COMPUTER DESIGN SYSTEMS. THEORY AND PRACTICE

Vol. 6, No. 1, 2024

Mykola Khranovskyi[1], Andriy Kernytskyy[2]

[1] Computer Aided Design Department, Lviv Polytechnic National University, Ukraine, Lviv, S. Bandery street 12,E-mail: mykola.m.khranovskyi@lpnu.ua, ORCID 0000-0002-1633-6639

[2] Computer Aided Design Department, Lviv Polytechnic National University, Ukraine, Lviv, S. Bandery street 12, E-mail: andriy.b.kernytskyy@lpnu.ua, ORCID 0000-0001-8188-559X

BLOCKCHAIN AND BIOMETRICS: CHALLENGES AND SOLUTIONS

Received: March 25, 2024 / Revised: April 01,2024 / Accepted: April 05, 2024

https://doi.org/

Abstract. Blockchain technology has garnered significant attention in recent years due to its ability to revolutionize conventional processes by providing faster, more secure, and cost-effective solutions. This study explores the symbiotic relationship between blockchain and biometrics, investigating how these technologies can mutually reinforce each other. The research makes a dual contribution: firstly, it comprehensively analyses blockchain and biometrics, highlighting their convergence's potential advantages and obstacles. Secondly, it delves deeper into utilising blockchain for safeguarding biometric templates.

Although the potential benefits outlined earlier are promising, integrating blockchain and biometric technologies faces challenges due to constraints within current blockchain technology. These constraints include a limited transaction processing capacity, the need to store all system transactions leading to increased storage demands, and insufficiently explored resilience against diverse attacks.

Historically, biometric systems have been vulnerable to both physical and software-based attacks. While techniques like presentation attack detection can somewhat mitigate physical sensor vulnerabilities, safeguarding against software attacks necessitates adopting biometric template protection measures. Despite advancements in this area, there remains scope for enhancing these methods.

Integrating blockchain and biometrics promises to enhance security and efficiency across various sectors. By combining blockchain's immutability and transparency with biometric data's uniqueness and reliability, organizations can establish robust systems that protect sensitive information while streamlining processes. This research underscores the importance of understanding the intricacies of merging these technologies to leverage their full potential effectively.

Overall, this study sheds light on the transformative power of integrating blockchain and biometrics, offering insights into how this synergy can drive innovation, improve security measures, and optimize operations in a rapidly evolving digital landscape.

Keywords: Blockchain, biometrics, security, privacy, vulnerability, zero-knowledge proof, consensus.

Introduction

Blockchain and biometrics have recently become the centre of attention among today's revolutionary technologies. On the one hand, blockchain technology provides an immutable and decentralised data ledger, optionally enabling the execution of distributed secure code. Its origin is linked to the cryptocurrency Bitcoin, created in 2009, where it has been used to solve an old problem openly since the 80s in the cryptographic community: the design of a distributed consensus algorithm for economic transactions without the involvement or presence of a central authority. However, nothing is stopping any other digital data from being stored instead of financial transactions. This aspect opens the door to many potential applications, such as smart energy and power grids, healthcare, smart devices or digital identification schemes.[1]

On the other hand, biometric technologies aim to authenticate the identification of subjects using physiological (e.g., face, fingerprints) or behavioural (e.g., voice, handwritten signature) traits. Its advantages over traditional authentication methods (e.g., no need to carry tokens or remember passwords, harder to circumvent, and at the same time, provide a more vital link between an object and an action or event) have allowed for the widespread deployment of biometric systems, including large-scale national and international initiatives.

The combination of blockchain and biometrics has many advantages. As a first approximation, blockchain technology can provide biometric systems with some desirable characteristics, such as immutability, accountability, accessibility, or universal access.

By definition, a blockchain guarantees the immutability of registries that a biometric system can use to create a secure storage template. Derived from previous ownership, blockchain increases accountability and the ability to verify stored data, which can be very useful for demonstrating to a third party (e.g., a regulator) that biometric templates have not been altered. The public blockchain also provides full accessibility and universal access for any user.[2]

Furthermore, integrating biometric technology would be very beneficial for blockchains as well. Among many other new use cases, biometrics could significantly improve blockchain-based distributed digital identification schemes. Another exciting application of biometrics in blockchain is related to smart devices. A smart device is any digital or physical asset with access to the blockchain that can perform actions and make decisions based on the information stored there. For example, a car can be fully managed (rented or bought) through a smart contract. However, adequate user identification still needs to be fully solved. In this case, a biometrics-based authentication protocol can significantly improve the current level of security.

