Research on Digital Identity Authentication System based on Spark Blockchain

Kai Yuan[a], Minghao Gu[b]*, Yadong Hu[c]

China Academy of Information and Communications Technology Beijing, China

[a]yuankai@caict.ac.cn, [b]guminghao@caict.ac.cn,
[c]huyadong@caict.ac.cn

Abstract. At present, Internet network only has the ability to transmit data accurately and efficiently end-to-end, which cannot determine the identity of the sender and receiver. Traditional authentication systems, plagued by vulnerabilities and inefficiencies, necessitate a shift towards more secure, decentralized solutions. In this work, we proposed a novel authentication model that leverages blockchain's inherent features for enhanced security and user control. Specifically, the system utilizes cryptographic hash functions and digital signatures to create a unique digital identity for each user. As for registration, identity information is encrypted and a digital signature is created, which is then recorded on the spark blockchain. For authentication, the system matches the presented digital signature with the one stored on the blockchain, ensuring that only the legitimate user can access their identity. The framework of proposed model integrates cryptographic methods for identity verification, ensuring data privacy and integrity. Through our extensive experiments validation, we can observe that the system demonstrates significant improvements in security against identity theft and unauthorized access, while offering a streamlined, user-friendly authentication process.

Keywords: Digital identify authentication, Encryption algorithm, Spark blockchain, Information security.

1 Introduction

With the continuous development of the Internet, more and more users use the online services provided by service providers through the Internet, among which there is a problem that has not been considered at the beginning of the Internet design, that is, the Internet itself does not have a unified and secure identity authentication scheme. Today's Internet only has the ability to transmit data accurately and efficiently end-to-end, but it cannot determine the identity of the sender and the identity of the receiver. Therefore, identity authentication has become an essential procedure of online security, privacy, and trust system [1]. As we increasingly shift our lives into the digital realm, from financial transactions to social interactions, the need to accurately and securely verify digital identities has never been more critical. Traditional methods of identity

K. Subramaniyam et al. (eds.), *Proceedings of the 3rd International Academic Conference on Blockchain, Information Technology and Smart Finance (ICBIS 2024)*, Atlantis Highlights in Computer Sciences 21,
https://doi.org/10.2991/978-94-6463-419-8_30

verification, relying on passwords, security questions, or physical documents, are becoming outdated and vulnerable in the face of sophisticated cyber threats. These challenges have spurred the search for more secure, efficient, and user-centric approaches to digital identity authentication.

Further, digital Identity Authentication represents a fundamental mechanism for ensuring that individuals or entities engaging in digital activities are who they claim to be. This process is pivotal in preventing unauthorized access to personal data, securing online transactions, and fostering trust in digital ecosystems. However, the evolution of digital technologies and the proliferation of online services have also amplified the complexities and challenges associated with managing digital identities [2]. Issues such as identity theft, fraud, data breaches, and privacy violations are becoming increasingly prevalent, highlighting the limitations of conventional authentication methods. Multi-center or decentralized authentication solutions can alleviate or avoid the problems caused by centralized authentication, but also bring new usability and security problems. This paper combines identity authentication with blockchain technology, and uses the characteristics of blockchain to be decentralized, tamper-proof, and distributed to solve the problems of trust transfer between multiple centers and multi-party data consistency. However, the existing blockchain-based decentralized system has the problem of low security and availability [3].

In today's digital age, digital identity verification has become one of the key technologies to ensure the security of online transactions and communications. With the dramatic increase in cyberspace activity, people are increasingly relying on digital identities to access and use a variety of online services, from online banking to social media to e-commerce and government services. This reliance not only highlights the importance of digital identity management, but also exacerbates the need for strong, reliable, and user-friendly authentication mechanisms [4]. Digital identity verification is a technical process by which a system is able to confirm that an individual's identity matches their claimed digital identity. This includes a range of methods and technologies designed to ensure the authenticity of an individual's or entity's online identity, such as passwords, two-factor authentication, biometrics, and digital certificates. The right authentication mechanism not only prevents unauthorized access, but also ensures data integrity and privacy protection, thus providing security for interactions between users and service providers [5].

