Journal homepage: https://itce.com.ua/en

Information Technologies and Computer Engineering **Vol. 22, No. 2. 2025**

Article's History: Received: 10.04.2025 Revised: 15.07.2025 Accepted: 28.08.2025

UDC 004.421.7:004.62:338.48 DOI: 10.31649/vitce/2.2025.20

SDN and blockchain integration: Overview of the current state and prospects for ensuring network security

Oleksandr Pidpalyi*

Postgraduate Student
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteiskyi Ave., Kyiv, Ukraine
https://orcid.org/0009-0007-6852-7959

Oleksandr Romanov

Doctor of Technical Sciences, Professor
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteiskyi Ave., Kyiv, Ukraine
https://orcid.org/0000-0002-8683-3286

Abstract. The study was devoted to a comprehensive analysis of the integration potential of software-defined networking and blockchain technologies for ensuring network security in the context of the evolution of cyber threats. The research methodology was based on a systematic approach using 46 scientific sources published during 2020-2024, and included a critical analysis of architectural solutions, comparison of technological characteristics, and assessment of integration capabilities. The results of the study revealed the unique potential of synergy between software-defined networking and blockchain, which provides an increase in cybersecurity through decentralisation of management, cryptographic protection and immutability of network transactions. It was established that the integration of technologies allows implementing fundamentally new security mechanisms, in particular, automation of security policies through smart contracts, dynamic access control based on blockchain, and increasing the resiliency of information systems. Key architectural solutions that provide multi-level network infrastructure protection were identified: decentralised storage of security policies, secure event log management, and automation of routing through smart contracts. The effectiveness of implementing the Zero Trust concept using blockchain technologies was proved, which creates a fundamentally new approach to the cybersecurity of corporate networks. Architectural solutions demonstrated high efficiency in protecting network infrastructure, especially in IoT environments, telecommunications, and corporate networks. The scientific originality of the study consisted in the substantiation of the conceptual model of software-defined networking and blockchain integration, which significantly exceeds the capabilities of conventional approaches to network security. The results of the study and the formulated recommendations for the deployment of integrative technological solutions within critical information infrastructures can be effectively applied to the design of secure network architectures. They also establish a theoretical basis for subsequent applied research in the domains of cybersecurity and network engineering

Keywords: network infrastructure; cybersecurity; distributed systems; smart contracts; information and communication technologies

Introduction

The ongoing development of information and communication technologies is characterised by a continuous complication of network architectures and mechanisms for ensuring cybersecurity. Fundamental transformations in the field of network technologies, in particular, the introduction of software-defined networking (SDN) and

Suggested Citation:
Pidpalyi, O., & Romanov, O. (2025). SDN and blockchain integration: Overview of the current state and prospects for ensuring network security. *Information Technologies and Computer Engineering*, 22(2), 20-34. doi: 10.31649/vitce/2.2025.20

*Corresponding author

blockchain technologies, are conditioned by the critical need to solve systemic information security problems in the face of constantly evolving cyber threats.

Research on the architectural features of SDN demonstrates its revolutionary potential in rebuilding conventional network infrastructures. T. Alharbi (2020) analysed in detail the evolution of SDN, highlighting its ability to centrally manage network flows through a clear separation of the control, infrastructure, and application planes. H.N. Nguyen *et al.* (2021) further highlighted the unique advantages of SDN in dynamically configuring network policies, in particular, the ability to instantly adapt to variable security and load requirements. The main architectural features of SDN include: first, abstraction of network infrastructure through software interfaces; second, centralised management of network resources; and third, dynamic routing and configuration of network devices. S. Sharma & A. Nag (2023) emphasised that this approach allows network operators to manage network resources more flexibly and efficiently compared to conventional static architectures.

Simultaneously, studies of blockchain technologies have revealed their unique potential in ensuring information security. S.W. Turner *et al.* (2023) and L. Elhaloui *et al.* (2023) described in detail the cryptographic mechanisms of the blockchain that ensure the immutability and transparency of transaction records. They focused on the decentralised nature of the technology, which significantly complicates unauthorised access and manipulation of data. Key advantages of blockchain technologies include: cryptographic information protection, distributed consensus architecture, the impossibility of reverse interference in records, and full transparency of transactions. Y. Li *et al*. (2022) proved that these properties make blockchain a powerful tool for ensuring data integrity in distributed systems.

A comprehensive analysis of scientific sources revealed significant challenges in existing approaches to network security, including the vulnerability of conventional network architectures, especially in the IoT ecosystem. E. Barka *et al*. (2021) emphasised the need to develop integrated protection mechanisms that can dynamically adapt to new cyber threats. Prospects for such integration for creating resilient network infrastructures were outlined. S. Wadhwa *et al.* (2022) analysed the limitations of consensus mechanisms in blockchain systems, whereas S.W. Turner *et al.* (2023) focused on the problems of inter-control interaction in SDN architectures. The analysis of scientific sources convincingly demonstrates the existence of significant unresolved problems in the field of integration of SDN and blockchain technologies.

Existing research is fragmented and does not offer a holistic approach to harnessing the potential of these technologies for network security. The technical implementation of integration of SDN and blockchain technologies requires solving a complex of architectural and operational tasks. Critical aspects include optimising synchronisation mechanisms between SDN controllers and blockchain network nodes, minimising transaction validation delays, and ensuring efficient interaction between management and data planes. Special attention should be paid to the development of data transfer protocols between components of an integrated system, considering the requirements for network bandwidth and latency. Architectural solutions should provide an optimal balance between the decentralisation inherent in blockchain systems and centralised management typical of SDN. An important aspect is the development of redundancy and fault tolerance mechanisms that guarantee the stability of the integrated system in conditions of partial unavailability of network components or attempts at malicious interference.

The purpose of the study was to comprehensively analyse the architectural, security, and functional aspects of SDN integration and blockchain technologies, aimed at developing innovative approaches to ensuring network security in the face of ever-growing cyber threats. The main objectives of the study included a systematic analysis of existing approaches, identification of mechanisms for strengthening security through SDN and blockchain integration, development of a conceptual model of their interaction, and a comprehensive assessment of the effectiveness of the proposed integration solutions.

Materials and Methods

The study of the integration of SDN and blockchain technologies was conducted comprehensively using a wide range of information sources and methodological approaches. The main research material was scientific publications devoted to the architectural features of SDN and blockchain technologies, their security mechanisms, published during 2020-2024 in specialised international publications on information security, network technologies, and computer science.

The source base of the study consisted of 42 research papers selected for key search queries: “SDN and blockchain integration”, “blockchain-based SDN security”, “SDN security enhancement”, “blockchain in network security”, “smart contracts in SDN”. Sources included papers from highly rated journals indexed in Scopus and Web of Science, such as IEEE Access, Security and Communication Networks, Future Internet, Sensors, and other specialised publications. The criteria for selecting sources were the relevance of the problem, scientific originality, and relevance of research tasks.

The research methodology provided for a structured approach to the analysis of scientific sources, which included consistent identification, classification, and systematisation of research papers on the integration of SDN and blockchain technologies. The source base was structured according to the problem-thematic principle, which helped to comprehensively disclose the architectural, security and functional aspects of the technologies under study. Additional material was technical specifications and standards in the field of SDN and blockchain technologies, in particular, OpenFlow, Ethereum, Hyperledger Fabric,

which provided a deep understanding of the architectural features and mechanisms of interaction of technologies.

The methodological approach was based on a systematic study of the integration capabilities of SDN and blockchain technologies, which provided for the identification and critical analysis of key scientific concepts, comparison of various opinions, and identification of promising areas for further scientific research in the context of network security. Special attention was paid to the assessment of potential risks and limitations in the implementation of integration solutions, which allowed forming a more balanced understanding of the problem under study.

The sequence of scientific research and methodological tools of the study included critical analysis of existing architectural solutions and approaches, systematisation and comparison of technological characteristics, investigation of network security mechanisms, and evaluation of the effectiveness of integration solutions. In the course of the study, a comprehensive approach was applied to the analysis of architectural features and mechanisms of interaction of technologies, which helped to identify key factors of successful integration. The research was based on the results of experimental implementations of blockchain technologies in the SDN architecture, presented in the studies by Y. Li *et al.* (2022), S.W. Turner *et al.* (2023), L. Elhaloui *et al.* (2023). Special attention was paid to the analysis of practical implementations, in particular, the BCNBI framework, BlockCSDN, VQoSRR, and other integration solutions.