Problem Statement

In the context of blockchain technology integrated with biometric systems, the challenge lies in ensuring secure and reliable decision-making processes while mitigating risks associated with unauthorized data modifications, channel interceptions, and potential overrides of final decisions. The integration of consensus mechanisms is crucial to establishing trust, transparency, and decentralization within the system. However, the effectiveness of these consensus algorithms in safeguarding biometric data and preventing unauthorized access needs to be thoroughly evaluated. Additionally, addressing concerns related to data integrity, privacy protection, and system resilience is essential to enhance the overall security posture of biometric systems leveraging blockchain technology.

Review of Modern Information Sources on the Subject of the Paper

Oscar Delgado-Mohatar in “Blockchain and Biometrics: A First Look into Opportunities and Challenges” highlights several key aspects that may be useful for dissertation research. Opportunities and challenges of using blockchain for storing and exchanging biometric data are considered. The limitations of blockchain technology, such as low processing power, confidentiality in public blockchains, the complexity of using smart contracts, and others, are given. The article explores the possibility of using blockchain to protect biometric templates. The article's authors discuss privacy issues in public blockchains and propose different layers of privacy. The article also analyzes the stages of the biometric system and indicates how the blockchain can increase the level of security, in particular in the field of biometric template protection.

Mahdi Ghafourian, in the article “Combining Blockchain and Biometrics: A Survey on Technical Aspects and a First Legal Analysis”, explores the possibilities and limitations of combining blockchain and biometric technologies. The main results and conclusions of the article include an overview of the intersection of blockchain and biometrics from the point of view of both technical and legal possibilities and limitations. It analyzes the impact of blockchain characteristics on biometric systems, considering aspects such as scalability, smart contracts, consensus algorithms, security and data privacy.

Objectives and Problems of Research

Despite the opportunities mentioned in the preceding sections, the amalgamation of blockchain and biometric technologies encounters complexities owing to existing limitations in current blockchain technology. Noteworthy among these limitations are 1) its current low transaction processing capacity (approximately tens of transactions per second), 2) the requirement to store all system transactions, causing rapid growth in necessary storage space for management, and 3) the inadequately studied robustness against various types of attacks.

Now, we elaborate on the limitations of using blockchain public networks for deploying and operating biometric systems.

Economic Cost of Executing Smart Contracts: To support smart contracts in blockchains (e.g., Ethereum) and compensate nodes utilizing their computing capacity for maintaining the system, each executed instruction necessitates a fee payment in cryptocurrency (referred to as gas). Simple instructions, such as a sum, cost 1 gas, while others, like calculating a SHA3 hash, can incur significantly higher costs (e.g., 20 gas). Storage space, costly (around 100 gas for every 256 bits), presents a research challenge in minimising the cost of running a biometric system (either wholly or partially) in a blockchain and optimising the coding efficiency of smart contracts involving biometrics.[3]

Privacy: Inherent to public blockchains is the transparency of all operations to participating nodes. Direct use of secret cryptographic keys is limited, aiming to preserve a wide range of potential applications. Privacy considerations in public blockchains encompass three layers: 1) participants, ensuring participant anonymity both inside and outside the blockchain through cryptographic mechanisms; 2) terms, maintaining the secrecy of smart contract logic using range proofs or Pedersen commitments; and 3) data, crucial for biometrics, emphasising the encryption of transactions, smart contracts, and data like biometric templates, both on-chain and off-chain. Current cryptographic tools, including zero-knowledge proofs (ZKP) and zk-SNARKS, Pedersen commitments, and off-chain privacy layers like hardware-based trusted execution environments (TEEs), are limitedly applied in blockchains. Ethereum introduced basic verification capabilities for ZKPs in late 2017, and more advanced cryptographic tools like Aztec or ZK range proofs have been developed for specific cases. However, the application of these cryptographic tools remains restricted, with ZKP transactions being expensive and computationally intensive (approximately 1.5M gas/verification).[1]

Processing Capability: A vital limitation is related to the processing capability of blockchains. Ethereum, for instance, can execute only around a dozen transactions per second, which may need to be improved for specific scenarios. A minimum confirmation time exists before considering a transaction adequately added to the blockchain. This time varies across blockchains, ranging from tens of seconds to minutes, reducing usability for biometric systems.[2]

Scalability: An inherent challenge since its inception, blockchain technology requires all nodes in the network to store all blocks of the blockchain network. The size of public blockchains like Bitcoin and Ethereum is approximately 200GB, which is growing. This poses challenges for application scenarios like the Internet of Things (IoT).

