important in corporate and financial systems. Literature sources [1, 13] indicate that methods for integrating on-chain and off-chain components are still actively being formed, and the development of optimal practices is an open research task.

In summary, current work indicates that decentralized accounting systems are a natural step in the transition from centralized data management to self-governing information ecosystems, where trust is based not on institutional authority, but on cryptographic and algorithmic mechanisms. DARS can be defined as a system that provides storage, processing and verification of accounting data in a network of peer nodes, using consensus, cryptography and smart contracts to ensure the integrity and authenticity of information.

**The aim of the article** is a theoretical and analytical review of the evolution of accounting systems: from centralized models to decentralized architectures, with a focus on the role of cryptographic mechanisms to ensure the integrity, authenticity and protection of information accounting data.

## 1. Analysis of the evolution of accounting systems

Based on the literature analysis [1, 3, 7, 8, 13-17], Table 1 summarizes the main directions of development of accounting systems: from centralized to decentralized models, highlighting the problems of operation, advantages, as well as key aspects that modern researchers pay attention to.

*Table 1* – **The evolution of accounting systems: from centralized to decentralized models**

| Development stage / System type | Highlighted issues/limitations | Positive aspects and advantages |
|---|---|---|
| *Centralized accounting systems (ERP, 1980–2010)* | Dependence on a single center; possibility of data manipulation; complexity of auditing between organizations | Easy administration, clear control model, easy integration into internal business processes |
| *Network (distributed) accounting* | Data consistency issues; difficulty verifying the | Increased fault tolerance; ability to work in |

| Development stage / System type | Highlighted issues/limitations | Positive aspects and advantages |
|---|---|---|
| *systems (2010–2015)* | authenticity of records; no common "source of truth" | geographically distributed structures |
| *Triple-entry accounting (conceptual stage)* | Lack of unified technical standards; need for reliable cryptographic protocols | Automatic verification of transactions; improving trust between participants |
| *Permissioned blockchain for accounting (2020–2023)* | Limited scalability; difficulty integrating with existing ERPs; need for regulatory recognition of records | Immutability of transactions; real-time auditability; increased transparency |
| *Public blockchain systems (2020–2024)* | High power consumption, slow processing, data privacy issues | Complete independence from central authorities; reliability and provability of transaction history |
| *Self-sovereign identity (2023–2025)* | Key management; access recovery; need for new revocation protocols | User control over their own data; increased access security; support for audit logs |
| *Zero-knowledge proof systems (2024–2025)* | High computational costs; difficulty integrating into production environments | Combining transparency and confidentiality; possibility of private audit |
| *Hybrid accounting architectures (on-chain/off-chain, from 2025)* | The need for interoperability standards; the risk of a disconnect between on-chain and off-chain data | Flexibility, scalability, compliance with legal requirements regarding personal data |

The analysis of the evolution of accounting systems, presented in Table 1, shows a clear trend of transition from centralized architectures to hybrid and, ultimately, to fully decentralized models based on blockchain technologies and cryptographic protocols. The central idea of this evolution is the replacement of administrative trust with technical trust, when the integrity and authenticity of data is ensured not by a separate server or organization, but by consensus between equal network participants.

Centralized systems, despite their simplicity, have proven vulnerable to internal threats, attacks and data manipulation due to their dependence on a single center of control. Hybrid models have become an intermediate stage of development, which has allowed the integration of blockchain elements to increase the transparency and reliability of accounting records, while maintaining the manageability and performance of traditional databases.

Decentralized architectures that are now gaining popularity provide immutability, transparency, and cryptographic protection for all transactions, making them particularly promising for building accounting, auditing, asset management, and digital identification systems. However, issues of scalability, power consumption, regulatory acceptance, and interoperability of such systems remain open.

Thus, the further development of the industry is associated with the search for effective hybrid and optimized decentralized solutions that will provide a balance between security, trust, performance and compliance with regulatory requirements.

The analysis of scientific sources in the field of decentralized accounting systems [7, 8, 13, 16, 18, 19] made it possible to identify a number of current trends that determine the current directions of their evolution:

1. Combining Autonomous Digital Identity (SSI) with Blockchain for Access Management and Compliance. SSI is increasingly being seen as the foundational mechanism for managing digital identities in ledgers. It enables the selective disclosure of user attributes, while critical cryptographic proofs of authenticity can be stored on the blockchain, creating an increased level of trust and controlled transparency.