The specifics of the study necessitated the application a cross-technological approach, which helped to comprehensively assess the potential of SDN and blockchain integration from the standpoint of information security, network management, and architectural efficiency. The methodological strategy of the study also considered the interdisciplinary nature of the problem, which made it necessary to integrate approaches from different fields of knowledge: information security, network technologies, cryptography, and computer science. The application of such an integrated approach facilitated the comprehensive investigation of the problem and the development of reasonable conclusions about the prospects for integrating the technologies under study.

Results and Discussion

Overview of SDN and blockchain technologies

SDN architectural decomposition implements the principle of separation of functioning planes, which provides abstraction of network functions and programmable control over the network infrastructure. The fundamental SDN architecture consists of three functional planes: data, control, and application, each of which performs specific functions in the overall network management hierarchy. Data plane implements mechanisms for transmitting network traffic through switching equipment. According to H. Nejadnik *et al.* (2020), this plane is characterised by the absence of internal decision-making logic, functioning solely based on instructions obtained from the control plane. Switching elements of the data plane perform atomic packet processing operations in accordance with established routing rules and security policies. Control plane implements centralised network infrastructure management logic. T. Alam & M. Aljohani (2020) demonstrated that this plane provides global visibility of the network topology and dynamic configuration of network elements. Southbound interface integration creates a standardised communication protocol between the controller and data plane devices, which was confirmed by J. Sun *et al.* (2021). Application plane provides a software interface for implementing high-level network services and management functions. This plane provides an opportunity to implement specialised network applications, including monitoring systems, service quality control, and security mechanisms. The architectural abstraction of the application plane allows software management of network resources through standardised interfaces for interaction with the control plane.

Figure 1 shows a three-level SDN architecture that demonstrates the hierarchical interaction between the application plane (upper level), the control plane (middle level), and the data plane (lower level). Interaction between planes is implemented through standardised Northbound and Southbound API interfaces that provide programmable management of the network infrastructure. Each plane contains specific functional components that provide an appropriate level of abstraction and network management.

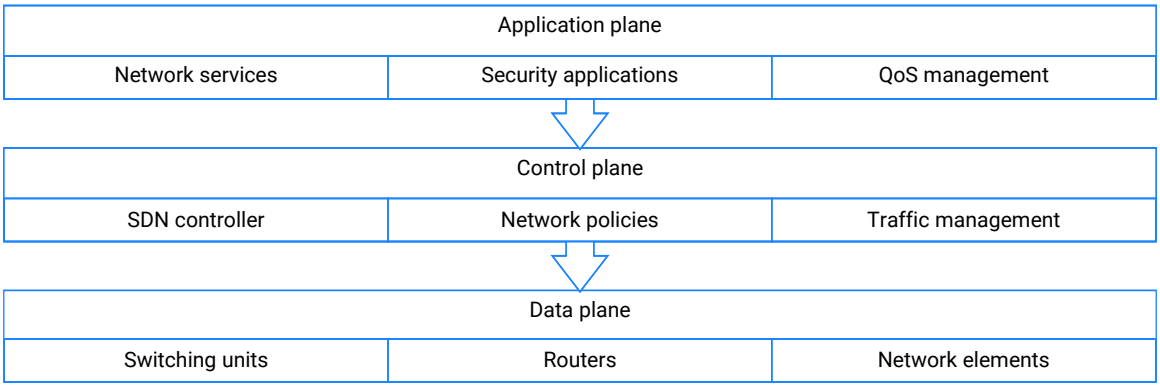

Figure 1. SDN architecture

Source: compiled by the authors

Interaction between functional planes is implemented through standardised software interfaces, which ensures modularity of the architecture and the possibility of independent development of each architectural component. This decomposition increases the flexibility of the network infrastructure and simplifies the processes of automating network resource management. Software-oriented networks represent an innovative network infrastructure management paradigm that provides significant benefits for dynamic control of network resources. The main advantages of SDN are centralised management, prompt policy configuration, and adaptive routing.

Centralised management is a fundamental characteristic of SDN, which implements global visibility of the network topology. Unlike conventional networks, where each device requires an individual configuration, SDN implements centralised control through a single controller, which optimises administration and minimises the likelihood of configuration errors (Zadkhosh *et al.*, 2020). The controller implements centralised management functions, providing prompt response to network load fluctuations and potential security threats. This architecture promotes optimal use of network resources through dynamic routing optimisation and real-time traffic management.

Quick policy configuration is provided via a programmable network resource management interface. Software abstraction allows quickly modifying routing rules and security policies, which is critical for dynamic environments with variable network infrastructure requirements. This functionality minimises response time to security incidents and optimises network adaptation to changing operating conditions, increasing overall system reliability. If anomalies in network traffic are detected, it is possible to instantly modify policies to block suspicious data flows.

Routing flexibility is provided by the architectural separation of control and data planes. This segregation allows optimising routing based on the current state of the network infrastructure. The system can dynamically adapt to changes in network load while simultaneously providing certain quality of service (QoS) parameters. When congestion occurs on certain routes, SDN automatically redirects traffic through alternative paths, which minimises latency and packet loss.

Security analysis of SDN architecture calls reveals three critical vectors of potential attacks: controller vulnerability, control plane DDoS attacks, and Southbound API compromise. A controller vulnerability poses a primary risk due to its centralised role in the SDN architecture. Compromising the controller potentially gives an attacker full control over the network infrastructure, making it possible to manipulate traffic routing and gain unauthorised access to data. The criticality of this component is conditioned by its function of centralised management of network resources and coordination of network devices.

DDoS attacks on the control plane pose a significant threat due to the possibility of disrupting the controller's functionality by exhausting computing resources. Degradation of the controller's performance leads to a decrease in the efficiency of processing requests from network devices, causing delays in data transmission or complete failure of network services. The classification of DDoS attacks includes impact vectors on data planes, controls, and the application layer, each of which requires specific security mechanisms (Samaan & Jeiad, 2023).

Attacks on the Southbound Interface API, in particular the OpenFlow protocol, pose risks due to the possibility of compromising communication between the controller and data plane devices. Potential attack scenarios include substitution of command instructions and modification of configuration parameters, which can lead to unauthorised traffic redirection. Implementing Southbound Interface API security mechanisms is critical to ensuring the integrity of network operations and data privacy.

Blockchain technology implements a distributed storage architecture based on three fundamental principles: decentralisation, record immutability, and cryptographic protection. The decentralised blockchain architecture implements distributed data storage through a network of nodes, each of which contains a complete copy of the transaction register. According to V. Vakulenko & D. Smetan (2024), the lack of centralised control significantly increases the system's fault tolerance and minimises the risks of data compromise. Distributed transaction verification ensures transparency and auditability of all operations on the network. The architectural organisation of a blockchain network is shown in Figure 2, which demonstrates the structure of a sequential chain of blocks. Each block contains a hash of the previous block, which provides cryptographic binding and guarantees the integrity of historical records.

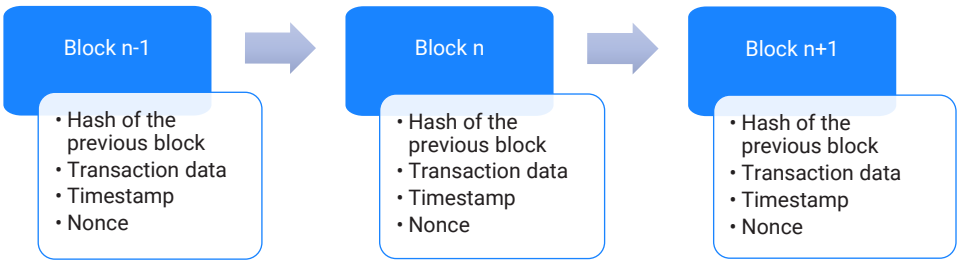

Figure 2. Block chain structure in a blockchain network

Source: compiled by the authors

The immutability principle is implemented by cryptographically linking blocks to a sequential chain, where each block contains the hash value of the previous block. According to V. Chobitok & S. Litvinchik (2024), this architecture allows modifying historical records without breaking the integrity of the entire chain and obtaining consensus among most network nodes. This property is critical for applications that require guaranteed data integrity. Cryptographic mechanisms ensure the security of the blockchain network by integrating data encryption in blocks and digital signatures to authenticate transactions. Implementing consensus mechanisms such as Proof of Work and Proof of Stake ensures network state consistency and protection against unauthorised data modifications. The integrated application of cryptographic primitives creates a solid foundation for ensuring the integrity and confidentiality of information in a distributed environment.