Security: Blockchain security characterisation remains a work in progress. Among potential attacks, the 51% attack is noteworthy, where an attacker gaining over 50% of the computational capacity of any public or private blockchain could reverse or falsify transactions. This risk applies even to blockchains with consensus algorithms not based on proof-of-work schemes, such as PoS or PoA, typically used in private or consortium topologies. However, to date, primary security issues in blockchains are primarily linked to programming errors, exemplified by the DAO attack in 2016, jeopardising the entire Ethereum ecosystem [2].

Main Material Presentation

Biometric systems have long been susceptible to physical [14] and software-based attacks [11]. While physical attacks on biometric sensors can be mitigated to some extent through presentation attack detection techniques [7], addressing software attacks requires the implementation of biometric template protection methods, which, despite advancements [12,10], still have room for improvement [9].

Figure 1 illustrates the typical stages of a biometric system (depicted in blue), highlighting potential attack vulnerability points alongside a representation of biometric template protection leveraging blockchain (shown as a green block). By substituting the conventional template storage with a blockchain, the security of the resulting biometric system is significantly enhanced. If implemented correctly, attacks such as channel interception (6) and template modification (7) become obsolete.

This design offers several advantages:

1. Minimal modifications to existing biometric systems, allowing the continued use of conventional biometric techniques and algorithms (e.g., feature extraction and matching).
2. Performing the biometric process off-chain mitigates scalability issues typically associated with public blockchains (except in instances of massive user registration batches).
3. Avoidance of complex smart contracts, streamlining development and reducing execution costs. Smart contracts solely manage essential functions for template storage (creation, modification, etc.) rather than implementing biometric "logic."

However, it's essential to note that blockchain storage space is relatively expensive compared to computation, intended to discourage abusive usage. For instance, considering the current Ether price (around $3000 as of February 2024), storing a 1KB fingerprint template in Ethereum would cost approximately $0.0185. Nevertheless, blockchains typically utilise distributed storage platforms like IPFS [3] instead of directly storing data.

Decomposing of the system

The start of the biometric system is input. We enter the biometric data into the sensor. Biometric sensors capture and convert raw biological signals from individuals into digital representations suitable for identification and recognition. They play a crucial role in biometric systems, enabling the automatic identification of people based on unique physiological or behavioural characteristics. Examples of biometric modalities and corresponding sensors include [3]:

- Fingerprint Scanners: Optical and capacitive sensors are commonly used for capturing fingerprints. Optical sensors utilise a prism, light source, and light sensor, while capacitive sensors detect electrical currents generated by finger ridge patterns.
- Optical sensors: Use a prism, light source, and light sensor to capture images of fingerprints.
- Capacitive sensors: Based on a silicon chip that detects electrical currents when the finger ridges make contact.
- Digital Cameras (for Facial Images): Mobile phones, consumer-grade digital SLRs, pocket cameras, and webcams are used to capture facial images. Interocular resolutions of around 60–90 pixels are typically needed for effective one-to-one and one-to-many matching.
- Iris Cameras: Require infrared imagery to enhance image contrast and facilitate machine-based analysis. Special cameras are used to illuminate the iris with infrared light and filter out visible light.
- Microphones (for Voice Recognition): Smartphones are particularly viable for deploying large-scale voice biometrics due to their audio capabilities and ubiquity.
- Keyboards (for Keystroke Dynamics): Keyboard dynamics can be analysed to recognise typing patterns.

Other less common biometric sensors include signature recognition, gait biometrics, and gesture recognition. Biometric sensors are often integrated into edge devices or operate within cloud environments, depending on the complexity of the security or surveillance system.

Biometric sensors capture measurable biological characteristics, known as biometric signals, from individuals. These sensors convert these signals into digital data that can be used with biometric recognition algorithms for automated person identification. The type of sensor used depends on the biometric signal being measured. For instance, simple sensors like good-quality microphones are sufficient for capturing voice biometrics, while specialised hardware is required for other modalities like fingerprint or iris recognition.