2. Active use of zero-knowledge cryptographic proofs (ZKP). The use of protocols that allow to confirm the truth of a certain statement without providing additional data is growing. Such schemes provide a high level of privacy and trust, while preserving the evidentiary value of accounts. Research proves that ZKP is a key tool in achieving a balance between auditability and privacy protection, and also offers practical scenarios for integrating these protocols into real systems.

3. Improving BFT consensus for corporate systems. One of the important areas of development is the modernization of Byzantine Fault-tolerant (BFT) consensus protocols to improve their efficiency in corporate decentralized registries. Hierarchical, clustered, and combined models are being developed to achieve the optimal balance between performance, security, and minimal latency.

4. Development of hybrid architectures using AI and IoT. There is growing interest in decentralized systems that integrate AI and IoT components for automated data collection and verification. This approach aims to ensure efficient load distribution between blockchain components and external repositories, where cryptographic commitments are used to guarantee integrity.

5. Increased focus on regulatory, legal and procedural aspects. Research highlights that technological innovations alone do not guarantee the appropriate level of security and trust. The implementation of decentralized accounting systems requires a comprehensive regulatory framework, clear operational policies and audit procedures. Defining roles, responsibilities, legal status of records and rules of interaction between participants is critical to implementing and ensuring the protection of these systems in commercial and government processes. The presence of transparent regulatory standards acts as a catalyst for the adoption of decentralized technologies, providing a balance between innovation and legal certainty.

A summary of the trends considered is presented in Table 2.

*Table 2* – **Generalization of trends in the development of accounting system architectures towards decentralization**

| Trend | The essence of the changes | Unresolved issues |
|---|---|---|
| *From centralization to decentralization* | Moving from a single trust center to a shared distributed verification mechanism | Agreement between the parties, legal recognition of digital records |
| *From transparency to privacy through cryptography* | Using ZKP and SSI for controlled data disclosure | Computational efficiency, key management |
| *From static audit to continuous monitoring* | Smart contracts and analytical algorithms create a "live audit" | Issues of liability and reliability of automated procedures |
| *From monolithic ERPs to integrated ledger ecosystems* | Accounting becomes part of the organization's digital infrastructure | The need for standardization of APIs, data ontologies, reporting formats |

The trends in Table 2 demonstrate a systemic shift from traditional centralized accounting models to flexible decentralized accounting systems, where cryptographic mechanisms, automated verification procedures, and data integration across organizational domains play key roles. This evolution is changing the accounting paradigm itself, from administrative control to algorithmic trust, while creating new challenges in the areas of legal regulation, standardization, and cyber resilience.

However, despite significant scientific and applied progress in the creation of decentralized accounting systems, a number of key issues remain unresolved.

First, the integration of zero-disclosure proofs into real-world accounting processes still has a gap between theoretical models and the performance requirements of enterprise-level systems. This requires the development of optimized proof generation schemes, as well as the use of hardware and parallel computing to achieve acceptable service level agreement rates.

Second, autonomous digital identity systems based on cryptographic key management face challenges in restoring access, revocation, and trust in nodes. Production systems require standardized operational policies for cryptographic key management, including procedures for backing up, delegating, and auditing.

Third, in the area of ensuring a balance between transparency and confidentiality, there is a need for universal patterns for selective data disclosure, evidence generation, and audit trails without compromising privacy. Despite the promise of cryptographic protocols that allow data to be authenticated without revealing the information itself, there are currently no industrial solutions that can scale such mechanisms to real business workloads.

## 2. Architectural foundations and conceptual principles of decentralized accounting systems

As already emphasized in the study [6], the fundamental basis of decentralized accounting systems is the concept of cryptographic trust, which replaces traditional centralized administrative control. In such systems, trust is formed not through institutional oversight, but through the use of cryptographic mechanisms: digital signatures, hash functions, commitment schemes and zero-disclosure protocols. The use of these tools ensures the immutability of records, the authenticity of transactions and the provability of the actions of all participants even in a fully distributed environment.