Blockchain technology is differentiated into two fundamental types of architectures: public and private, each of which is characterised by specific properties and functional limitations. A public blockchain implements an open network architecture with unlimited access to transaction validation and data viewing. Based on the definition by S. Al-E'mari *et al.* (2021), the key characteristics are high transparency of operations, increased resistance to attacks through a distributed architecture, and open access to network infrastructure. However, the scalability of public blockchains is limited due to the need to reach consensus between a significant number of nodes, which affects transaction latency and overall system performance (Li *et al.*, 2022). A private blockchain implements a closed architecture with controlled access of participants. This model provides optimised performance due to the limited number of validation nodes and an increased level of data privacy. However, centralising access control creates potential vulnerabilities due to the concentration of management in a limited group of participants. A comparative analysis of architectures demonstrates a trade-off between decentralisation and performance: public blockchains provide maximum transparency and resilience to manipulation, while private blockchains optimise performance and privacy through partial centralisation of control.

Smart contracts implement software logic on the blockchain platform to automatically fulfil contractual obligations when certain conditions occur. The principle of their operation is based on deterministic algorithms and immutability of programme code after deployment on the network. Figure 3 shows the main stages of the smart contract lifecycle: from initial deployment through condition verification to performing operations and updating the state in the blockchain. The cyclical nature of the process demonstrates constant verification of conditions and automatic execution of operations when they occur.

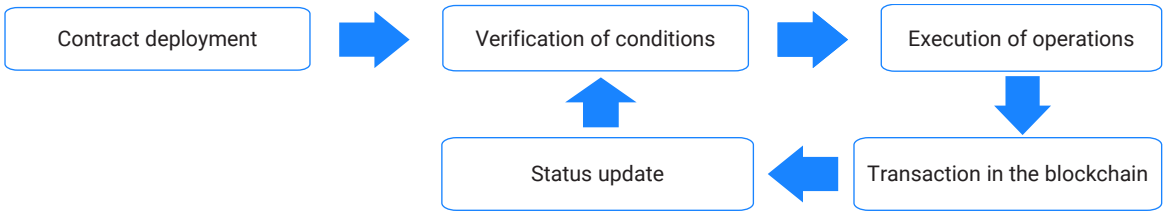

Figure 3. Smart contract lifecycle structure

Source: compiled by the authors

The functionality of smart contracts is implemented through automated execution of pre-programmed conditions. The process involves verifying trigger conditions, performing appropriate operations, and recording the results in the blockchain. Such automation minimises the need to involve intermediaries and reduces the risks associated with the human factor. The security mechanisms of smart contracts are based on cryptographic primitives and properties of the blockchain platform. Implementation on platforms such as Ethereum ensures code immutability and protection against unauthorised interference. The decentralised nature of contract execution increases resistance to manipulation and fraud.

The analysis of scientific research in the field of integration of SDN and blockchain technologies demonstrates several key areas of development. Current research focuses on architectural solutions, security mechanisms, and specific applications in the context of IoT systems. Figure 4 shows the main areas of research, including the development of architectural solutions, security mechanisms, and specific applications in IoT systems, reflecting the complex nature of SDN integration and blockchain technologies.

Figure 4. Areas of research on SDN integration and blockchain

Source: compiled by the authors

Fundamental research on SDN and blockchain integration architectures focuses on developing effective mechanisms for component interaction. L. Elhaloui *et al.* (2023) explored the potential of integration for IoT systems, focusing on optimising the security and performance of network infrastructure. W. Li *et al.* (2020) and R. Kovacs *et al.* (2024) proposed architectural solutions for scalable networks, focusing on validating network functions and optimising performance. S. Nithyaselvakumari *et al.* (2023) focused on mechanisms to improve security through blockchain integration into SDN, offering new architectural solutions for mobile networks.

The implementation of blockchain technology in the SDN architecture implements three key security mechanisms: decentralised storage of security policies, secure management of event logs, and automation of routing through smart contracts, which is schematically shown in Figure 5, which reflects the hierarchical structure of security mechanisms and their functional relationships.

Decentralised storage of security policies, investigated by H.N. Nguyen *et al.* (2021), ensured immutability and verifiability of network configurations. The distributed blockchain architecture minimises the risks associated with centralised management of SDN controllers, which is demonstrated at the top of the diagram through the connection between the "Blockchain" and "Security policies" blocks. Secure event log management presented in the paper by E. Barka *et al.* (2021), implements mechanisms for auditing and verifying network operations, which is reflected in the central part of Figure 5 through the "Event logs" components. The blockchain ensures immutability of historical records and prevents unauthorised modification of event logs.

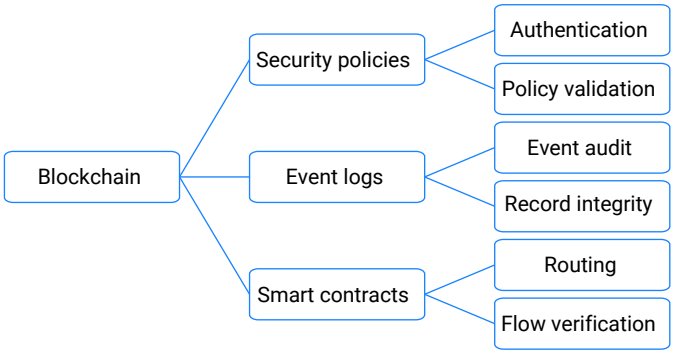

Figure 5. Blockchain-based security mechanisms in SDN

Source: compiled by the authors

The study by A. Derhab *et al.* (2021) demonstrated the effectiveness of smart contracts for automating routing in SDN, which is shown at the bottom of the diagram through smart contract nodes and their relationships with routing components. Blockchain validation of network stream updates increases the reliability and security of routing. J. Hu *et al.* (2021) proposed an edge computing architecture with an integrated blockchain for verifying data flows in IoT networks running SDN, which corresponds to the complex interaction of all components presented in the diagram and optimises security at the switching level.

The implementation of blockchain technology in software-oriented networks demonstrates practical implementation through a number of technical solutions and architectural approaches, which is confirmed by implemented projects in various application domains. The BCNBI framework implements a comprehensive mechanism for protecting the northern interface in the SDN architecture through the implementation of a multi-level transaction verification system between the controller and network applications. The solution provides decentralised verification of requests to the controller, cryptographic verification of the identity of network applications, and an immutable transaction register for network operations audit (Algarni *et al.*, 2022).

The blockCSDN collective intrusion detection system implements a distributed mechanism for exchanging threat data through synchronisation of information between network nodes. The system architecture implements a consensus mechanism for verifying new threats and decentralised storage of attack signatures, which significantly increases the effectiveness of intrusion detection (Li *et al.*, 2022). The practical implementation of smart contracts for routing automation demonstrates efficiency through automatic validation of routing rules and programmable logic for optimising network flows. Network status verification mechanisms via the blockchain ensure the reliability and security of routing.

The VQoSRR model implements an integrated approach to service quality management through dynamic adaptation of QoS parameters and blockchain validation of service quality policies. Automated resource management optimises the transmission of video content over the network. According to research W. Guo (2023), expanding the scope of SDN and blockchain integration to supply chain management demonstrates the versatility of the approach by automating compliance verification and controlling logistics operations using smart contracts. The combination of technical solutions presented confirms the practical viability and effectiveness of integrating

SDN and blockchain technologies in various application areas, demonstrating the potential for further development and implementation.