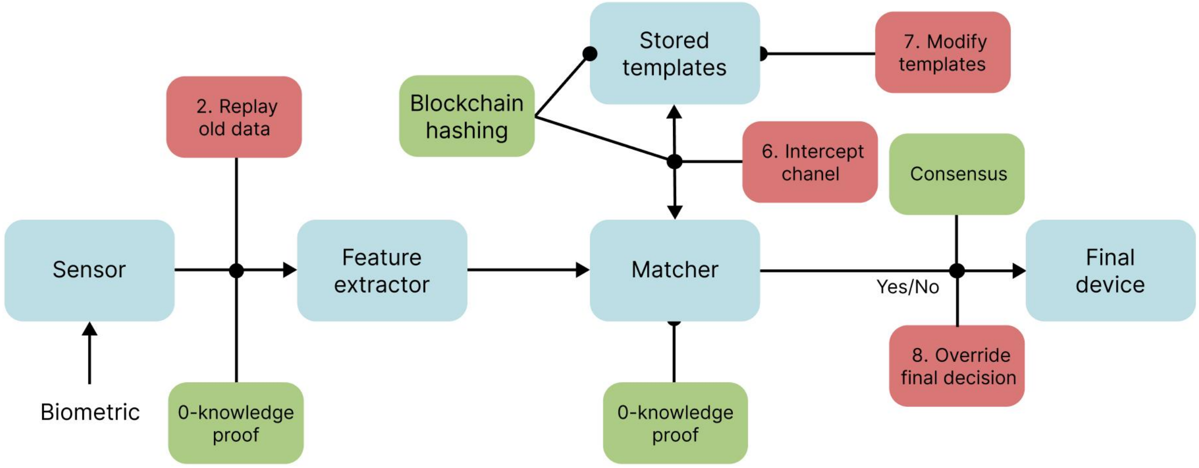

Fig. 1. Biometric system. It's vulnerables and blockchain solutions.

In practical terms, biometric sensors allow biological signals to interface with electronics. For example, a fingerprint sensor captures unique identifiers from a person's fingerprint, which are then processed by algorithms to differentiate one fingerprint from another. Similarly, heart rate monitors record real-time health data. Biometric sensors are widely used in various applications such as device unlocking (fingerprint and facial recognition on phones/laptops), voice recognition in smart speakers, and even in high-security systems like biometric smart cards [1][3].

The feature extractor module is crucial in processing raw biometric data captured by sensors in biometric systems. Its primary function is to extract essential features from the input data, removing noise and irrelevant information to generate a biometric template that can be used for comparison with stored templates in the database.

Some common methods used in feature extraction for biometric systems include:

- Templates that store characteristic patterns or templates derived from the biometric data.
- Applying mathematical transformations to extract distinctive features.
- Identifying and extracting minutiae points (ridge endings, bifurcations) in fingerprint recognition.
- Tracking and extracting specific lines or patterns in biometric data.
- Extracting binary features from the input data.
- Analysing histograms of biometric data to extract relevant features.

Feature extraction is critical as it prepares the data for comparison with stored templates using matching algorithms. It ensures that only relevant and distinctive information is retained for accurate identification or verification [13][4].

The matcher in biometric systems is responsible for comparing biometric templates with stored templates to determine whether a given biometric sample belongs to a particular individual. The matcher uses matching algorithms to calculate similarity scores between the database's input and reference templates. A higher match score indicates a stronger likelihood that the samples belong to the same individual.

For example, the Fingerprint Matcher component from Neurotechnology can match up to 40,000 fingerprints per second, making it suitable for both desktop and mobile biometric systems [4]. Another example, the Fast Face Matcher from Neurotechnology, can match up to 200,000 faces per second, demonstrating its suitability for large-scale biometric systems running on powerful computer hardware [5].

Stored templates in biometric systems are mathematical representations of unique features extracted from biometric samples, such as fingerprints, facial images, or voices. These templates serve as references for comparison purposes during the authentication or identification processes. Templates are not images themselves but rather binary files containing numerical data points that represent the unique characteristics of the biometric sample [15][6].

Several approaches have been developed to maintain the security of biometric templates. Templates can be encrypted before being stored in a database, ensuring they remain unreadable unless decrypted with the appropriate key [1]. Some biometric template protection schemes apply transformation functions to the templates, rendering them unusable without the correct inverse function. Biometric cryptosystems may use helper data to assist in the matching process, providing additional security measures [2]. Distributing templates among multiple nodes reduces the risk of compromise.