As already noted, an important component of modern DARS architectures is the autonomous identity model, which allows users to independently manage their digital attributes without the participation of centralized registrars or intermediaries [20]. In such a model, the user does not delegate the management of personal data to third-party organizations, but acts as the source and carrier of verified evidence of his identity. Trust in these attributes is ensured by cryptographically confirmed certificates and decentralized verification mechanisms. This forms a new ecosystem of decentralized trust, where control and confirmation of operations are carried out not by administrators, but by network consensus.

Thus, the development of architectural principles of accounting systems demonstrates the transition from centralized, organizationally managed structures to a decentralized trust infrastructure, within which control, verification and audit mechanisms are built directly into the technological platform. In this context, decentralized accounting systems act not only as a means of protecting information, but also as the basis for forming a new model of digital asset management, increasing transparency and accountability in distributed environments.

Table 3 provides a description of each stage of development of decentralized accounting systems depending on the type of system and the technological basis of its construction.

*Table 3* – **Stages of development of decentralized accounting systems, their characteristic features and architectural features**

| Stage of development of a decentralized accounting system | System type and characteristics | Technological basis / architectural features |
|---|---|---|
| *Stage I (2015–2020)* | Triplet accounting – creating a shared transaction log signed by all parties | The concept of "third record" with cryptographic signatures; the birth of the idea of a distributed ledger; the use of a shared environment with trust |
| *Stage II (2020–2023)* | Permissioned blockchain for accounting – distributed ledgers with access control; PBFT or Raft | Private (permissioned) blockchain architecture; transaction access control; consensus among trusted |

| Stage of development of a decentralized accounting system | System type and characteristics | Technological basis / architectural features |
|---|---|---|
| | consensus | participants |
| *Stage III (2020–2024)* | Public blockchain systems – open networks (Ethereum, Bitcoin) for automating records and data verification through smart contracts | Public blockchain with decentralized consensus (PoW, PoS); smart contracts; open access to transaction history |
| *Stage IV (2023–2025)* | SSI-oriented accounting systems – user identity management without intermediaries, DID, Verifiable Credentials | Decentralized identifiers (DID) integration with ledger; autonomous key management; audit-trail support |
| *Stage V (2024–2025)* | Zero-knowledge proof systems – selective confirmation of transactions without revealing the content | Implementation of zk-SNARK/STARK for privacy; additional cryptographic layer on top of blockchain; private audit |
| *Stage VI (з 2025 р.)* | Hybrid accounting architectures (on-chain/off-chain) – combining blockchain with traditional databases to optimize performance | Dual architecture: hashes and proofs stored on-chain, data stored off-chain; interoperability and compatibility standards |

As can be seen from Table 3, the evolution of decentralized accounting systems demonstrates a gradual transition from simple concepts of a shared transaction log to complex architectures that combine blockchain, cryptography, and autonomous identity management. While in the early stages the main achievement was to eliminate the need for a centralized intermediary, further development led to architectures with consensus mechanisms (PBFT, PoS) and smart contracts that ensured automation and immutability of records. In modern systems, SSI and ZKP are integrated, which shifts the focus from trust in nodes to cryptographically guaranteed verifiability and confidentiality. The latest stage is hybrid on-chain/off-chain architectures that seek to balance the security of blockchain with the scalability of traditional systems, forming the basis for the practical implementation of decentralized accounting in corporate and government environments.

Thus, the conducted research shows that the structure of the architecture of a decentralized accounting system includes the following main components:

a distributed transaction log that ensures the immutability of records;

participating nodes that perform verification and storage of data copies;

smart contracts that automate business logic;

cryptographic modules to ensure confidentiality, signing and verification of transactions;

access interfaces through which integration with corporate systems and external services occurs.

Building the architecture of decentralized accounting systems involves not only the technical organization of components such as nodes, communication channels, consensus protocols or data storage, but also a conceptual rethinking of the very principle of trust in accounting processes. In such systems, the architecture acts as a reflection of the basic logical and functional principles: instead of centralized control, there is distributed mutual verification, instead of administrative management, there is algorithmic consistency, instead of institutional trust, there is a cryptographic guarantee of authenticity.

