UDC 004.7:004.056.55
DOI: https://doi.org/ 10.17721/3041-2323.2024.433-439

Volodymyr NAKONECHNYI, DSc (Engin.), Prof.
ID: 0000-0002-0386-2162
e-mail: nvc2006@i.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Vladyslav LUTSENKO, PhD Student
ID: 0000-0002-2377-1858
e-mail: vladyslav.lutsenko99@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

BLOCKCHAIN-BASED MODELS AND METHODS FOR PROTECTING DATA AGAINST UNAUTHORIZED ACCESS

Blockchain era has received massive interest for its capacity to decorate records protection in a variety of applications, from monetary offerings to healthcare. This article explores how blockchain-primarily based totally fashions and techniques offer strong safety in opposition to unauthorized records access, leveraging decentralized architecture, cryptographic techniques, and consensus mechanisms. It examines the strengths and boundaries of numerous blockchain protection frameworks and highlights capacity regions for destiny research.

Keywords: ***blockchain, data protection, unauthorized access, decentralized architecture, cryptographic security, consensus mechanisms, permissioned blockchain, permissionless blockchain, smart contracts, decentralized identity management, data encryption, immutable ledger, cybersecurity, data privacy, access control models, scalability, regulatory compliance, interoperability, hybrid blockchain solutions.***

Background

In the virtual age, facts has end up one of the maximum precious assets, and shielding it towards unauthorized get entry to is a number one challenge for businesses throughout industries. Traditional facts safety methods, at the same time as powerful to a few extent, are an increasing number of challenged through state-of-the-art cyber threats, together with facts breaches, insider attacks, and different styles of unauthorized get entry to. As a result, there may be a developing want for modern answers which can provide more potent safety for touchy information (Nakamoto, n. d.).

Blockchain technology, to start with advanced because the spine of cryptocurrencies like Bitcoin, has emerged as a promising answer for information security. With its decentralized, immutable ledger and cryptographic foundations, blockchain can probably revolutionize the manner information is stored, accessed, and protected.

Results

Blockchain Fundamentals and Security Features. To recognize how blockchain can decorate facts protection, it's far critical to comprehend its center ideas and safety features. At its center, blockchain is a disbursed ledger that data transactions in a decentralized way throughout a community of nodes. Each transaction is grouped right into a block, that is cryptographically connected to the preceding block, growing a series of blocks or a "blockchain." This shape guarantees that facts is immutable, which means it can not be altered or deleted as soon as recorded (Zheng et al., 2017).

A key function of blockchain era is decentralization, which removes the want for a government or middleman to control the ledger. This decentralized structure distributes records throughout a couple of nodes, making it tremendously resilient to attacks.

Blockchain additionally employs consensus mechanisms to make sure settlement amongst members at the kingdom of the ledger. Consensus algorithms, consisting of Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT), save you fraudulent sports with the aid of using requiring community members to validate transactions. These mechanisms make sure that almost all of nodes have to agree at the validity of every transaction, making it extraordinarily tough for a unmarried entity to control the data (Kosba et al., 2016).

Blockchain-Based Models for Data Protection. Various blockchain-primarily based totally fashions were evolved to beautify facts safety towards unauthorized get right of entry to. One essential difference is among permissioned and permissionless blockchains. Permissionless blockchains, along with the ones used for cryptocurrencies, permit absolutely everyone to enroll in the community and take part withinside the consensus process. These blockchains provide a excessive degree of decentralization and transparency, making them appropriate for public programs in which consider amongst members is limited.

However, they'll now no longer be best for situations that require strict get right of entry to controls and privacy.

Permissioned blockchains, on the alternative hand, limitation community participation to legal entities only. This version is greater ideal to organization environments in which statistics safety and privateness are paramount. Permissioned blockchains provide a stability among decentralization and control, permitting businesses to keep strict get admission to controls at the same time as cashing in on the transparency and safety of blockchain technology (Yaga et al., n. d.).

Within those varieties of blockchains, numerous get admission to manage fashions had been proposed to defend data. One not unusual place version is Role-Based Access Control (RBAC), wherein get admission to rights are assigned primarily based totally at the person`s position inside an organization. By retaining a decentralized ledger of person roles and permissions, blockchain guarantees steady get admission to manage throughout all nodes, lowering the threat of unauthorized get admission to.