As technology evolves, so does the increasingly complex challenge of digital authentication. These challenges include how to handle large amounts of identity data, protect user privacy, prevent identity theft and fraud, and improve the user experience without sacrificing security. In addition, with the development of blockchain, artificial intelligence, and IoT technologies, digital identity verification solutions are moving in the direction of more secure, decentralized, and user-controlled, which opens up new possibilities for digital identity management [6]. Therefore, exploring the current state, challenges, and future trends of digital identity verification is critical to understanding and shaping our digital future. By ensuring that the development of authentication technology can meet the growing demand for security, we can lay a solid foundation for the healthy development of a digital society.

Spark Blockchain is an innovative blockchain technology that aims to solve the challenges of existing blockchain systems while providing high efficiency, scalability, and security. With the rapid development of the digital economy and the popularity of cryptocurrencies, blockchain technology has become a key infrastructure in the fields of financial technology, supply chain management, and digital identity verification. However, as blockchain applications continue to expand, the limitations of traditional blockchain platforms such as Bitcoin and Ethereum in terms of processing speed, transaction costs, and scalability are becoming apparent [7]. Spark Blockchain was born to provide a faster, more efficient, and scalable blockchain solution through an innovative consensus mechanism, optimized network structure, and advanced encryption technology [8].

Spark Blockchain is designed with the needs of both business and individual users in mind, focusing not only on performance improvements, but also on user experience and security. By employing a layered architecture, sidechain technology, and a smart contract platform, Spark Blockchain aims to provide developers and businesses with a flexible, easy-to-use blockchain development environment while ensuring immutability of data and transparency of transactions [9]. In addition, Spark Blockchain has also introduced an environmentally friendly consensus algorithm to reduce the environmental impact of blockchain operation, which is of great significance to improve the acceptance of blockchain technology in society. As blockchain technology continues to advance, Spark Blockchain is expected to be a key force in driving the widespread adoption of blockchain technology and realizing its potential value. This article will delve into the technical architecture, core features, and how it solves the pain points of existing blockchain technology, and also looks forward to its application prospects in the future digital economy [10].

2 Notions

We summarize the primary used parameters in following Table 1.

Table 1. Primary notions description

Notions	Definition
(P,K)	The user's public key, which is used to publicly identify the user in the system.
(S,K)	The private key, paired with the public key, is known only to the user.
$ID_{identify}$	A unique identifier generated for each user, based on the user's public key and other identifying information, is generated through a hash function.
INFO	Personal information provided by the user to establish a digital identity during the registration process.
SIG	A digital signature generated by the user on the information using the private key
H	Cryptographic functions

3 Methodologies

3.1 Spark blockchain

The goal of the model is to build a digital identity verification system based on Spark Blockchain, which involves a complex process of implementing identity verification on distributed ledger technology. Such systems are designed to take advantage of the immutable and decentralized nature of blockchain to ensure the security and trustworthiness of digital identities. Following items describe the procedures of used spark blockchain.

- Initialization phase: System initialization includes setting up the Spark blockchain network, creating smart contracts, and defining data structures for users and authentication. Each user's digital identity is represented by a pair of public and private keys, where the public key serves as the identity identifier and the private key is used for authentication.
- Registration phase: Users create their digital identity by submitting a registration request that includes their public key and other identifying information, including biometrics, email, etc. The smart contract verifies the submitted information, records it on the blockchain after confirming that it is correct, and generates a unique identity ID for the user.
- Authentication phase: When a user requests access to the system, they need to provide their identity ID and a digital signature generated by the private key. The system verifies the validity of the digital signature using the user's public key. If the authentication is successful, the request was indeed initiated by the user, thus completing the authentication.
- Permissions and access control: Once authentication is successful, the smart contract will determine whether the user has access to the requested resource or service based on the user's identity ID and access policy. Access rights can be dynamically adjusted based on factors such as the user's role, the context of the authentication, and more.

3.2 Smart contract

Additionally, smart contracts play a vital role in the Spark Blockchain-based digital identity verification system. They are self-executing contracts stored on the blockchain with the ability to automatically enforce the terms of the contract when predetermined conditions are met. This means that once a smart contract is deployed on the blockchain, it is able to operate independently without any third-party intervention. In the context of digital authentication, smart contracts are used to handle critical operations including user registration, authentication, access control, and rights management.