## 3. Cryptographic mechanisms for ensuring trust and protection in decentralized systems

As is known, the main goals of using cryptographic mechanisms for ensuring data security are to guarantee authentication, integrity and confidentiality of data. The transition from centralized models to decentralized accounting systems, in which data is stored distributedly, and trust is ensured not through administrative control, but through cryptography, puts forward new requirements for the architecture and operational mechanisms for ensuring trust and protection. If earlier authentication, confidentiality, integrity and availability were ensured by centralized servers, then in decentralized registries this function is implemented through a set of cryptographic tools, such as digital signatures, hash functions, commitments, proofs without disclosure, key management mechanisms, tokenization and smart contracts. Therefore, understanding the theoretical foundations of such mechanisms is a necessary prerequisite for their practical application in the context of accounting systems.

Let us consider in more detail the cryptographic principles that provide the basic security properties of authenticity, integrity, and controlled access.

Authentication is the process of confirming that a participant in a system is who he claims to be. In the cryptographic context, this is implemented through public/private keys, digital signatures, and mutual authentication mechanisms. For example, a digital signature algorithm allows a private key to create a signature that can be verified by a public key and confirms the origin of a message and its integrity. [21]

In a decentralized system, the cryptographic authentication model includes the following stages:

key generation. The user creates a pair of cryptographic keys: private (for signing) and public (for verification). These keys form the basis of the user's cryptographic identity;

formation of a decentralized identifier (DID). Based on the public key, a DID is generated and registered in a decentralized registry. The DID serves as a unique record that links the user to their public key without intermediaries;

cryptographic signature. When accessing the system, the user signs a request or transaction with a private key, which guarantees the authenticity and impossibility of forging the message;

signature verification. A system node or smart contract verifies the signature using the public key obtained from the DID record. If the verification is successful, the user is recognized as authenticated and is granted access to the system resource or function.

Thus, the authentication process in decentralized accounting systems occurs without the participation of centralized verification bodies and is based on asymmetric cryptography. DID identifiers act as a key link between the user and the network, providing self-control over digital identity, preserving the integrity of transactions and reducing the risks of data compromise.

Data integrity means that information has not been tampered with since its creation or last verification. In cryptographic systems, this is guaranteed using hash functions, commitment schemes and, in distributed ledgers, through a sequence of blocks that reinforce each other or the “hash of the previous block” function. [22] That is, integrity in a distributed ledger is based on the use of hash dependencies between blocks. This approach makes it impossible to change data without a corresponding update of the entire chain, which guarantees the reliability and immutability of transaction history in a distributed environment.

Access control determines who has the right to perform what actions in the system. In decentralized accounting systems, roles, attribute-based access (ABAC), access control lists (ACLs), or smart contracts that control access programmatically are widely used. [23]

As a mechanism for managing user rights, smart contracts are used that act as an intermediary between the user and system resources. Next, the smart contract checks the user's role or attribute according to the access policy (for example, according to the ABAC principles). If the user meets the requirements, the contract generates and issues an access token - a cryptographic marker that certifies the right to perform a certain action. At the final stage, the system node verifies the token before performing the requested operation, which provides decentralized, transparent and controlled access without a centralized administrator.

Thus, the use of smart contracts for access control allows for the implementation of an automated, verifiable and secure authorization model. This approach eliminates the need for centralized user management, increases trust between nodes and guarantees the implementation of access policies at the code level, which is especially important for decentralized accounting systems.

As a result of the research, the most effective cryptographic mechanisms that ensure authenticity, integrity and trust in decentralized accounting systems can be identified:

1. Authentication module (digital signature) – provides authentication, i.e. allows you to uniquely establish who performs the operation; guarantees non-repudiation, since the signature cannot be forged without the owner's private key; helps build trust between network nodes without an administrator.

2. ZKP-confirmation – allows for selective disclosure of attributes while maintaining confidentiality; increases the level of trust and privacy due to the fact that participants can verify the fact without receiving "extra" information; optimally integrates into the process of verifying attributes in the smart access contract.

