Proceedings of the 2023 International Conference on Machine Learning and Automation
DOI: 10.54254/2755-2721/30/20230094

A review of identity authentication based on blockchain technology

Jiawei Li

Macau University of Science and Technology

18030453895@163.com

Abstract. Blockchain, as one of the emerging technologies in recent years, is essentially a decentralized distributed ledger. By leveraging blockchain, it provides a new approach to identity authentication. This paper provides an overview of the applications of identity authentication based on blockchain. Firstly, the background knowledge of blockchain is introduced. Then, the technical aspects of identity authentication based on blockchain are discussed and classified from the perspectives of identity authentication techniques and cryptographic algorithms. Subsequently, the applications of identity authentication based on blockchain technology are introduced and classified in various fields. Finally, a summary of the entire paper is presented.

Keywords: Blockchain, Identity Authentication, Information Security.

1. Introduction

The network environment has become increasingly complex, and the demand for security and privacy of personal information by users in the network has become more prominent.

To protect user data security and privacy, the application of identity authentication plays a key role. Identity authentication is a process of verifying the authenticity of the authenticated party, based on the idea of the authenticating party validating the characteristic information of the authenticated party to confirm its validity and effectiveness [1]. In order to achieve the goal, designing novel identity authentication methods is one of the crucial factors.

Originating from Bitcoin, blockchain was first introduced in 2008. Blockchain possesses characteristics such as decentralization, openness, independence, tamper-proof information, and anonymity. Based on these features, the information recorded on the blockchain is more transparent, authentic, and reliable [2].

The design and application of identity authentication based on blockchain can address the security vulnerabilities in the authentication process. Utilizing blockchain for storing user identity information takes advantage of the decentralized, tamper-proof, and traceable nature of the blockchain itself, ensuring the security and privacy of user information.

2. Introduction of blockchain technology

Blockchain, as a distributed ledger technology, can be used to record transactions and data, and share and verify these records among multiple nodes in a network. Originally used as the underlying technology for Bitcoin, blockchain is now widely applied in various fields.

DOI: 10.54254/2755-2721/30/20230094

The fundamental concept of blockchain is the "block," which contains a series of transactions and other information. These blocks are linked together using hash functions from cryptography, forming a growing chain, hence the name "blockchain."

Blockchain can be mainly categorized into the following four types [3].

Table 1. Classification of Blockchain.

Blockchain Type	Characteristic
Public Blockchain	-Open and transparent, anyone can participate. -Decentralized, no central authority control.
Private Blockchain	-Restricted,only specific participants can access. -Higher privacy and control.
Consortium Blockchain	-Blockchain network composed of multiple organizations or entities. -Participants require authorization to join.
Hybrid Blockchain	-Combines characteristics of public and private blockchains. -Provides greater flexibility and customization.

2.1. Distributed Ledger

A distributed ledger is a general term that describes a shared database. Technically, all blockchains fall under the category of shared databases or distributed ledgers. As a data structure for recording transactions and data, a distributed ledger achieves decentralized data management and verification by sharing and synchronizing copies of the ledger among multiple nodes in a network.

In traditional centralized ledger systems, data is managed and maintained by a central authority or a third party. In contrast, a distributed ledger transfers the control of data to multiple participants in the network. Each node has a complete copy of the ledger and consensus algorithms are used to achieve agreement, ensuring that the ledger remains synchronized and consistent across all nodes.

2.2. Consensus Mechanisms

In blockchain, consensus mechanisms are used to address issues such as confirming transaction order, validating transaction validity, and maintaining ledger consistency among nodes.

In a distributed system, factors such as network latency, node failures, and malicious attacks can result in differences in views and data among nodes. The objective of consensus mechanisms is to enable multiple nodes to reach a consensus decision or state through specific rules and processes, ensuring the reliability, security, and consistency of the system.

2.3. Smart Contracts

Smart contracts are automated contracts executed on blockchain. They are defined in the form of code and establish transaction rules and conditions among the involved parties. Smart contracts enable the automatic validation and execution of the agreed-upon terms without the need for intermediaries, and the outcomes are recorded on the blockchain.

Smart contracts possess characteristics of immutability, decentralization, and security. Their execution takes place on the blockchain, and both the code and the execution results are recorded on the blockchain, making them tamper-proof and unalterable. Cryptography and encryption techniques are employed in smart contracts to ensure the security of transactions and data. The code and execution logic of smart contracts undergo verification processes to mitigate potential vulnerabilities and attacks.

3. Identity Authentication Based on Blockchain Technology

Currently, there is a significant amount of researches on blockchain-based identity authentication. In this section, we will categorize and introduce these studies from two technical perspectives: identity authentication technologies and encryption algorithms.

