Leveraging Blockchain for Trust in Digital Identity: Advantages and Implications

Zicheng Xie

xy31425523zc@outlook.com

School of Information Engineering, Sichuan Agricultural University, Ya'an, China

Abstract. Blockchain is increasingly used in various industries to provide effective solutions. The paper explores the advantages and impacts of blockchain technology on digital identity. It provides an introduction to both blockchain and digital identity technologies. The text demonstrates the technological advantages of blockchain authentication, including security, transparency, and efficiency. It also discusses the impact and advantages of blockchain's technological trust in the field of digital identity. Finally, the text summarizes future trends. The study demonstrates that blockchain technology can greatly enhance the security, transparency, and efficiency of digital identity. Additionally, technical trust based on blockchain algorithmic trust has a positive impact on the traditional trust mechanism in the field of digital identity, promoting innovation and development in this area.

Keywords: Blockchain, digital identity, algorithmic trust, technological trust.

1 Background and Significance of Research

In the digital age, digital identity is crucial for network security, verifying users in various online activities like financial transactions and social networks. However, traditional verification methods have security and privacy issues, risking theft of user information and fraud.

In modern society, trust takes the form of contract-based trust among strangers. New technologies are urgently needed to meet various needs, such as digitization and informatization. Blockchain is often referred to as a 'machine for manufacturing trust' due to its algorithmic trust mechanism [[1]]. This allows people to reach a consensus on trust based on the algorithm, which reconstructs the 'validity of the commitment'. The algorithmic operation mechanism of the traditional trust system is adjusted and supplemented by this technology. The inherent simplicity of this technology ensures controllability and stability of operation, providing advantages in terms of security and efficiency for its application in the field of digital identity.

The aim of this paper is to examine the benefits and consequences of blockchain's technological trust in the realm of digital identity. Firstly, a brief introduction to blockchain technology and digital identity will be provided. Secondly, this text demonstrates the current applications of blockchain in the field of digital identity. It discusses how blockchain can improve the security, transparency, and efficiency of identity verification, highlighting the technological trust that blockchain provides. Additionally, it examines the future development trend of blockchain identity verification, emphasizing the importance of addressing technical challenges and finding solutions.’

ICBBEM 2024, March 29-31, Wuhan, People's Republic of China

DOI 10.4108/eai.29-3-2024.2347422

In conclusion, this study aims to offer novel ideas and approaches to theoretical research in the field of digital identity. It seeks to promote innovation and application in the field and to provide a fresh perspective on understanding cybersecurity challenges.

2 Related Technology Introduction

2.1 Blockchain

In 2008, 'Bitcoin: A Peer-to-Peer Electronic Cash System' published by Satoshi Nakamoto, which describes blockchain as a distributed ledger and the core technology of Bitcoin [[2]]. This technology offers advantages in the field of electronic currency and solves the problems of 'Double Flower' and the 'Byzantine General' problem, opening the 1.0 era of blockchain. As blockchain's potential continues to be explored, its applications have expanded beyond e-money. Its decentralization, non-tampering, and anonymity features have garnered widespread attention and have been researched and applied in various fields. Blockchain is a new application model that integrates various existing computer technologies. It establishes trust between nodes at a low cost in various scenarios with multiple participants, ensuring openness and transparency of information [[3]]. After the birth of open-source blockchain platforms in the Blockchain 2.0 era, such as Super Ledger and Ethereum, blockchain applications have become increasingly extensive. It is now being applied in various fields, including healthcare, finance, and logistics, providing unique decentralized solutions to these industries. This marks the beginning of the Blockchain 3.0 era. Blockchain technology has the potential to transform the internet of information into an internet of value. Unlike traditional digital identity systems that rely on identity information in records to establish trust, blockchain uses reliable mathematical encryption algorithms to protect user privacy. It establishes trust in the network through a consensus based on algorithms, creating a technological trust system that enables peer-to-peer trust. This results in a simple, stable, secure, and efficient trust-building system.

2.2 Digital Identity

A digital identity is a description of a network entity used to authenticate a user's identity on the network [[4]]. Users hold unique digital identities in specific application services and use them to identify themselves in different applications [[5]]. As an interface be-tween users and Internet applications, digital identity has gone through three phases of centralized identity, federation-based identity, and SSI under the influence of the demand for controllability and security in the application field.

(1) Centralized identity. Centralized identity management is the most common mode of existence of the Internet, the user's identity information and operational authentication are dependent on the central agency, at the same time, different application services have different identity systems, resulting in the user's identity information in different applications can not be interoperable, so that the user needs to be submitted for different systems many times to submit identity information, which brings about the "pain of passwords "and excessive "sharing" of identity information [[6]].