3. Hashing and cryptographic commitments – ensures data integrity due to the immutability of hashes in the blockchain; implements a reliable audit model: any off-chain modification of data can be detected due to hash divergence; eliminates the need to store large amounts of data in the blockchain, but maintains trust in their authenticity.

4. Smart access contract – uses digital signatures and ZKP to verify access requirements; guarantees determinism, i.e. the same verification result on all nodes; protects against forgery and unauthorized changes.

5. Cryptographic validation of user data – provides authorization, i.e. confirms that the user has the right to perform an action; promotes data integrity and authenticity through cryptographic verification; works in conjunction with a smart contract and an authentication module.

Thus, each component of cryptographic mechanisms provides a separate aspect of protection, which together form a cryptographic foundation of trust that replaces centralized control and ensures the secure functioning of decentralized accounting systems.

## Discussion of results

The analysis conducted in the article shows that the evolution of accounting systems from centralized models to decentralized solutions is driven by the need to increase trust, resilience to compromise, and reduce dependence on a single control center. At the same time, the transition to decentralized architectures places new demands on cryptographic mechanisms that must provide not only authentication and integrity, but also scalable privacy, transparent auditing, and fault tolerance.

It should be noted that despite significant progress in the development of blockchain infrastructures, cryptographic tools are at different stages of maturity in terms of performance and integration into real-world accounting processes. Of particular note is the gap between theoretical cryptographic models and the practical constraints of enterprise systems, where service level agreements, throughput, and low latency remain critical.

In addition, it has been shown that the combination of on-chain and off-chain data storage requires a consistent model of access control and attribute

verification, which actualizes the role of smart contracts as cryptographically secure mechanisms for automating rules. However, the lack of industry standards and patterns for confidential access and scalable privacy limits the widespread adoption of decentralized accounting systems in critical industries.

Taking into account the identified limitations, promising areas of further research towards the formation of a system for protecting decentralized accounting systems are the development of high-performance proof schemes with zero disclosure, the formation of standardized models of confidential access, as well as the construction of agreed-upon interoperable protocols capable of integrating different accounting domains into a single decentralized space of trust.

## Conclusions

The article summarizes the evolutionary path of accounting systems and identifies key architectural principles that shape modern decentralized models. It shows that cryptography is the foundation of their secure functioning, from ensuring data integrity to building trust between participants without intermediaries.

The mechanisms considered, such as digital signatures, cryptographic hashes, commitments, smart contracts, ZKP protocols and selective attribute disclosure, form a comprehensive security infrastructure capable of supporting transparency, security and decentralization. At the same time, it has been established that the further development of decentralized accounting systems requires the optimization of cryptographic protocols, the formation of industry standards and overcoming performance limitations.

Thus, cryptographic mechanisms actually become the basis of a new accounting model in which trust arises not due to central control, but due to mathematically proven guarantees, transparent rules and the possibility of open verification of each operation.