Analysis of the benefits of SDN and blockchain integration

Blockchain technology provides multi-level data protection in the SDN management plane through the implementation of cryptographic mechanisms and decentralised information storage. Architectural integration of the blockchain into SDN implements the mechanism of immutability of records through cryptographic binding of blocks, where modifying data in one block requires recalculating the hash values of all subsequent blocks. This structure guarantees the integrity of security policies and routing rules in the SDN infrastructure. Blockchain cryptographic mechanisms implement a digital signature system for authenticating transactions and verifying access to network resources. Research confirms the effectiveness of blockchain authentication for protecting network information exchange in the SDN architecture.

Blockchain implementation for event log management provides verification of data flows at the edge switch level, which optimises real-time anomaly detection. The distribution architecture increases the transparency of network operations and the effectiveness of security monitoring (Sinha *et al.*, 2024). Automation of routing management is implemented through smart contracts that provide programmable validation and execution of routing policies. According to Z. Zeng *et al.* (2022), this integration increases the efficiency of traffic management and minimises the risks of unauthorised route modification. Smart contracts implement an automated mechanism for managing access policies in the SDN architecture, which is schematically shown in Figure 6, which illustrates the interaction of access control system components.

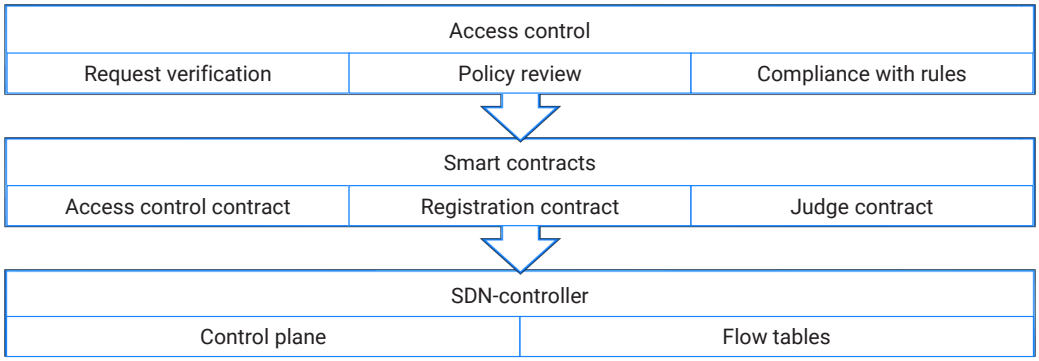

Figure 6. Smart contract-based access control architecture in SDN
Source: compiled by the authors

The FACSC fine access control method implements multi-level verification using an attribute control model. The system implements the following functional components: an attribute verification module, an access policy validator, and a dynamic rule update mechanism. Smart contract integration provides automatic request validation and policy modification in real time.

The SC-CAAC scheme extends functionality by implementing context-sensitive verification mechanisms. The architecture combines context analysers that evaluate user parameters, time characteristics, and environment specifications. Smart contracts automate the decision-making process based on multivariate contextual data analysis. The integrated access control system implements three types of smart contracts, which is reflected in the central part of Figure 6: the access control contract (ACC) validates requests, the registration contract (RC) manages accounts, and the judge contract (JC) provides system monitoring. This architecture optimises authentication and abnormal behaviour detection processes (Alotaibi *et al.*, 2022; Nandiyanto *et al.*, 2023; Merlec & In, 2024).

Integrated security architecture proposed by J. He & C. Li (2022) integrates dynamic policy management through programmable smart contracts with the SDN controller system, providing flexible reconfiguration of network policies. Automation principles demonstrate effectiveness in various application areas, including financial transactions and contract management. The implementation of blockchain technology in event logging systems implements complex mechanisms for immutable storage and cryptographic verification of data through a distributed architecture that provides a high level of security and transparency.

Cryptographic verification and journal immutability provided by blockchain demonstrates critical importance for protecting sensitive data in healthcare and genomic research. Blockchain mechanisms guarantee the confidentiality and integrity of information through a distributed transaction register, which eliminates unauthorised data modification. The implementation of these mechanisms optimises the processes of auditing and controlling access to sensitive information (Gürsoy *et al.*, 2020).

Blockchain integration with IPFS implements an optimised storage architecture that provides scalability and efficient search through the implementation of smart contracts. The distribution architecture increases data availability while maintaining its security, and integration

with IPFS optimises the management of large amounts of data. Research by P. Patel & H. Patel (2023) confirmed the effectiveness of such a hybrid architecture for cryptographic storage, providing an optimal balance between performance and security.

Systematic analysis of process mining demonstrated the potential of the blockchain to optimise operational processes through data tracking and analysis mechanisms. The implementation of these mechanisms allows organisations to improve the efficiency of business processes through transparent tracking and verification of operations. A distributed logging system provides protection against tampering while maintaining high performance in scalable systems (Shekhtman & Waisbard, 2021; M'Baba *et al.*, 2022).

The technological evolution of blockchain and IPFS opens up prospects for the development of advanced encryption algorithms and optimisation of consensus mechanisms. Integration of new cryptographic primitives and improved consensus protocols improves the efficiency of event logging systems. Research in this area focuses on developing standardised approaches to implementing blockchain systems that meet modern information security and scalability requirements.

Implementation of smart contracts for automated implementation of routing rules and security policies implements programmable control mechanisms in distribution systems. The smart contract architecture provides automatic fulfilment of conditions when verifying certain triggers, minimising dependence on the human factor in critical security processes. The functionality of smart contracts in the context of security is implemented through automated mechanisms for controlling access and verifying user rights. Integration with blockchain platforms ensures the immutability and transparency of contract fulfilment, which increases the overall level of system security. The technical implementation of smart contracts on the Ethereum platform implements cryptographic security mechanisms and consensus protocols for verifying transactions. The system architecture makes it impossible to modify contracts without reaching network consensus, which guarantees the integrity of security policies.

The development of smart contracts requires the implementation of secure software patterns and compliance with security standards to minimise potential vulnerabilities. Integrating best development practices is critical to ensuring the reliability and security of automated access control systems. Integration of blockchain technology into access and security policy management systems implements automation of administrative processes through a distribution architecture and an immutable transaction register. For example, the PyRos system implements state channels for automated access control in public blockchain networks, optimising performance by reducing manual operations. The system architecture provides access verification and real-time transaction monitoring.

The distribution registry minimises information asymmetry by automatically documenting transactions and verifying access. The implementation of smart contracts automates verification and control processes, reducing dependence on manual administration. Software-oriented networks integrate the blockchain for automatic monitoring of network activity and access control. Decentralised applications implement programmable resource management mechanisms through consensus protocols and cryptographic primitives. Technological integration optimises operational efficiency by automating access control and reducing manual processes while maintaining a high level of system security and transparency.

The analysis of current research demonstrated a wide range of smart contract implementations for automating the security of information systems. There is a systematic integration of blockchain technologies into access control and security verification mechanisms. The significant potential of this technology for optimising security management processes can be stated. Fundamental research by D.V. Lubko & M.Yu. Miroshnichenko (2024) in the field of information security confirmed the effectiveness of using security classes to develop automated policies based on smart contracts. The proposed approach provides formalisation of audit processes and measurement of the effectiveness of security mechanisms through automated verification protocols. Significant progress is being made in the field of smart cities, where the implementation of blockchain technologies provides an increased level of security through automated transaction tracking and access verification (Palka, 2023). Automation of access control to critical infrastructure elements, including monitoring and resource management systems, is of practical importance.

Special attention should be paid to the use of smart contracts in e-government systems. Research S. Vasylyshyn & I. Origskuu (2022) demonstrated the effectiveness of automating verification processes for access to confidential data through the implementation of cryptographic mechanisms and consensus protocols. International research H. Jamshed *et al.* (2022) focused on analysing smart contract vulnerabilities and developing automated security verification methods. The relevance of developing formal validation methods and secure programming environments were confirmed by the growing number of smart contract implementations in critical systems. The integration of machine learning methods to optimise verification processes demonstrates promising results (Ali & Chen, 2023). Further development of the technology involves improving the tools for automated security testing of smart contracts and implementing standardised development protocols. A critical factor remains the need for a balance between automating security processes and ensuring the reliability of verification mechanisms. Optimising the performance of automated security systems requires developing robust validation methods and improving verification protocols.