Blockchain-Based Methods for Data Protection. Blockchain era additionally permits numerous techniques to decorate facts safety in opposition to unauthorized access. One of the maximum distinguished techniques is facts encryption and garage (Xu, Weber, & Staples, n. d.). Blockchain may be incorporated with superior encryption techniques, which includes Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) encryption, to stable facts earlier than it's miles saved on-chain or off-chain. For big volumes of facts, decentralized garage answers just like the InterPlanetary File System (IPFS) may be used along with blockchain to make sure facts confidentiality and availability. In this setup, touchy facts is encrypted and saved off-chain, even as cryptographic hashes of the facts are saved on-chain, presenting a tamper-evidence reference that may be used to affirm facts integrity (Wood, n. d.).

Blockchain additionally gives sturdy auditing and tracking capabilities. The immutable nature of blockchain guarantees that every one get admission to tries and transactions are completely recorded in a tamper-evidence ledger. This audit path may be used for real-time tracking and auditing, supporting businesses come across and save you unauthorized get admission to whilst making sure compliance with regulatory requirements. The transparency and traceability of blockchain

statistics additionally facilitate responsibility and consider amongst stakeholders (Kshetri, 2017).

Case Studies and Applications. Several real-global packages reveal the effectiveness of blockchain-primarily based totally fashions and strategies in protective statistics in opposition to unauthorized access. In healthcare, for instance, blockchain is getting used to steady affected person records, hold privacy, and make sure statistics integrity. Blockchain`s immutability and decentralization make it an excellent answer for handling touchy scientific statistics, because it prevents unauthorized changes and presents a obvious audit path for regulatory compliance (Yaga et al., n. d.).

In deliver chain management, blockchain complements transparency and safety with the aid of using monitoring statistics and property throughout the deliver chain. By recording each transaction and statistics change on a decentralized ledger, blockchain reduces the hazard of fraud, counterfeiting, and unauthorized access. This functionality is specifically precious for industries inclusive of pharmaceuticals, in which the integrity of the deliver chain is essential to make certain product protection and authenticity (Zheng et al., 2017).

Challenges and Limitations. While blockchain gives several blessings for facts protection, it isn't with out its demanding situations and limitations. One tremendous subject is scalability. As blockchain networks grow, the quantity of facts saved at the blockchain increases, main to longer processing instances and better garage costs. This difficulty is mainly acute in permissionless blockchains, wherein each node need to shop a duplicate of the whole ledger. Several solutions, including sharding and off-chain transactions, had been proposed to deal with scalability, however they arrive with trade-offs in phrases of protection and complexity (Kshetri, 2017).

Another challenge is the high energy consumption associated with certain consensus mechanisms, such as Proof of Work (PoW). PoW requires participants to solve complex mathematical puzzles to validate transactions, which consumes significant computational resources. Alternative consensus mechanisms, such as Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT), are being explored to reduce energy consumption, but they may have their own security vulnerabilities and limitations (Christidis, & Devetsikiotis, 2016).

Interoperability is every other issue, as integrating blockchain with present structures and requirements may be complex. Many companies

have legacy structures that might not be like minded with blockchain technology, requiring sizable funding in integration and migration efforts. Additionally, the shortage of standardized protocols and frameworks for blockchain improvement can result in fragmentation and prevent collaboration amongst stakeholders.

Future Directions and Research Opportunities. To absolutely comprehend the capability of blockchain for records protection, in addition studies and innovation are needed. One promising place of studies is the improvement of extra energy-green and scalable consensus algorithms. For example, new algorithms, consisting of Proof of Authority (PoA) and Delegated Proof of Stake (DPoS), purpose to lessen the computational assets required for consensus at the same time as preserving security.

Hybrid blockchain answers, which integrate the strengths of public and personal blockchains, provide any other road for innovation. These answers can offer the transparency and decentralization of public blockchains whilst keeping the manage and privateness of personal blockchains. By allowing steady statistics sharing amongst a couple of events with out compromising privateness, hybrid blockchains have the ability to conquer some of the boundaries of modern-day blockchain models (Zyskind, & Nathan, 2015).

The integration of blockchain with rising technologies, together with synthetic intelligence (AI), the Internet.