These security mechanisms aim to protect biometric templates from unauthorised access, modification, or duplication, thereby preserving the integrity and confidentiality of the stored data.

The decision maker in biometric systems plays a critical role in determining the outcomes of the system's operations, such as authentication or identification. The decision maker may be a human operator or an automated process that evaluates the results provided by the matching algorithm and decides whether to grant access or deny it based on predefined criteria.

Key aspects related to the decision-maker in biometric systems include the following steps. Decision-makers use biometric data to analyse trends and trade-offs to improve decision-making regarding deploying biometric systems [9]. Decision-makers need to consider various factors such as sensor selection, matching algorithms, and cost implications when deploying biometric systems [8]. Visual analysis tools can effectively support decision-makers in deploying biometric systems by providing insights into system performance and requirements [1].

The decision maker's role is crucial in ensuring the efficient and secure operation of biometric systems, especially in complex environments where multiple factors need to be considered for successful deployment [3].

This suite of components constitutes the core functionality of a biometric system, working together to ensure reliable and secure identification or authentication [12]. Additionally, biometric systems may integrate with external devices, such as access control panels or databases, to enable seamless integration with broader security architectures [4].

Threads and Solutions

Replaying old data to the feature extractor in biometric systems can pose a significant security risk, potentially leading to unauthorised access or identity theft. Attackers may attempt to replay stolen biometric data to the feature extractor, forcing it to produce feature sets chosen by the attacker instead of the actual values generated from the current data obtained from the sensor. This manipulation can compromise the integrity of the biometric system and result in fraudulent access.

Integrating zero-knowledge proofs (ZKPs) into biometric systems can enhance security by mitigating the risk of replaying old data to the feature extractor. Zero-knowledge proofs allow a party (prover) to demonstrate knowledge of specific information without revealing the data itself. In the context of biometric systems, ZKPs can be utilised to prove the authenticity of biometric data without exposing the raw biometric information, thus preventing replay attacks.

By incorporating ZKPs into the authentication process of biometric systems, the following benefits can be achieved:

- It enables authentication without disclosing sensitive biometric data, preserving user privacy [1].
- ZKPs add a layer of security by ensuring that only legitimate users can authenticate without the risk of replaying old data [4].
- It helps prevent unauthorised access and identity theft by verifying the authenticity of biometric data securely and privately [2].

Overall, integrating zero-knowledge proofs into biometric systems can significantly enhance security and privacy, safeguarding against replay attacks and ensuring the integrity of the authentication process [1][2][4].

The dangers associated with modifying templates or channel interception between template storage and matcher in biometric systems include several threads.

Malicious actors who gain access to stored templates can use them to impersonate genuine users, circumventing the authentication process [1]. Adversaries might modify templates to increase the chances of passing the authentication process, posing a threat to system security [1]. Attacks aimed at intercepting the communication channels between the template database and the matcher module can expose sensitive biometric data [1]. Template Database Breaches: Hacking or stealing the template database exposes all stored templates, putting the entire system at risk [3]. Tampering with the Matcher Module: Introducing malware or exploiting vulnerabilities in the Matcher module can lead to false positives, allowing unauthorised access [1].

To mitigate these risks, biometric systems should implement robust encryption protocols, access controls, and secure communication channels between components. Blockchain integration can reduce the risks of rewriting of storing templates or channel interceptions between template storage and matcher by introducing increased security and transparency. Here are some ways blockchain can contribute to securing biometric systems [3]:

- Secured Storage: Blockchain enables tamper-proof storage of biometric templates, making it difficult for unauthorised parties to alter or delete the data.
- Immutable Records: Once recorded on a blockchain, biometric templates cannot be altered, reducing the possibility of data manipulation.
- Decentralised Architecture: Blockchain eliminates single points of failure, spreading data across numerous nodes and minimising the risk of centralised data breaches.
- Advanced Consensus Mechanisms: Blockchain utilises sophisticated consensus algorithms like proof-of-work (PoW) or proof-of-stake (PoS) to validate transactions, improving the security of biometric data.
- Zero-Knowledge Proofs (ZKP): Integrating ZKPs with blockchain technology can further enhance the security of biometric systems by protecting sensitive data without revealing the original biometric information.
- Multi-Party Computation (MPC): MPC allows multiple parties to jointly compute a result without revealing their inputs, which can be applied to biometric systems to share data securely.
- Privacy Preservation: Blockchain can facilitate privacy-preserving methods, such as homomorphic encryption, to keep biometric data safe while permitting authorised access.