DOI: 10.54254/2755-2721/30/20230094

3.1. Identity authentication

3.1.1. Password identity authentication

Static password identity authentication is the most fundamental form of identity authentication, where users verify their identities by inputting pre-set static passwords.However, static password identity authentication has certain security vulnerabilities. For instance, passwords might be maliciously intercepted during transmission, or be susceptible to being compromised.

In contrast, dynamic password identity authentication is another form of password-based identity authentication. It relies on one-time passwords for identity verification, requiring users to utilize dynamically changing passwords generated by applications for each authentication attempt. Compared to static password identity authentication, dynamic password identity authentication offers higher security.

As a prevailing identity authentication technology, dynamic password identity authentication finds widespread use in blockchain-based identity authentication. Zhu et al. [4] designed a blockchain-based dynamic password identity authentication system. This system utilizes information stored in the blockchain, such as public keys and the current block height (nonce) array, to generate unique combinations of public keys and nonce arrays for each authentication attempt. The authentication is completed through verification by the entire network of nodes. By incorporating these features, this system significantly enhances security during the authentication process compared to traditional identity authentication systems, while also increasing system flexibility.

3.1.2. PKI Identity authentication

PKI (Public Key Infrastructure) identity authentication utilizes asymmetric encryption algorithms to ensure secure identity verification and data transmission. Compared to traditional identity authentication, blockchain-based PKI identity authentication enhances trust among nodes and improves authentication efficiency through the characteristics of blockchain.

Zhao et al. [5] proposed a two-tier cross-domain identity authentication model by constructing an alliance blockchain consisting of an authentication server node (AS) and a partial internal blockchain. This model significantly improves the scalability of the PKI system without altering its internal architecture. The results demonstrate that the proposed system exhibits strong security and performance in handling cross-domain identity authentication transactions.

3.1.3. Biometric identity authentication

Biometric identity authentication is a method of identity verification based on individual biological characteristics. It involves the generation of templates from pre-collected unique biological features of individuals, such as fingerprints, irises, and facial features. During the identity authentication process, the biometric features of the authenticated party are compared with the previously stored templates to achieve the purpose of identity authentication.

Toutara et al. [6] proposed a distributed biometric authentication scheme. This scheme utilizes blockchain and IPFS (InterPlanetary File System), employing the FV homomorphic encryption algorithm to encrypt users' biometric templates. The user's biometric template undergoes transformation and encryption before being sent from the device for authentication. The homomorphic properties of the encryption algorithm allow calculations to be performed on the encrypted vectors without the need to decrypt them into plaintext. Therefore, third parties can make decisions on authentication attempts without accessing the user's actual biometric data.

3.2. Encryption Algorithm

During the process of identity authentication, encryption algorithms are used to encrypt sensitive data and authenticate user identities. Various types of encryption algorithms are currently employed in blockchain-based identity authentication research.

DOI: 10.54254/2755-2721/30/20230094

Hash algorithms are utilized to transform input data of arbitrary lengths into fixed-length output data. They play a vital role in data integrity verification and identity authentication. Commonly used hash algorithms include MD5 and SHA-256. For instance, in the study conducted by Dinesh et al. [7], fingerprint scan images are converted into passwords using the MD5 algorithm, taking reference from blockchain-based biometric identity authentication.

Symmetric encryption algorithms employ the same key for both encryption and decryption of data. Well-known symmetric encryption algorithms include AES and DES. In the model of a blockchain-based identity management system designed by Gupta et al. [8], the AES algorithm is used for encrypting biometric features and demographic data.

In contrast, asymmetric encryption take the public key and the private key, for encryption, decryption, digital signing, and verification. For example, in the research conducted by Yadav et al. [9] on the 5G-AKA security protocol in communication systems, the elliptic curve algorithm (ECC) is used as an encryption algorithm for security protection and key negotiation.

Table 2. Classification of encryption algorithms in identity authentication.

Encryption Algorithm	Characteristic
Hash Algorithm	-Maps input data of arbitrary length to output of fixed length. -Examples: SHA-256, SHA-3, MD5
Symmetric encryption algorithm	-An encryption algorithm that uses the same key for encryption and decryption. -Examples: DES, AES, IDEA
Asymmetric encryption algorithm	-An encryption algorithm that uses different keys for encryption and decryption -Examples: RSA, ECC, DSA

4. Blockchain identity authentication application

4.1. Internet of Things

The Internet of Things (IoT) is an industrial model based on Internet technologies that connects and integrates various devices and data in the physical world, enabling them to interact and communicate with each other.