Micro-segmentation and dynamic authentication mechanisms implement a comprehensive approach to protecting network infrastructure from internal threats through the implementation of isolated segments and

context-sensitive access verification. Micro-segmentation implements a security architecture by creating isolated network zones with differentiated access policies. The technology minimises the area of potential attack by limiting lateral movement between segments. Functional implementation includes virtualisation of network components and implementation of controlled access points. Dynamic authentication implements multi-factor user verification based on contextual parameters, including geolocation, time characteristics, and behavioural patterns. The system provides continuous verification of access rights by integrating multiple authentication factors and mechanisms for detecting abnormal activity. Integrating micro-segmentation with dynamic authentication forms a multi-level security architecture. Each network segment implements specific authentication mechanisms optimised for specific security requirements. The system provides automated detection and blocking of suspicious activity by analysing deviations from established access patterns.

The architectural solution demonstrated high efficiency in countering internal threats through a combination of network space segmentation and dynamic access control. The technology optimises the processes of detecting and neutralising potential attacks while maintaining the operational efficiency of the network infrastructure. Integration of blockchain technology into the Zero Trust model implements an improved security mechanism through the implementation of the principles of zero trust and distributed verification. The architectural solution provides an increased level of protection against internal threats through permanent access validation. The distributive nature of the blockchain optimises authentication and access control processes by implementing multi-factor verification in an immutable registry. The technology provides context-sensitive validation of users, considering behavioural patterns and access specifics.

The blockchain-based Zero Trust model solves scalability and adaptability problems through a decentralised data storage and verification architecture. The system provides transparency and traceability of transactions, optimising the detection of anomalies and potential threats. Dynamic authentication within the blockchain infrastructure implements the "never trust, always verify" principle through continuous access validation. The architecture supports adaptive security policies optimised for the specific requirements of various industry applications. The immutability and transparency of the blockchain registry ensure effective audit and monitoring of network activity. The implementation of zero-trust policies in the blockchain provides a solid foundation for detecting and preventing internal threats through continuous analysis of user behaviour.

Problems and limitations of SDN and blockchain integration

The issue of scalability of blockchain technologies is determined by bandwidth limitations and increased requirements for computing resources when processing transactions in large networks. Transaction confirmation delays occur due to architectural limitations of consensus mechanisms and block size. In the Bitcoin network, latency is caused by the time it takes to form blocks, while in Ethereum, additional delays are caused by the computational complexity of executing smart contracts. Integration of smart contracts significantly affects network bandwidth due to the need for parallel execution of programme code on all nodes. Increased consumption of computing resources during mass user interaction with smart contracts leads to an increase in latency and an increase in the cost of transactions.

Scalability optimisation is implemented through the introduction of second-level technologies and modification of consensus mechanisms. Lightning Network and Optimistic Rollups provide processing of transactions outside the main chain, reducing network load. Migrating from Proof of Work to Proof of Stake demonstrates the potential to increase throughput by optimising the transaction validation process. Further development of scalable solutions requires a comprehensive approach to optimising the blockchain network architecture, including improving consensus protocols and sharding mechanisms for parallel transaction processing.

The introduction of blockchain technology in software-oriented networks has a significant impact on system performance, especially on data processing speed and flow management. SDN provides centralised network management, which increases the flexibility and speed of configuring network resources. However, as noted by T. Alharbi (2020), the centralised SDN architecture can become a bottleneck under high load, which negatively affects the speed of data processing.

Blockchain integration into SDN allows distributing the load and reducing data processing delays. The blockchain provides an additional layer of security that speeds up detection and response to attacks such as DDoS. This allows the system to filter malicious traffic faster and focus on legitimate requests, improving the overall data processing speed.

In addition, the implementation of blockchain optimises flow management in SDN. H.N. Nguyen *et al.* (2021) noted that the distribution of authentication methods through the blockchain increases the security and speed of information processing, reducing delays associated with verification of access rights. The blockchain also allows implementing policy-oriented forwarding control in multi-domain SDN networks, automating routing based on predefined policies. This significantly improves data processing speed and flow management efficiency.

Comparing SDN performance before and after blockchain implementation shows a significant improvement in data processing speed and flow management efficiency. Blockchain solves the problems of a centralised SDN architecture by providing load distribution, speeding up attack detection and response, optimising authentication and routing, and improving the security and sustainability of the system as a whole. These advantages make blockchain

integration into SDN a promising area for further development and improvement of software-oriented networks.

The introduction of private blockchain solutions and hybrid approaches is a promising area for solving the problem of delays in processing transactions in blockchain networks. Private blockchains, by restricting access to the network, reduce the number of participants required to verify transactions, and allow for more efficient consensus mechanisms such as Practical Byzantine Fault Tolerance (PBFT), which reduces latency compared to conventional algorithms such as Proof of Work. Hybrid blockchain solutions, combining elements of public and private blockchains, provide an optimal balance between security and performance. The use of sharding in hybrid blockchains helps to distribute the load between network segments and process transactions in parallel, increasing system throughput.

The integration of artificial intelligence (AI) into blockchain technologies allows automating transaction confirmation processes and adapting real-time security parameters, reducing delays and improving the system's response to changes in workload and threats. Implementing more efficient consensus algorithms, such as hybrid algorithms, Directed Acyclic Graph (DAG), or Lightning Network, provides a balance between security, scalability, and processing speed, helping to process thousands of transactions per second and significantly reducing latency. The use of protocol or wallet-level load balancing methods in sharded blockchains contributes to an even distribution of the load between network participants, reducing transaction processing delays.

To maximise the performance optimisation of blockchain systems, it is also necessary to consider additional factors and implement comprehensive solutions. The use of off-chain transaction processing technologies, such as state channels or plasma, reduces the burden on the underlying blockchain network by conducting most off-chain transactions while maintaining data security and integrity. Optimising the architecture of blockchain networks, in particular, the topology and protocols of communication between nodes, improves the efficiency of information dissemination and reduces delays. The use of hardware accelerators, such as GPUs or specialised integrated circuits (ASIC), increases transaction processing speed and reduces latency by optimising critical operations. Implementing standardised interaction protocols and data formats in the blockchain ecosystem simplifies the integration of various blockchain platforms and applications, reducing the overhead of data matching and transformation between systems.

Thus, an integrated approach that combines the integration of private and hybrid blockchain solutions, the use of AI, efficient consensus algorithms, load balancing methods, off-chain technologies, network architecture optimisation, hardware acceleration and protocol standardisation can effectively solve the problem of delays in blockchain networks and ensure high performance and scalability of blockchain systems. The security of smart contracts is a critical aspect in the context of blockchain technologies. Smart contracts, being self-contained and immutable software artefacts, require careful design and implementation to avoid potential vulnerabilities. Errors in the smart contract code can lead to unpredictable behaviour, loss of funds, or exploitation by attackers. One of the main problems is the complexity of smart contract programming languages such as Solidity, which increases the likelihood of development errors. The lack of standardised secure coding practices and limited testing capabilities make it difficult to identify and address vulnerabilities before deploying contracts on the blockchain network. In addition, smart contracts are vulnerable to transaction-level attacks. Attackers can manipulate the order or timing of transactions to exploit flaws in contract logic. Examples of such attacks include re-entrance attacks, where a malicious contract recursively calls victim functions, or front-running attacks, where the attacker uses information about future transactions to gain an advantage.

To solve these problems, it is necessary to implement comprehensive security measures. This includes carefully designing the smart contract architecture, using proven design patterns and libraries, and conducting comprehensive code audits and testing. The use of formal verification methods can help to guarantee the correctness and security of smart contracts mathematically. It is also important to develop and comply with standards for secure coding of smart contracts, ensure proper key management, and implement mechanisms for emergency suspension or renewal of contracts in case of critical vulnerabilities.