Hashing plays a crucial role in maintaining the integrity and security of blockchain networks by enabling the creation of unique digital fingerprints for data. When using blockchain integrated with biometric systems, hashing contributes to several security mechanisms.

By comparing the hash of a block to the stored hash, it becomes possible to confirm that the data has not been tampered with. Each block in the chain contains the preceding block's hash, forming an indelible chain that prevents modifications to earlier blocks without invalidating subsequent ones. Hashed biometric data can be stored safely without revealing the underlying biometric information, enhancing privacy and security. Modifications to the data would cause the resulting hash to differ from the expected value, alerting the system to suspicious activity. Hashing facilitates the consensus process among network participants, ensuring that only valid transactions are included in the blockchain.

Without hashing, blockchain-based biometric systems could not guarantee the security and integrity of the stored data, undermining their effectiveness [4].

Integrating consensus mechanisms into the decision-making process of biometric systems can help secure the system from unauthorised overrides of the final decision. Consensus mechanisms ensure that all nodes in a blockchain network agree on the validity of transactions or decisions, preventing any single entity from unilaterally altering the outcome. By leveraging consensus mechanisms within blockchain technology, biometric systems can establish a secure and trustworthy environment where decisions made by the system are resistant to unauthorised changes or manipulations.

Consensus algorithms are fundamental components of blockchain technology that enable nodes in a network to agree on the validity of transactions and the order in which they are added to the blockchain. These algorithms play a crucial role in maintaining blockchain networks' integrity, security, and decentralisation.

Consensus algorithms are the foundation for achieving agreement and reaching decisions within blockchain networks. They provide a set of rules or protocols that enable nodes to agree on the validity of transactions and the order in which they are added to the blockchain. Several popular consensus algorithms include:

- Proof of Work (PoW)– Requires miners to compete to find a solution to a mathematical problem, which confirms new transactions and adds new blocks to the blockchain.
- Proof of Stake (PoS)– Selects validators based on the size of their stake in the currency, encouraging holders to participate in the validation process.
- Delegated Proof of Stake (DPoS)– Combines elements of PoS and representative democracy, allowing voters to elect representatives called "witnesses" or "delegates."
- Proof of Activity (PoA)– Hybrid consensus mechanism combining aspects of PoW and PoS, aiming to improve efficiency and reduce energy consumption.
- Proof of Identify (PoI)– Uses identity verification to ensure that only known entities can participate in the consensus process, promoting security and authenticity.

These consensus algorithms enable nodes to reach a consensus on the validity of transactions and the order in which they are added to the blockchain. By doing so, they help secure the decision-maker from potential overrides and ensure the integrity of the blockchain network [3].

Overall, consensus algorithms are essential for establishing trust, security, and reliability in blockchain networks, making them a cornerstone of decentralised systems like biometric applications integrated with blockchain technology.

Results and Discussion

The exploration of the integration between biometric systems and blockchains has revealed intriguing insights, presenting both opportunities and challenges. This section summarizes the key findings and engages in a comprehensive discussion to elucidate the implications of the research.

The discussion on blockchain fundamentals underscored the decentralized and chronological ledger nature of blockchains. The classification into public, consortium, and private blockchains highlighted the diverse access control schemes and consensus algorithms. The choice of blockchain type, dependent on the specific use case, was emphasized, with considerations for transaction efficiency and completion time. Additionally, the overview touched upon the role of smart contracts in executing code in a secure environment, with Ethereum emerging as a prominent platform supporting smart contracts.

The examination of challenges and limitations in combining blockchain and biometric technologies shed light on several critical issues. The low transaction processing capacity, storage space requirements, and the need for robust security against diverse attacks were identified as primary challenges. The economic cost of executing smart contracts, privacy concerns, processing capability limitations, scalability issues, and evolving security threats were discussed in detail. These challenges set the stage for considering the viability of integrating blockchain and biometrics.

The investigation into using blockchain for biometric template protection outlined a promising approach to enhance the security of biometric systems. By substituting traditional template storage with blockchain, vulnerabilities such as channel interception and template modification were addressed. This design offered advantages, including minimal modifications to existing systems, scalability benefits, and reduced development costs. However, the expensive nature of blockchain storage raised considerations about its economic feasibility, leading to discussions on alternatives such as distributed storage platforms like IPFS.