For smart devices in the IoT, ensuring data security is particularly crucial as they interact and communicate with each other and other devices via the Internet. In the research conducted by Gong et al. [10], they propose the iot-chain security authentication system, which combines access control with blockchain technology to provide dynamic security authentication management for the IoT. Additionally, the application of blockchain allows devices in the IoT to maintain high throughput and achieve effective consensus.

At the national level, the scale of smart grids is continuously expanding. Leveraging smart contracts and consensus mechanisms in the blockchain [11], users can perform corresponding operations once they obtain permission, linking the information stored in the authentication system to the application system. This approach effectively promotes data sharing, facilitates information circulation, and ensures system security.

4.2. Finance/Healthcare

In addition to its applications in the field of IoT, blockchain-based identity authentication has also been extensively researched in the domains of finance and healthcare.

In the finance sector, blockchain is widely used in BFSI (Banking, Financial Services, and Insurance) sectors. Akram et al. [12] provided numerous technical and business use cases, such as using smart contracts as protocols for financial transactions, encrypting transactions, and using blockchain for encrypted authentication in electronic payments.

DOI: 10.54254/2755-2721/30/20230094

In the healthcare domain, blockchain-based identity authentication is applied to authenticate and encrypt personal information and health records in health management systems, as well as secure authentication of smart health devices associated with patients. In another study by Gong et al. [13], mentioned earlier, they proposed a scheme for identity authentication that utilizes fuzzy extraction techniques to derive random keys from individual biometric features. Shukla et al. [14], in their research, introduced blockchain into the healthcare IoT to achieve secure and reliable transactions. They proposed a fog computing (FC) and blockchain-based solution, which improves the accuracy and reliability of malicious node detection, ensuring secure data transmission and authentication.

5. Summary

In conclusion, this paper provides a comprehensive overview of blockchain-based identity authentication, covering its foundations, research directions, and practical applications. The potential of this technology for improved development and wider adoption is evident. It is anticipated that blockchain-based identity authentication will play a crucial role in addressing the security challenges associated with identity verification and will find extensive applications in various domains in the future. Further research and development in this area are essential to enhance its capabilities and ensure its seamless integration into existing systems and processes.

References

[1] Liansong Zhou, Jie Yang, Pingzhang Tan, et al. (2009) Identity Authentication Technology and Its Development Trend. Communications Technology, 42(10).
[2] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System.
[3] Bashir, Imran. (2018) Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explaine (2nd Edition).
[4] Jintao Zhu, Yinzhen Wei, Xiaoxiao Shang. (2021) Decentralized Dynamic Identity Authentication System Based on Blockchain. 2021 INSAI.
[5] Gang Zhao, Bingbing Di, Hui He. (2022) A novel decentralized cross-domain identity authentication protocol based on blockchain. Transactions on emerging telecommunications technologies, 33(1).
[6] Foteini Toutara, Georgios Spathoulas. (2020) A distributed biometric authentication scheme based on blockchain. 2020 IEEE International Conference on Blockchain.
[7] A.D.Dinesh, C.D.P.Reddy, G.V.Gopi, et al. (2021) A Durable Biometric Authentication Scheme via Blockchain. 2021 ICAECT.
[8] Shreya Gupta, A.K.Bairwa, S.S.Kushwaha, et al. (2023) Decentralized Identity Management System using the amalgamation of Blockchain Technology. 2023 3rd International Conference on Intelligent Communication and Computational Techniques
[9] A.K.Yadav, An Braeken, Manoj Misra, et al. (2023) A Provably Secure and Efficient 5G-AKA Authentication Protocol using Blockchain. IEEE 20th Consumer Communications & Networking Conference.
[10] Gongguo Zhang, Zhou Wan. (2021) Blockchain-based IoT security authentication system. 2021 International Conference on Computer, Blockchain and Financial Development (CBFD)
[11] Lijun Zhang, Liang Hu, Wenbo Xie, et al. (2022) Distributed Authentication Method for Power Grid Based on Consortium Blockchain. 2022 6th International Conference on Wireless Communications and Applications (ICWCAPP)
[12] Md Akram, Anshuman Sen. (2022) A case study Evaluation of Blockchain for digital identity verification and management in BFSI using Zero-Knowledge Proof. 2022 International Conference on Decision Aid Sciences and Applications (DASA)
[13] Gongguo Zhang, Zuo Ou. (2021) Personal health data identity authentication matching scheme based on blockchain. 2021 International Conference on Computer, Blockchain and Financial Development (CBFD)

DOI: 10.54254/2755-2721/30/20230094

[14] Saurabh Shuklaa, Subhasis Thakur, Shahid Hussain, et al. (2021) Identifification and Authentication in Healthcare Internet-of-Things Using Integrated Fog Computing Based Blockchain Model. Internet of Things, 15:100422