## References


1. Han, H., Shiwakoti, R.K., Jarvis, R., Mordi, C. and Botchie, D. (2023), “Accounting and auditing with blockchain technology and artificial intelligence: A literature review”, *International Journal of Accounting Information Systems*, Vol. 48, https://doi.org/10.1016/j.accinf.2022.100598
2. Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Goldfeder, S. (2016), “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”, *Princeton University Press*, 308 p. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.lopp.net/pdf/princeton_bitcoin_book.pdf
3. Liu, C., Muravskyi, V. and Wei, W. (2024), “Evolution of blockchain accounting literature from the perspective of CiteSpace (2013–2023) ”, *Heliyon*, Vol. 10, iss. 11, https://doi.org/10.1016/j.heliyon.2024.e32097
4. Buterin, V. (2015), “A Next-Generation Smart Contract and Decentralized Application Platform”, *Ethereum White Paper*, URL: https://courses.cs.duke.edu/spring23/compsci512/papers/ethereum.pdf
5. Javaid, M., Haleem, A., Singh, R. P., Suman, R. and Khan, S. (2022), “A review of Blockchain Technology applications for financial services”, *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, Vol. 2, iss. 3, https://doi.org/10.1016/j.tbench.2022.100073
6. Zetzsche, D. A., Buckley, R. P. and Arner, D. W. (2020), “Decentralized Finance (DeFi)”, *Journal of Financial Regulation*, Vol. 6, pp. 172–203, https://doi.org/10.1093/jfr/fjaa010
7. Akter, M., Kummer, Tyge-F. and Yigitbasioglu, O. (2024), “Looking beyond the hype: The challenges of blockchain adoption in accounting”, *International Journal of Accounting Information Systems*, Vol. 53, https://doi.org/10.1016/j.accinf.2024.100681
8. Pava-Díaz, R.A., Gil-Ruiz, J. and López-Sarmiento, D. A.(2024), “Self-sovereign identity on the blockchain: contextual analysis and quantification of SSI principles implementation”, *Sec. Blockchain Security and Privacy*, Vol. 7, https://doi.org/10.3389/fbloc.2024.1443362
9. Nair, A. J., Manohar, S. and Rao, S. A B. (2025), “Self-sovereign identity in e-governance: blockchain solutions for fintech compliance and citizen-centric financial services”, *Humanities and Social Sciences Communications*, Vol. 12, https://doi.org/10.1057/s41599-025-05880-y
10. Luo, X., Chen, X., Chen, X. and Cheng, Q. (2024), “A survey on the application of blockchain in cryptographic protocols”, *Cybersecurity*, Vol. 7, https://doi.org/10.1186/s42400-024-00324-7
11. Read, O. (2025), “Decentralised Finance: Growth, Risks and Regulation of a Shadow Financial System with Crypto-assets”, *Working Paper*, No. 18, URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.econstor.eu/bitstream/10419/328275/1/1938433971.pdf
12. Bosu, A., Iqbal, A., Shahriyar, R. and Chakraborty, P. (2019), “Understanding the motivations, challenges and needs of Blockchain software developers: a survey”, *Empirical Software Engineering*, Vol. 24(4), pp. 2636–2673, https://doi.org/10.1007/s10664-019-09708-7
13. Prokopenko, O., Koldovskiy, A., Khalilova, M., Orazbayeva, A. and Machado, J. (2024), “Development of Blockchain Technology in Financial Accounting”, *Computation*, Vol. 12(12), https://doi.org/10.3390/computation12120250
14. Anis, A. (2023), “Blockchain in accounting and auditing: unveiling challenges and unleashing opportunities for digital transformation in Egypt”, *Journal of Humanities and Applied Social Sciences*, Vol. 5, No. 4, pp. 359-380, DOI:10.1108/JHASS-06-2023-0072
15. Ou, H.-H., Chen, G.-Yu. and Lin, I.-Ch. (2025), “A Self-Sovereign Identity Blockchain Framework for Access Control and Transparency in Financial Institutions”, *Cryptography*, Vol. 9(1), https://doi.org/10.3390/cryptography9010009
16. Zhou, L., Diro, A., Saini, A., Kaisar, S. and Hiep, P. C. (2024), “Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities”, *Journal of Information Security and Applications*, Vol. 80, https://doi.org/10.1016/j.jisa.2023.103678
17. Yuan, F., Huang, X., Zheng, L., Wang, L., Wang, Y., Yan, X., Gu, S. and Peng, Y. (2025), “The Evolution and Optimization Strategies of a PBFT Consensus Algorithm for Consortium Blockchains”, *Information*, Vol. 16, iss.

4, https://doi.org/10.3390/info16040268
18. Fang, J., Feng, T., Guo, X. and Wang, X.(2024), “Privacy-enhanced distributed revocable identity management scheme based on self-sovereign identity”, *Journal of Cloud Computing*, https://doi.org/10.1186/s13677-024-00715-8
19. Guo, R., Guo, Z., Lin, Z. and Jiang, W. (2024), “A hierarchical byzantine fault tolerance consensus protocol for the Internet of Things”, *High-Confidence Computing*, Vol. 4, iss. 3, https://doi.org/10.1016/j.hcc.2023.100196
20. Schardong, F. and Custódio, R. (2022), “Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy”, *Sensors*, Vol. 22(15), https://doi.org/10.3390/s22155641
21. Digital Signature Algorithm / *Wikipedia*. URL: https://en.wikipedia.org/wiki/Digital_Signature_Algorithm?utm_source=chatgpt.com
22. Cryptographic hash function / *Wikipedia*. URL: https://en.wikipedia.org/wiki/Cryptographic_hash_function?utm_source=chatgpt.com
23. Ullah, S. S., Oleshchuk, V. and Pussewalage, H. S. G. (2023), “A survey on blockchain envisioned attribute based access control for internet of things: Overview, comparative analysis, and open research challenges”, *Computer Networks*, Vol. 235, https://doi.org/10.1016/j.comnet.2023.109994