By automating these processes, smart contracts not only increase the efficiency of the system, but also enhance security and transparency, as all operations are immutable and verifiable. This automation and security are essential for building a trusted digital identity ecosystem because it ensures the authenticity and integrity of a user's identity while reducing the risk of fraud and identity theft. Smart contracts are the cornerstone

of an efficient and secure digital identity verification system, and they leverage the unique benefits of blockchain technology to provide a reliable solution. Following algorithm 1describes the execution of smart contract.

ALGORITHM 1: Smart contract for digital identify authentication

Inputs: Public Key (Purbridge), Identity Information (Edentitinver), Identity Eid (Edentide), Signature (Signa Toure)

Output: Id, whether the verification is successful

```
1function register(publicKey, identityInfo) {
2   identityID = generateID(publicKey, identityInfo)
3    blockchain.store(identityID, publicKey)
4    return identityID }
5 function authenticate(identityID, signature) {
6    record = blockchain.retrieve(identityID)
7    return verifySignature(record.publicKey, signature)}
```

4 Experiments

4.1 Experiment setups

We preparing for the Spark Blockchain-based digital identity verification system experiment, our goal was to evaluate the performance, security, and scalability of the system. This includes thoroughly testing the system using simulated user identity data, access requests, and resource information. By deploying smart contracts on the Spark Blockchain platform and using a client emulator to generate and send requests, we can measure the system's response time, throughput, success rate, and resource consumption. This comprehensive approach allows us to accurately evaluate the performance of digital identity verification systems while protecting user privacy, providing a solid basis for future optimization and improvement.

4.2 Experiment analysis

When analyzing the digital identity verification system based on Spark Blockchain, we will focus on two key technologies: symmetric encryption (SE) [11] and consensus algorithm (CA) [12], and compare their performance on different evaluation indicators through experiments. Symmetric encryption is a method of encryption in which the same key is used for encryption and decryption. This approach is used in digital authentication systems to protect the confidentiality of data, ensuring that only users with the correct keys can access or decrypt information.

The advantage of symmetric encryption is that the encryption and decryption process is fast and efficient, but its main disadvantage is the security of key management and distribution. The consensus algorithm is a mechanism used in blockchain technology

to achieve unanimous agreement between all nodes in the network. In a digital identity verification system, the consensus algorithm ensures that all transaction records and updates are correct and consistent, enhancing the security and transparency of the system. The consensus algorithm has the advantage of providing decentralized trust and an immutable record, but may sacrifice some performance because it takes time and resources to reach consensus.

We will compare the performance of symmetric encryption and consensus algorithms in digital authentication systems through two evaluation indicators, including response time and system throughput. The response time is the time it takes for the system to process the request and give feedback, and the system throughput is the number of requests processed by the system per unit of time. Following Figure 1 demonstrates the response time comparison results and the system throughput comparison results are shown in following Figure 2.

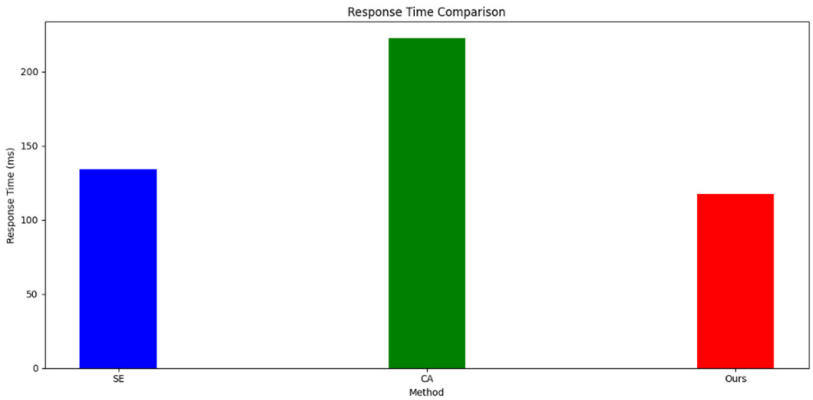

Fig. 1. System response time comparison results.