The concluding remarks acknowledged the nascent stage of research on the integration of biometric systems and blockchains. Despite the initial steps, the potential for collaboration and mutual growth between the technologies was affirmed. The paper highlighted the main characteristics and limitations of blockchains, emphasizing their impact on implementing biometric systems. The discussion also explored potential mutual benefits and presented an initial architecture using blockchain for biometric template protection. Looking forward, the question of integrating biometric processes on-chain was posed, acknowledging the current challenges but pointing towards promising research areas like state channels and zero-knowledge proofs.

The integration of biometric systems and blockchains presents a complex landscape with both technological potential and inherent challenges. While the protection of biometric templates using blockchain showcases a promising avenue, the economic feasibility, scalability concerns, and the need for continued technological advancements in blockchain security remain critical considerations. The future trajectory of this integration will likely hinge on addressing these challenges, exploring innovative solutions, and adapting to the evolving landscape of both biometric and blockchain technologies..

Conclusions

While exploring the convergence of biometric systems and blockchains is in its early stages, the potential for collaboration and substantial mutual growth between these technologies is undeniable.

This paper has delved into the key characteristics and limitations of blockchains, particularly those directly impacting the implementation of biometric systems. The discussion has also centred on potential reciprocal advantages for both technologies, presenting an initial approach to a combined architecture utilizing blockchain to protect biometric templates.

Looking ahead, a crucial question emerges: to what extent can biometric processes be integrated or transferred onto a blockchain, i.e., conducted on-chain? For instance, is implementing a biometric matcher through a smart contract feasible? If so, how and what challenges need to be addressed?

Given blockchain technology's current constraints and features, achieving a comprehensive integration with biometric processes appears highly challenging in the short term. Nonetheless, promising research avenues exist, such as exploring state channels [7], which could significantly reduce costs and enhance bandwidth. The development of novel zero-knowledge proofs holds potential, allowing user authentication through biometrics without either party possessing knowledge of the user's identity.

References

[1] Ahmed, M.R., Islam, A.M., Shatabda, S., Islam, S.: Blockchain-based identity management system and self-sovereign identity ecosystem: a comprehensive survey. IEEE Access 10, 113436–113481 (2022) https://doi.org/10.1109/ACCESS.2022.3216643

[2] CHOUDHARI, S., DAS, S.K., PARASHER, S.: Interoperable blockchain solution for digital identity management, 6th International Conference for Convergence in Technology (I2CT), IEEE, pp. 1–6. (2021). https://doi.org/10.1109/I2CT51068.2021.9418220

[3] Delgado-Mohatar, O., Fierrez, J., Tolosana, R., Vera-Rodriguez, R.: Blockchain and biometrics: a first look into opportunities and challenges. In: Blockchain and Applications: International Congress, pp. 169–177. Springer (2020) https://doi.org/10.1007/978-3-030-23813-1_21

[4] Puthal, D., Malik, N., Mohanty, S.P., Kougianos, E., Yang, C.: The blockchain as a decentralized security framework [future directions]. IEEE Consum. Electron. Mag. 7, 18–21 (2018) https://doi.org/10.1109/MCE.2017.2776459

[5] Rivera, R., Robledo, J.G., Larios, V.M., Avalos, J.M.: How digital identity on blockchain can contribute in a smart city environment, international smart cities conference (ISC2). IEEE 2017, 1–4 (2017) https://doi.org/10.1109/ISC2.2017.8090839

[6] Patwary, A.A.N.; Fu, A.; Battula, S.K.; Naha, R.K.; Garg, S.; Mahanti, A. FogAuthChain: A secure location-based authentication scheme in fog computing environments using Blockchain. Comput. Commun. 2020, 162, 212–224. https://doi.org/10.1016/j.comcom.2020.08.021

[7] Tuli, S.; Mahmud, R.; Tuli, S.; Buyya, R. Fogbus: A blockchain-based lightweight framework for edge and fog computing. J. Syst. Softw. 2019, 154, 22–36. https://doi.org/10.1016/j.jss.2019.04.050

[8] Guo, Y.; Guo, Y. FogHA: An efficient handover authentication for mobile devices in fog computing. Comput. Secur. 2021, 108, 102358. https://doi.org/10.1016/j.cose.2021.102358