Received (Надійшла) 30.09.2025
Accepted for publication (Прийнята до друку) 14.10.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

**Єграшин Олександр Олексійович** – аспірант, кафедра кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
**Oleksandr Iegrashyn** – PhD student of Cyber Security Department, National Technical University “Kharkiv polytechnic institute”, Kharkiv, Ukraine;
e-mail: oiegrashyn@gmail.com; ORCID Author ID: https://orcid.org/0009-0006-8176-4601.

**Погасій Сергій Сергійович** – доктор технічних наук, доцент, професор кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
**Serhii Pohasii** – Doctor of Technical Sciences, Docent, Professor of Cyber Security Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: spogasiy1978@gmail.com; ORCID Author ID: https://orcid.org/0000-0002-4540-3693;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57217487471.

**Мельник Маргарита Олександрівна –** кандидат технічних наук, доцент кафедри кібербезпеки та захисту інформації, Університет науки, підприємництва та технологій, Київ, Україна;
**Marharyta Melnyk** – PhD, assistant professor Department of Cyber Security and information protection, Science Entrepreneurship Technology University, Kyiv, Ukraine;
e- mail: Margaritochek@gmail.com; ORCID Author ID: https://orcid.org/0000-0003-0619-7281;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=58577562400.

## ЕВОЛЮЦІЯ ОБЛІКОВИХ СИСТЕМ ТА КРИПТОГРАФІЧНІ ЗАСОБИ ЇХ ЗАХИСТУ В УМОВАХ ДЕЦЕНТРАЛІЗАЦІЇ

О.О. Єграшин, С.С. Погасій, М. О. Мельник

**Анотація. Актуальність дослідження.** Стаття присвячена огляду еволюції облікових систем , що формуються під впливом розвитку блокчейн-технологій та криптографічних засобів захисту. Актуальність теми зумовлена зростанням вимог до прозорості, стійкості та довіри в умовах цифровізації, коли централізовані моделі дедалі частіше демонструють вразливість до компрометації, монополізації контролю та кіберзагроз. **Предметом дослідження** є криптографічні механізми: цифрові підписи, хеш-функції, комітмент-схеми, протоколи нульового розголошення, смарт-контракти та моделі селективного розкриття даних, які забезпечують автентичність, цілісність і контроль доступу в децентралізованих облікових системах. **Мета статті** полягає у проведенні теоретико-аналітичного огляду еволюції облікових систем: від централізованих моделей до децентралізованих архітектур, із зосередженням на ролі криптографічних механізмів, для забезпеченні цілісності, достовірності та захисту інформаційних облікових даних. **Результати**. Визначено ключові тенденції розвитку децентралізованих реєстрів, зокрема інтеграцію SSI-підходів, оптимізацію консенсусних алгоритмів, поєднання on-chain та off-chain інфраструктур і зростання ролі регуляторних механізмів. Показано, що сучасні криптографічні інструменти перебувають на різних етапах технологічної зрілості та потребують подальшого удосконалення для відповідності вимогам продуктивності, масштабованості та конфіденційності. **Висновки.** Обґрунтовано, що криптографія стає ключовим драйвером переходу до нової парадигми обліку, у якій довіра забезпечується не централізованим контролем, а математичними гарантіями, прозорими правилами та можливістю відкритої верифікації. Визначено напрями подальших досліджень, серед яких підвищення продуктивності ZKP у практичних застосуваннях, стандартизація моделей конфіденційного доступу та розробка адаптивних архітектур децентралізованих систем для реальних бізнес-середовищ.

**Ключові слова:** децентралізовані облікові системи, криптографічні механізми, цілісність даних, контроль доступу, доказ з нульовим розголошенням, блокчейн.