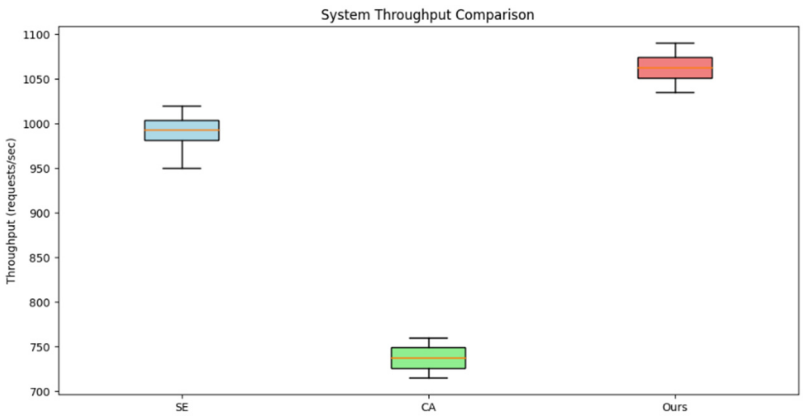

Fig. 2. System throughput comparison results.

5 Conclusion

In conclusion, the system leverages the core advantages of blockchain technology, such as decentralization, immutability, and transparency, to provide a revolutionary framework for digital identity authentication. By storing user identity information on the blockchain, the system ensures the security and integrity of the data while preventing identity theft and fraudulent activities. Furthermore, experimental analysis has shown that, compared to traditional symmetric encryption and consensus algorithms, the method based on Spark Blockchain performs better in terms of response time and system throughput. This indicates that the digital identity authentication system utilizing this technology is not only secure but also efficient in handling a large volume of requests, meeting the strict performance requirements of modern digital applications.

Acknowledgement

This work was supported by the 2018 Industrial Internet Innovation and Development Project —— Industrial Internet Identification Resolution System: National Top-Level Node Construction Project (Phase I).

References

1. Ante, L., Fischer, C., & Strehle, E. (2022). A bibliometric review of research on digital identity: Research streams, influential works and future research paths. Journal of Manufacturing Systems, 62, 523-538.
2. Sule, M. J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: issues and trends. Technology in Society, 67, 101734.
3. Yang, X., & Li, W. (2020). A zero-knowledge-proof-based digital identity management scheme in blockchain. Computers & Security, 99, 102050.
4. Masiero, S., & Arvidsson, V. (2021). Degenerative outcomes of digital identity platforms for development. Information Systems Journal, 31(6), 903-928.
5. Laborde, R., Oglaza, A., Wazan, S., Barrere, F., Benzekri, A., Chadwick, D. W., & Venant, R. (2020, January). A user-centric identity management framework based on the W3C verifiable credentials and the FIDO universal authentication framework. In 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-8). IEEE.
6. Sanni, M. I., & Apriliasari, D. (2021). Blockchain Technology Application: Authentication System in Digital Education. Aptisi Transactions on Technopreneurship (ATT), 3(2), 151-163.
7. XIE, J., LI, Z., & JIN, J. (2022). Cross-chain mechanism based on Spark blockchain. Journal of Computer Applications, 42(2), 519.
8. Kiran, G. M., & Nalini, N. (2022). SparkGrid: Blockchain Assisted Secure Query Scheduling and Dynamic Risk Assessment for Live Migration of Services in Apache Spark based Grid Environment.

9. Sánchez-Gómez, N., Torres-Valderrama, J., García-García, J. A., Gutiérrez, J. J., & Escalona, M. J. (2020). Model-based software design and testing in blockchain smart contracts: A systematic literature review. IEEE Access, 8, 164556-164569.
10. Zhong, C., Liang, Z., Huang, Y., Xiong, F., Qin, M., & Guo, Z. (2022, January). Research on cross-chain technology of blockchain: Challenges and prospects. In 2022 IEEE 2nd International Conference on Power, Electronics and Computer Applications (ICPECA) (pp. 422-428). IEEE.
11. Guerrero-Sanchez, A. E., Rivas-Araiza, E. A., Gonzalez-Cordoba, J. L., Toledano-Ayala, M., & Takacs, A. (2020). Blockchain mechanism and symmetric encryption in a wireless sensor network. Sensors, 20(10), 2798.
12. Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A., & Colman, A. (2020). Blockchain consensus algorithms: A survey. arXiv preprint arXiv:2001.07091.