Ensuring the security of smart contracts requires a comprehensive approach that combines careful design, regular code audits, testing, and compliance with secure programming standards. Smart contract security audits are conducted by independent cybersecurity experts who conduct a thorough analysis and verification of contract code for potential vulnerabilities and flaws. Audit includes static code analysis, dynamic testing, verification of contract logic, and evaluation of potential attack vectors. The audit results allow identifying and eliminating critical vulnerabilities before deploying a smart contract in a blockchain network.

The use of security standards in the development of smart contracts is a key factor in minimising risks. Standards such as OpenZeppelin offer proven design patterns, libraries, and recommendations for secure programming in Solidity. Compliance with these standards avoids common errors and vulnerabilities, such as integer overflow, incorrect access control, or lack of input validation. Security standards also define best practices for key management, exception handling, and providing emergency mechanisms in case critical errors are detected in smart contracts.

Regular security audits and compliance with secure programming standards are essential conditions for ensuring the reliability and integrity of smart contracts. These measures allow minimising the risks of exploiting vulnerabilities by intruders and ensuring the correct operation of smart contracts in the blockchain environment.

Integrating blockchain technology into large-scale infrastructures, such as corporate or telecommunications networks, is a complex and potentially costly process. However, the potential benefits, including increased security, transparency, and efficiency, have prompted many organisations to consider implementing blockchain. A comprehensive assessment of the costs and benefits associated with implementing blockchain solutions is crucial for making informed decisions.

Implementation costs vary depending on factors such as the architecture chosen, data volume, and industry requirements. Organisations should consider both one-time and fixed costs, including development, testing, integration, and maintenance. The involvement of external developers may be necessary if internal resources do not have experience with the blockchain. Significant investments in new infrastructure, such as hardware and software upgrades, may be required to support the technology, especially for large enterprises with existing complex data management systems.

Despite the high initial costs, implementing a blockchain can bring significant benefits. Increased transparency and data security can reduce fraud risks and reduce audit and control costs, as the blockchain provides an immutable record of all transactions. Improving the efficiency of data management allows organisations to respond faster to market changes and reduce information processing costs, which is especially important in telecommunications networks, where data processing speed is extremely important.

Hybrid blockchain solutions that combine public and private blockchains can reduce implementation costs by providing flexibility and scalability, enabling organisations to adapt their systems to changing environments and use available resources. Maintenance costs are another important factor. Blockchain systems need constant monitoring and updates to ensure security and efficiency, including staff training, software updates, and risk management. To further optimise the cost-benefit ratio, organisations can explore the following strategies: collaborative development, step-by-step implementation, standardisation, automation, and scalability planning.

Thus, while the costs of implementing blockchain technology in large-scale infrastructures can be significant, the potential benefits in terms of increased security, transparency, and efficiency may substantiate the investment. Careful cost-benefit assessment combined with strategic approaches to optimising the cost-benefit ratio is important for organisations planning to implement blockchain. As technology evolves and best practices emerge, implementation costs are likely to decrease, making blockchain integration more accessible and cost-effective for a wider range of organisations. The combination of software-configurable network and blockchain technologies creates significant technical challenges for configuring and maintaining integrated systems. Effective implementation and management of such complex infrastructures requires a high level of qualification and specialised knowledge of personnel.

The technical complexity of configuring SDN and blockchain integration is conditioned by the need to ensure compatibility between different protocols, interfaces, and architectures. Configuring network policies, routing rules, and consensus mechanisms for optimal interaction between SDN controllers and blockchain nodes requires a deep understanding of both technologies. In addition, ensuring data security, confidentiality, and integrity in such a hybrid environment is a non-trivial task that requires careful design and implementation of cryptographic protocols and access control mechanisms.

Support for integrated SDN and blockchain systems is also associated with significant challenges. Performance monitoring, anomaly detection, and troubleshooting in a distributed environment require the use of specialised tools and techniques. Updating and scaling such systems should be performed with minimal impact on network availability and uptime. In addition, the constant evolution of SDN and blockchain technologies requires regular updating of personnel knowledge and skills to effectively manage and adapt to new functionality and standards.

Managing Integrated SDN and blockchain systems requires interdisciplinary expertise covering network technologies, distributed systems, cryptography, and information security. Employees must have a deep knowledge of the SDN architecture and operating principles, and an understanding of the consensus mechanisms, smart contracts, and cryptographic primitives underlying blockchain technologies. The ability to effectively integrate this knowledge and apply it to solve complex technical problems is a key requirement for specialists in this field.

Given the high requirements for staff qualifications, organisations need to invest in talent training and development to successfully implement and manage Integrated SDN and blockchain systems. This may include internal training programmes, collaboration with academic institutions, and participation in professional communities to share knowledge and best practices. In addition, the involvement of external experts and consultants can provide valuable support in solving complex technical problems and optimising management processes.

Development prospects and possible areas for further research

One of the promising areas of development of the identified approaches is the development of private blockchain solutions for scalable networks, which are conditioned by the dynamic transformations of the technological landscape of corporate and telecommunications infrastructures. Modern blockchain technologies demonstrate the potential to optimise processes by increasing security, reducing latency, and providing controlled access to distributed systems. Private blockchain platforms, in particular, Hyperledger Fabric, represent an innovative approach to building corporate networks with a clearly regulated mechanism for verifying participants. The selective access property allows minimising the risks of

unauthorised interference and ensuring high performance of transactional operations.

Hybrid blockchain architectures demonstrate the unique ability to integrate the benefits of public and private networks, which creates additional opportunities for adaptive customisation of corporate ecosystems. This approach allows for a differentiated level of transparency and control, depending on the specifics of business processes. Leading technology solutions such as Hyperledger Fabric, Corda, and Quorum are expanding the corporate communications paradigm by implementing decentralised authentication and verification mechanisms. Of particular importance is the potential of such platforms in the telecommunications sector, where the security parameters and speed of information exchange are critical.

The strategic advantages of private blockchain solutions are the ability to implement specialised consensus algorithms, such as Practical Byzantine Fault Tolerance, which significantly optimises the speed of transaction confirmation compared to conventional consensus mechanisms. The technology creates prerequisites for the development of a trust environment within corporate and inter-corporate communication spaces (Jamshed *et al.*, 2022). Prospects for further development are related to improving the mechanisms of identification, access control, and ensuring a high level of cybersecurity in distributed corporate networks. Blockchain technologies can transform approaches to risk management, optimisation of financial transactions, and inter-organisational interaction. The integration of machine learning, artificial intelligence and blockchain technologies with software-oriented networks is causing vigorous discussions in the scientific community. Although M. Aslam *et al*. (2022) emphasised the significant potential of such synergies for automating security processes, their conclusions were based mainly on theoretical modelling. In the context of detecting anomalies, R. Jmal *et al.* (2023) advocated the sufficiency of blockchain data to effectively detect malicious activity, whereas S.K. Sinha *et al.* (2024) argued for the need for an integrated approach that combines blockchain data with conventional monitoring methods.

Practical implementations also show mixed results. The study by R. Kovacs *et al. (*2024) represented the successful implementation of automation in large networks, but M.M. Merlec & H.P. In (2024) found significant limitations in the scalability of such solutions. There is a particularly heated debate about the role of artificial intelligence in blockchain systems – S.W. Turner *et al.* (2023) made reasonable reservations about the potential risks of fully automating decision-making, whereas P.A.D.S.N. Wijesekara & S. Gunawardena (2023) insists on the need for maximum automation to counter modern cyber threats. In the light of these discussions, the integration of the Zero Trust concept into the SDN network architecture using blockchain technologies, which represents an innovative approach to ensuring cybersecurity in distributed corporate environments, is particularly relevant. The fundamental Zero Trust paradigm is based on the principle of "trust no one by default", which provides for continuous authentication, authorisation, and verification of each network request, regardless of its origin. Blockchain mechanisms add a fundamentally new level of security to the Zero Trust architecture due to the immutability and distributed nature of network event logging. Each network transaction or access request can be documented in a distributed ledger with cryptographic protection, which prevents tampering or unauthorised interference.

The SDN architecture with integrated blockchain provides dynamic and granular management of network security policies. The smart contract mechanism allows automating the processes of identification, determining access levels, and instant response to potential threats in real time. The cryptographic mechanisms of the blockchain create an additional barrier to internal and external cyber threats, as each network node undergoes multi-level authentication using decentralised identifiers. This makes unauthorised access impossible even if individual network components are compromised.