(2) Federation-based identity. To address the problem of centralized identity, federation-based identity simplifies the operation within a federation by forming a federation of trusted websites.

Users enter personal information by submitting it to any member of the alliance to realize the interoperable use of this information when applying other websites or applications in the alliance, realizing single sign-on. This approach facilitates user operation and reduces the risk of information leakage to a certain extent, but the alliance-based system still suffers from security risks and insufficient privacy protection capabilities, and this trust established between third-party organizations does not give users trust.

(3) SSI. An identity verification method based on autonomous control of the identity owner improves centralized control of digital identity. This is achieved through decentralized data intermediaries and the application of cryptography, eliminating the need for a single institution or alliance. This returns ownership of identity information to the user, enabling autonomous preservation and operation of personal information and greatly reducing the possibility of identity abuse and leakage [[7]].

3 Analysis of the Technical Advantages of Blockchain Applied to the Digital Identity Field

Safety. In traditional authentication systems, if the central server fails, the entire system may become paralyzed. Blockchain technology stores data in a decentralized and distributed form across multiple nodes, reducing the risk of single-point failure. Its inerrancy forms a chain structure that ensures the security and integrity of authentication data. Any tampering destroys the consistency of the data, enhancing security and credibility compared to traditional models.

Transparency. The traditional system for identity verification suffers from non-transparency and difficult traceability, which leads to information asymmetry and a lack of trust. However, the open and transparent nature of blockchain technology allows for operations to be openly recorded, and the secure chain structure enables stable traceability. Users can independently view the details at any time, making identity verification more credible and enhancing users' trust and transparency in the system.

Efficiency. Digital identity applications should not only prioritize security but also user experience. However, traditional verification systems often hinder the service experience due to their cumbersome process. The blockchain model, which is based on the technical trust of the consensus mechanism, enables the establishment of large-scale cross-domain alliances and facilitates cross-platform operation. At the same time, multi-node distributed storage and parallel verification simplify user operations. Additionally, automated identity verification by smart contracts further streamlines the process.

4 The Impact and Benefits of Blockchain's Technological Trust in the Digital Identity Field

The blockchain utilizes a non-tamperable and traceable mathematical algorithm as credit backing, enabling organizations with different backgrounds to reach a consensus of trust. It adapts to various forms of trust and promotes objectivity. The smart contract guarantees the execution of trustworthy promises in the system, enlarging the scale of trust between trusted alliances, strengthening cooperation among all parties, and organizing small-scale peer-to-peer trust into

a systemic consensus algorithmic trust. This objective algorithmic trust enhances trust without subjective evaluations [[8]]. Based on the analysis of blockchain's technological advantages, its effectiveness and trustworthiness align with users' needs, enhancing the traditional digital identity system and increasing trust in the verification process. The use of blockchain technology is based on existing digital identity technology and the supplementation of the demand function. The technical trust of blockchain extends and improves upon early personal trust and traditional trust systems, established on effective technology that meets user needs [[9]]. The integration of blockchain technology in the digital identity system addresses its shortcomings and indicates the direction of development.

In the information age, the virtual network relies on information to create value, and user actions within this realm are built upon trust. Today's network systems rely on technical trust, facilitated by third-party credit endorsements, to safeguard security. However, centralized third-party credit endorsements often demand extensive user information, leading to vulnerabilities. This highlights the inadequacy of the old trust system. Blockchain's technical trust ensures user sovereignty over data, promoting accuracy, stability, convenience, and efficiency. Trust-building tasks are delegated to algorithms for consensus, resulting in significant cost reduction [[10]].

5 Future Trends and Perspectives

Blockchain technology is a cutting-edge cross-domain composite technology that is increasingly being used in the field of digital identity due to its ability to meet the demands for security, controllability, and convenience of identity information. As technology continues to develop in various fields, the application of cross-field blockchain will become more frequent. The flexible expansion of blockchain ensures that it remains advanced. Additionally, the platform's efficient and convenient operation meets user needs, while its data sharing function reduces the cost of building and maintaining the platform. Furthermore, blockchain-based identity authentication promises to be more secure, reliable, and cost-effective in the future. This responsible technology is expected to gain more adoption rates, demonstrating the development potential of blockchain applications [[11]].

On the other hand, blockchain can serve not only as a 'currency' representing credit in the financial field [[12]] but also establish trust between people through consensus. Algorithmic trust is a technological trust that operates through the innovation and improvement of traditional trust systems. It integrates trust relationships and bookkeeping behavior, and has the potential to become a crucial component of the social integrity systems of individuals, organizations, enterprises, and governments in the future.