Discussion and conclusions

Blockchain generation gives a promising framework for reinforcing information safety in opposition to unauthorized access. By leveraging its center principles of decentralization, immutability, cryptographic security, and consensus mechanisms, blockchain offers a strong basis for protecting touchy data in diverse applications, from healthcare to finance. Blockchain-primarily based totally models, along with permissioned and permissionless networks, and strategies like clever contracts, decentralized identification management, and encryption techniques, display the capacity to deal with most of the demanding situations confronted with the aid of using conventional information safety strategies.

However, the implementation of blockchain for facts safety isn't always with out its challenges. Issues associated with scalability, electricity consumption, regulatory compliance, and interoperability ought to be cautiously considered. As studies maintains to discover

extra green consensus mechanisms, hybrid blockchain solutions, and integrations with rising technologies, the capability of blockchain to revolutionize facts safety turns into more and more more apparent (Casino, Dasaklis, & Patsakis, 2018).

Ultimately, blockchain affords a transformative method to statistics protection, providing new fashions and techniques that could appreciably lessen the hazard of unauthorized access. Continued innovation, collaboration amongst stakeholders, and model to regulatory necessities may be crucial to absolutely harness the electricity of blockchain and create a extra steady virtual surroundings for all.

References

Casino, F., Dasaklis, T. K., & Patsakis, C. (2018). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. *Telematics and Informatics,* 36, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access,* 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *IEEE Symposium on Security and Privacy (SP),* 839–858. https://doi.org/10.1109/SP.2016.55

Kshetri, N. (2017). Can blockchain strengthen the Internet of Things? *IT Professional,* 19(4), 68–72. https://doi.org/10.1109/MITP.2017.3051335

Nakamoto, S. (n. d.). *Bitcoin: A peer-to-peer electronic cash system.* https://bitcoin.org/bitcoin.pdf

Wood, G. (n. d.). *Ethereum: A secure decentralized generalized transaction ledger.* Ethereum Project Yellow Paper. https://ethereum.github.io/yellowpaper/paper.pdf

Xu, X., Weber, I., & Staples, M. (n. d.). *Architecture for blockchain applications.* Springer. https://doi.org/10.1007/978-3-319-99058-3

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (n. d.). *Blockchain technology overview.* National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.IR.8202

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *IEEE International Congress on Big Data* (pp. 557–564). Honolulu, HI, USA. https://doi.org/10.1109/BigDataCongress.2017.85

Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. *IEEE Security and Privacy Workshops*, 180–184. https://doi.org/10.1109/SPW.2015.27

Отримано редакцією журналу / Received: 11.09.24
Прорецензовано / Revised: 23.09.24
Схвалено до друку / Accepted: 01.10.24

Володимир НАКОНЕЧНИЙ, д-р техн. наук, проф.
ORCID: 0000-0002-0386-2162
e-mail: nvc2006@i.ua
Київський національний університет
імені Тараса Шевченка, Київ, Україна

Владислав ЛУЦЕНКО, асп.
ORCID: 0000-0002-2377-1858
e-mail: vladyslav.lutsenko99@gmail.com
Київський національний університет
імені Тараса Шевченка, Київ, Україна

МОДЕЛІ ТА МЕТОДИ ЗАХИСТУ ДАНИХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ НА ОСНОВІ БЛОКЧЕЙНУ

Ера блокчейну викликала значний інтерес завдяки його здатності підвищувати рівень захисту даних у різних сферах застосування — від фінансових послуг до охорони здоров'я. У статті розглянуто, як блокчейн-орієнтовані моделі та методи забезпечують надійний захист від несанкціонованого доступу до даних, використовуючи децентралізовану архітектуру, криптографічні технології та механізми консенсусу. Виконано аналіз переваг та обмежень різних блокчейн-фреймворків безпеки, а також визначено перспективні напрями для майбутніх досліджень.

Ключові слова: ***блокчейн, захист даних, несанкціонований доступ, децентралізована архітектура, криптографічна безпека, механізми консенсусу, дозвільний блокчейн, відкритий блокчейн, смарт-контракти, децентралізоване управління ідентичністю, шифрування даних, незмінний реєстр, кібербезпека, конфіденційність даних, моделі контролю доступу, масштабованість, нормативна відповідність, інтероперабельність, гібридні блокчейн-рішення.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

.