Integration is particularly effective due to the immutability property of the blockchain registry, which ensures complete auditability and traceability of all network interactions. Each network request is recorded in a distributed database with a unique cryptographic signature, which creates a reliable monitoring mechanism. The architectural approach involves creating a multi-level security system, where each network node is considered potentially unreliable. Blockchain mechanisms allow implementing contextual and behavioural analytics that dynamically adapt security policies depending on detected network anomalies. The integration of Zero Trust with blockchain technologies in the SDN architecture represents a promising area in the evolution of cybersecurity systems, providing proactive protection of corporate information infrastructures from complex and dynamic cyber threats.

Conclusions

The study revealed the comprehensive potential of integrating software-defined networking and blockchain technologies in the context of network security. This study demonstrated significant progress in developing innovative approaches to protecting network infrastructure through a combination of the capabilities of both technologies. This study examines a conceptual model for integrating SDN and blockchain, which has provided an increased level of cybersecurity through decentralised management, cryptographic protection, and immutability of network transactions. It identifies architectural solutions for multi-level protection of network infrastructure, including decentralised storage of security policies, secure event log management, and routing automation using smart contracts; the effectiveness of implementing the Zero Trust concept using blockchain technologies has been substantiated. The proposed architectural solutions theoretically substantiated the possibilities of increasing the level of protection

of network infrastructure, especially in IoT environments, telecommunications, and corporate networks. The analysis showed that such solutions can potentially minimise the risks of unauthorised access, ensure transparency of network operations and improve the efficiency of network resource management, but this requires practical verification. The results of the study showed that the proposed architectural solutions provide an increase in the resiliency of information systems in various application environments. In particular, there was a significant improvement in protection in IoT environments, telecommunications networks, and corporate infrastructures by minimising the risks of unauthorised access, ensuring transparency of network operations, and improving the efficiency of network resource management.

The main limitations of the study were the theoretical nature of the developed model and the lack of full-scale testing under real loads. Further research is needed to detail the specification of industry implementations and evaluate the cost-effectiveness of implementation. Promising areas of research are in-depth integration of artificial intelligence and machine learning with SDN and blockchain technologies, development of improved consensus mechanisms, optimisation of security protocols, and creation of standardised approaches to the implementation of hybrid blockchain architectures. Further research should be aimed at overcoming the identified limitations and expanding the potential of integration solutions in the field of network security.

Acknowledgements
None.

Funding
The study was not funded.

Conflict of Interest
None.

References
[1] Alam, T., & Aljohani, M. (2020). Software defined networks: Review and architecture. *IAIC Transactions on Sustainable Digital Innovation,* 1(2), 143-151. doi: 10.34306/itsdi.v1i2.114.

[2] Al-E'mari, S., Anbar, M., Sanjalawe, Y., Manickam, S., & Hasbullah, I. (2021). Intrusion detection systems using blockchain technology: A review, issues and challenges. *Computer Systems Science and Engineering*, 40(1), 87-112. doi: 10.32604/csse.2022.017941.

[3] Algarni, S., Eassa, F., Almarhabi, K., Algarni, A., & Albeshri, A. (2022). BCNBI: A blockchain-based security framework for northbound interface in software-defined networking. *Electronics,* 11(7), article number 996. doi: 10.3390/electronics11070996.

[4] Alharbi, T. (2020). Deployment of blockchain technology in software defined networks: A survey. *IEEE Access*, 8, 9146-9156. doi: 10.1109/access.2020.2964751.

[5] Ali, G.M., & Chen, H. (2023). Power of fuzzing and machine learning in smart contract security validation. In A.J. Tallón-Ballesteros & R. Beltrán-Barba (Eds.), *Proceedings of FSDM 2023: Fuzzy systems and data mining IX* (pp. 788-796). Amsterdam: IOS Press. doi: 10.3233/faia231090.

[6] Alotaibi, R., Alassafi, M.O., Bhuiyan, M.S.I., Raju, R.S., & Ferdous, S. (2022). A reinforcement-learning-based model for resilient load balancing in hyperledger fabric. *Processes*, 10(11), article number 2390. doi: 10.3390/pr10112390.

[7] Aslam, M., Ye, D., Tariq, A., Asad, M., Hanif, M., Ndzi, D., Chelloug, S.A., Elaziz, M.A., Al-Qaness, M.A.A., & Jilani, S.F. (2022). Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for SDN-Enabled IoT. *Sensors*, 22(7), article number 2697. doi: 10.3390/s22072697.

[8] Barka, E., Dahmane, S., Kerrache, C.A., Khayat, M., & Sallabi, F. (2021). Sthm: A secured and trusted healthcare monitoring architecture using SDN and blockchain. *Electronics*, 10(15), article number 1787. doi: 10.3390/electronics10151787.

[9] Chobitok, V., & Litvinchik, S. (2024). Relevance using distributed register technologies in the development modern business systems. *Development Service Industry Management*, 2, 140-148. doi: 10.31891/dsim-2024-6(21).

[10] Derhab, A., Gabsi, M., Belaoued, M., & Cheikhrouhou, O. (2021). BMC-SDN: Blockchain-based multicontroller architecture for secure software-defined networks. *Wireless Communications and Mobile Computing*, 2021(1), article number 9984666. doi: 10.1155/2021/9984666.

[11] Elhaloui, L., Tabaa, M., Elfilali, S., & Benlahmar, E.H. (2023). Promises, challenges and opportunities of integrating SDN and blockchain with iot applications: A survey. *International Journal of Advanced Computer Science and Applications*, 14(12), 432-440. doi: 10.14569/ijacsa.2023.0141244.

[12] Guo, W. (2023). The impact of blockchain technology on integrated green supply chain management in China: A conceptual study. *Journal of Digitainability, Realism & Mastery*, 2(2), 58-65. doi: 10.56982/dream.v2i02.112.

[13] Gürsoy, G., Bjornson, R., Green, M.E., & Gerstein, M. (2020). Using blockchain to log genome dataset access: Efficient storage and query. *BMC Medical Genomics*, 13, article number 78. doi: 10.1186/s12920-020-0716-z.

[14] He, J.B., & Li, C.Q. (2022). Research on digital image intelligent recognition method for industrial internet of things production data acquisition. *Signal Processing*, 39(6), 2133-2139. doi: 10.18280/ts.390626.