The future trend of blockchain should focus on the following aspects:

(1) Scalability. The security of blockchain for businesses relies heavily on its internal use of cryptography. However, the encryption process can create a heavy computing and communication burden on the system. As the number of participants grows, the application of cryptography becomes a bottleneck that restricts scalability. Therefore, optimizing the cryptographic primitive and its application mode will be a main focus of future blockchain research to strengthen scalability. Therefore, optimizing cryptographic primitives and their application patterns will be a primary focus of future blockchain research to improve scalability.

(2) Consensus. The process of reaching consensus in the current blockchain technology requires a significant amount of computational resources. This results in a reduction of the blockchain system's throughput and an increase in system latency. Constructing a consensus mechanism to improve throughput is a major issue today. Therefore, proposing a consensus protocol that can aggregate and utilize the interaction mechanism of consensus nodes to reduce non-essential consumption and achieve high-quality energy and cost reductions is necessary to improve the security and privacy of the system in the future.

6 Conclusion

This paper examines the advantages and impact of blockchain technology on trust in the field of digital identity. It analyzes the benefits of blockchain technology in terms of security, transparency, and efficiency, and discusses its impact on digital identity. Based on existing research, it also explores future trends. Taking the field of digital identity as a breakthrough, it clarifies the adaptation of the algorithmic trust provided by blockchain to today's application trust ecosystem, and provides a new research perspective in terms of its work in constructing trust mechanisms in more fields.

The characteristics of blockchain technology, such as decentralization, non-tampering, and transparency, make it highly promising for digital identity. Its advantages in security, transparency, and efficiency can better meet users' demands for information security and autonomous control. In today's world of stranger trust, its algorithmic trust can effectively stabilize trust relationships between parties in the blockchain network of digital identity systems, including users, institutions, and enterprises. It lays the foundation for the future widespread implementation of a digital identity system, and also makes it possible to apply digital identity registration to society. The need for trust in technology will persist for a long time and extend to all areas of society. Research on the use of blockchain-generated technological trust in the field of digital identity will also have a significant impact on the development of trust mechanisms in society.

Although blockchain provides excellent technical services, it still faces challenges such as resource waste and insufficient throughput. In the future, researchers should address current issues by focusing on encryption technology, consensus mechanisms, and other related areas. Research should aim to upgrade encryption tools, develop efficient consensus protocols, and enhance configuration flexibility to maintain blockchain advancement, upgrade the digital identity system, and provide a favorable environment for users. Simultaneously, it is expected that additional research and innovation will be conducted on blockchain technology. This will allow for further exploration of the trust mechanism of blockchain and expand research horizons, ultimately advancing the technology and increasing its applicability across various fields.

Overall, blockchain technology has a significant impact on digital identity. It challenges the current verification system and presents new opportunities. In the future, research and practice will lead to a better understanding of the role of trust and the application of related technology to provide more effective services to users in the digital identity system.

References

[1] “The Promise of the Blockchain: The Trust Machine” [J]. The Economist,2015.31.

[2] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J].Decentralized Business Review, 2008:21260.

[3] Kristoffer F, David S.The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency[J]. Logistics, 2018, 2(1):2-4.

[4] MASIERO S, BAILUR S.Digital identity for development: the quest for justice and a research agenda[J].Information Technology for Development.2021,27(1):1-12.

[5] Grassi P.A., Garcia M.E and Fenton J.L.DRAFTNIST Special Publication 800-63-3 Digital Identity Guidelines[S].Gaithersburg: National Institute of Standards and Technology,2017.

[6] Weiyu Jiang, Neng Gao, Min Li. (2017). "Research on Network Trusted Identity Management Strategies and Methods." Journal of Information Security Research 3(9): 803-809. (in Chinese)

[7] Centre for Data Ethics and Innovation (CDEI). Unlocking the value of data: Exploring the role of data intermediaries[R].Centre for Data Ethics and Innovation,2021.

[8] Bohme R, Christin N, Edelman B, et al.Bitcoin: Economics, Technology, and Governance[J].Journal of Economic Perspectives,2015,29(2): 213-238.

[9] Guoqiang Hao. (2019). "From Personal Trust to Arithmetic Trust: Study of Block Chain Technology and Construction of Social Credit System." Journal of Nanning Normal University (Philosophy and Social Sciences Edition) (11).(in Chinese)

[10] Sas C, Khairuddin I E. Exploring Trust in Bitcoin Technology: A Framework for HCI Research [J]. Springer,eprint.iacr.org 2015.

[11] The Partnership on AI. Framework for promoting workforce well-being in the AI-integrated workplace[R].The Partnership on AI,2020.

[12] Litos O S T, Zindros D. Trust Is Risk: A Decentralized Financial Trust Platform [J]. Springer, eprint.iacr.org.2017.