[9] Fotohi, R.; Shams Aliee, F. Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT. Comput. Netw. 2021, 197, 108331. https://doi.org/10.1016/j.comnet.2021.108331

[10] Omar, I.A.; Hasan, H.R.; Jayaraman, R.; Salah, K.; Omar, M. Implementing decentralized auctions using blockchain smart contracts. Technol. Forecast. Soc. Chang. 2021, 168, 120786. https://doi.org/10.1016/j.techfore.2021.120786

[11] Maxmen A., ‘‘Ai researchers embrace bitcoin technology to share medical data,’’ Nature, vol. 555, pp. 293–294, Mar. 2018. https://doi.org/10.1038/d41586-018-02641-7

[12] Nebula Ai (NBAI)—Decentralized ai Blockchain Whitepaper, Nebula AI Team, Montreal, QC, Canada, 2018.

[13] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas. (2016). ‘‘Communication-efficient learning of deep networks from decentralized data.’’ [Online]. Available: https://arxiv.org/abs/1602.05629

[14] V. Lopes and L. A. Alexandre. (2018). ‘‘An overview of blockchain integration with robotics and artificial intelligence.’’ [Online]. https://doi.org/10.5195/ledger.2019.171

[15] T. Marwala and B. Xing. (2018). ‘‘Blockchain and artificial intelligence.’’ [Online]. Available: https://arxiv.org/abs/1802.04451.

Микола Храновський[1], Андрій Керницький[2]

[1] Кафедра систем автоматизованого проектування, Національний університет «Львівська політехніка»,
вул. С. Бандери 12, Львів, Україна, E-mail: mykola.m.khranovskyi@lpnu.ua, ORCID 0000-0002-1633-6639

[2] Кафедра систем автоматизованого проектування, Національний університет «Львівська політехніка»,
вул. С. Бандери 12, Львів, Україна,, E-mail: andriy.b.kernytskyy@lpnu.ua, ORCID 0000-0001-8188-559X

БЛОКЧЕЙН ТА БІОМЕТРИКА: ПРОБЛЕМИ І РІШЕННЯ

Отримано: березень 25, 2024 / Переглянуто: квітень 01,2024 / Прийнято: квітень 05, 2024

Анотація. Технологія блокчейн привернула значну увагу в останні роки завдяки своїй здатності революціонізувати звичайні процеси, надаючи швидші, безпечніші та економічно ефективніші рішення. У цьому дослідженні досліджується симбіотичний зв'язок між блокчейном і біометрією, досліджується, як ці технології можуть взаємно посилювати одна одну. Дослідження сфокусоване на двох аспектах: по-перше, всебічний аналіз блокчейну і біометрії, висвітлюючи потенційні переваги та перешкоди їхньої конвергенції. По-друге, глибше вивчення можливостей використання блокчейну для захисту біометричних шаблонів. Хоча описані раніше потенційні переваги є багатообіцяючими, інтеграція блокчейну та біометричних технологій стикається з проблемами через обмеження технології блокчейну. Ці обмеження включають обмежену здатність обробки транзакцій, необхідність зберігати всі системні транзакції, що призводить до збільшення вимог до пам'яті, і недостатньо вивчену стійкість до різноманітних атак. Історично біометричні системи були вразливими як до фізичних, так і до програмних атак. Хоча такі методи, як виявлення атак, можуть дещо пом'якшити вразливість фізичних сенсорів, захист від програмних атак потребує застосування заходів захисту біометричних шаблонів. Незважаючи на прогрес у цій галузі, залишається простір для вдосконалення цих методів. Інтеграція блокчейну у біометричні системи передбачає підвищення безпеки та ефективності в різних секторах. Поєднуючи незмінність і прозорість блокчейну з унікальністю та надійністю біометричних даних, організації можуть створювати надійні системи, які захищають конфіденційну інформацію, оптимізуючи процеси. Це дослідження підкреслює важливість розуміння тонкощів об'єднання цих технологій для ефективного використання їх повного потенціалу. Загалом це дослідження проливає світло на трансформаційну силу інтеграції блокчейну та біометрії, пропонуючи розуміння того, як ця синергія може стимулювати інновації, покращувати заходи безпеки та оптимізувати роботу в цифровому середовищі, що швидко розвивається.

Ключові слова: Блокчейн, біометрія, безпека, конфіденційність, вразливість, zero-knowledge proof, консенсус.