[15] Hu, J., Reed, M.J., Thomos, N., AI-Naday, M.F., & Yang, K. (2021). Securing SDN-controlled iot networks through edge blockchain. *IEEE Internet of Things Journal*, 8(4), 2102-2115. doi: 10.1109/jiot.2020.3017354.
[16] Jamshed, H., Zahid, A., Hassan, R.U., Ahmad, H., & Islam, N.E. (2022). Survey on vulnerabilities in blockchain's smart contracts. *Journal of Independent Studies and Research Computing*, 20(2), 10-14. doi: 10.31645/JISRC.22.20.2.2.
[17] Jmal, R., Ghabri, W., Guesmi, R., Alshammari, B.M., Alshammari, A.S., & Alsaif, H. (2023). Distributed blockchain-SDN secure IoT system based on ann to mitigate ddos attacks. *Applied Sciences*, 13(8), article number 4953. doi: 10.3390/app13084953.
[18] Kovacs, R., Buzura, S., Iancu, B., Dadarlat, V., Peculea, A., & Cebuc, E. (2024). Practical implementation of a blockchain-enabled SDN for large-scale infrastructure networks. *Applied Sciences*, 14(5), article number 1914. doi: 10.3390/app14051914.
[19] Li, P., Guo, S., Wu, J., & Zhao, Q. (2022). Blockrev: Blockchain-enabled multi-controller rule enforcement verification in SDN. *Security and Communication Networks*, 2022(1), article number 7294638. doi: 10.1155/2022/7294638.
[20] Li, W., Meng, W., Liu, Z., & Au, M. (2020). Towards blockchain-based software-defined networking: Security challenges and solutions. *IEICE Transactions on Information and Systems*, E103.D(2), 196-203. doi: 10.1587/transinf.2019ini0002.
[21] Li, Y., Wang, G., Yang, H., Zuo, F., Yu, J., & Xia, H. (2022). Grouping-based reliable privacy preservation for blockchain-assisted data aggregation in mobile crowdsensing. *Security and Communication Networks*, 2022(1), article number 56216305. doi: 10.1155/2022/5626305.
[22] Lubko, D.V., & Miroshnichenko, M.Yu. (2024). Analysis of modern approaches and methodologies in the field of information and data protection. *Visnyk of Kherson National Technical University*, 1(88), 231-236. doi: 10.35546/kntu2078-4481.2024.1.32.
[23] M'Baba, L.M., Sellami, M., Gaaloul, W., & Nanne, M.F. (2022). Blockchain logging for process mining: A systematic review. In T.X. Bui (Ed.), *Proceedings of the 55th annual Hawaii international conference on system sciences* (pp. 6197-6206). Honolulu: HICSS Conference Office.
[24] Merlec, M.M., & In, H.P. (2024). Sc-caac: A smart-contract-based context-aware access control scheme for blockchain-enabled iot systems. *IEEE Internet of Things Journal*, 11(11), 19866-19881. doi: 10.1109/jiot.2024.3371504.
[25] Nandiyanto, A.B.D., Hamza, C., & Aziz, M. (2023). A novel framework for enhancing security in software-defined networks. *International Journal of Computer Engineering in Research Trends*, 10(11), 19-26. doi: 10.22362/ijcert/2023/v10/i11/v10i113.
[26] Nejadnik, H., Sadeghi, R., & Imani, S.M.F. (2020). Load balancing in software-defined networking using controller placement. *Research Square*. doi: 10.21203/rs.3.rs-53407/v1.
[27] Nguyen, H.N., Fowler, S., & Souihi, S. (2021). A survey of blockchain technologies applied to software-defined networking: Research challenges and solutions. *IET Wireless Sensor Systems*, 11(6), 233-247. doi: 10.1049/wss2.12031.
[28] Nithyaselvakumari, S., Saidulu, V., Sulaiman, N., & Salameh, A. (2023). Enhancing the security of software defined mobile networks (SDMN) based on blockchain technology. *International Journal of Interactive Mobile Technologies*, 17(4), 117-133. doi: 10.3991/ijim.v17i04.37807.
[29] Palka, O.V. (2023). Analysis of blockchain and IoT integrated smart city architecture. *Scientific Bulletin of UNFU,* 33(6), 94-99. doi: 10.36930/40330612.
[30] Patel, P., & Patel, H. (2023). Lchain: A secure log storage mechanism using ipfs and blockchain technology. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(5), 22-27. doi: 10.17762/ijritcc.v11i5s.6592.
[31] Samaan, S.S., & Jeiad, H.A. (2023). Feature-based real-time distributed denial of service detection in SDN using machine learning and spark. *Bulletin of Electrical Engineering and Informatics*, 12(4), 2302-2312. doi: 10.11591/beei.v12i4.4711.
[32] Sharma, S., & Nag, A. (2023). Cognitive software defined networking and network function virtualization and applications. *Future Internet*, 15(2), article number 78. doi: 10.3390/fi15020078.
[33] Shekhtman, L., & Waisbard, E. (2021). Engravechain: A blockchain-based tamper-proof distributed log system. *Future Internet*, 13(6), article number 143. doi: 10.3390/fi13060143.
[34] Sinha, S.K., Kumari, S., Kataria, A., Thangarasu, N., & Sahoo, G.S. (2024). Blockchain empowerment: Investigating integration with software-defined networks and its impact on iot privacy. *Multidisciplinary Reviews*, 6, article number e2023ss073. doi: 10.31893/multirev.2023ss073.
[35] Sun, J., Liu, F., Li, Y., Zhang, L., & Shi, D. (2021). A software-defined architecture for integrating heterogeneous space and ground networks. *Frontiers in Communications and Networks*, 2, article number 717476. doi: 10.3389/frcmn.2021.717476.
[36] Turner, S.W., Karakuş, M., Guler, E., & Uludag, S. (2023). A promising integration of SDN and blockchain for IoT networks: A survey. *IEEE Access*, 11, 29800-29822. doi: 10.1109/access.2023.3260777.
[37] Vakulenko, V., & Smetan, D. (2024). Management of production processes of agricultural enterprises using blockchain technologies in terms of food security. *Economic Bulletin of National Technical University of Ukraine "Kyiv Polytechnical Institute"*, 27, 52-56. doi: 10.20535/2307-5651.27.2023.297219.

[38] Vasylyshyn, S., & Opirskyy, I. (2022). Security development of electronic government systems based on blockchain. *Ukrainian Information Security Research Journal*, 24(2), 58-70. doi: 10.18372/2410-7840.24.16931.
[39] Wadhwa, S., Rani, S., Kavita, K., Verma, S., Shafi, J., & Woźniak, M. (2022). Energy efficient consensus approach of blockchain for iot networks with edge computing. *Sensors*, 22(10), article number 3733. doi: 10.3390/s22103733.
[40] Wijesekara, P.A.D.S.N., & Gunawardena, S. (2023). A review of blockchain technology in knowledge-defined networking, its application, benefits, and challenges. *Network*, 3(3), 343-421. doi: 10.3390/network3030017.
[41] Zadkhosh, E., Bahramgiri, H., & Sabaei, M. (2020). Toward manageable middleboxes in software-defined networking. *ETRI Journal*, 42(2), 186-195. doi: 10.4218/etrij.2018-0565.
[42] Zeng, Z., Zhang, X., & Xia, Z. (2022). Intelligent blockchain-based secure routing for multidomain SDN-Enabled IoT networks. *Wireless Communications and Mobile Computing,* 2022(1), article number 5693962. doi: 10.1155/2022/5693962.

Інтеграція SDN та blockchain: огляд поточного стану і перспектив для забезпечення мережевої безпеки

Олександр Підпалий

Аспірант
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0009-0007-6852-7959

Олександр Романов

Доктор технічних наук, професор
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0000-0002-8683-3286

Анотація. Дослідження було присвячене комплексному аналізу інтеграційного потенціалу технологій software-defined networking та блокчейн для забезпечення мережевої безпеки в умовах еволюції кіберзагроз. Методологія дослідження ґрунтувалась на системному підході з використанням 46 наукових джерел, опублікованих впродовж 2020-2024 років, та передбачала критичний аналіз архітектурних рішень, порівняння технологічних характеристик та оцінку інтеграційних можливостей. Результати дослідження розкривають унікальний потенціал синергії software-defined networking та блокчейн, що забезпечує підвищення рівня кібербезпеки через децентралізацію управління, криптографічний захист та незмінність мережевих транзакцій. Встановлено, що інтеграція технологій дозволяє реалізувати принципово нові механізми захисту, зокрема автоматизацію політик безпеки через смарт-контракти, динамічний контроль доступу на основі блокчейн та підвищення резильєнтності інформаційних систем. Було виявлено ключові архітектурні рішення, що забезпечують багаторівневий захист мережевої інфраструктури: децентралізоване зберігання політик безпеки, захищене управління журналами подій та автоматизація маршрутизації через смарт-контракти. Доведено ефективність впровадження концепції Zero Trust з використанням блокчейн-технологій, що створює принципово новий підхід до кіберзахисту корпоративних мереж. Архітектурні рішення демонструють високу ефективність у забезпеченні захисту мережевої інфраструктури, особливо в IoT-середовищах, телекомунікаційних та корпоративних мережах. Наукова новизна дослідження полягає в обґрунтуванні концептуальної моделі інтеграції software-defined networking та блокчейн, яка суттєво перевершує можливості традиційних підходів до забезпечення мережевої безпеки. Результати дослідження та розроблені рекомендації щодо впровадження інтеграційних технологічних рішень у критичні інформаційні інфраструктури можуть бути користними для проектування захищених мережевих архітектур та створюють теоретичне підґрунтя для подальших прикладних досліджень у сфері кібербезпеки та мережевих технологій

Ключові слова: мережева інфраструктура; кіберзахист; розподілені системи; смарт-контракти; інформаційно-комунікаційні технології