Journal of King Saud University - Computer and Information Sciences 36 (2024) 102031

HOSTED BY

Contents lists available at ScienceDirect

Journal of King Saud University - Computer and Information Sciences

journal homepage: www.sciencedirect.com

Full Length Article

Blockchain user digital identity big data and information security process protection based on network trust

Feng Wang [a,b], Yongjie Gai [a,*], Haitao Zhang [b]

[a] School of Economics and Management, Hainan Normal University, 571158 Hainan, China
[b] Big Data Management Research Center, Jilin University, 130021 Jilin, China

ARTICLE INFO

Keywords:
Blockchain
Information security
Big data
Digital identity
Network trust

ABSTRACT

This study aims to delve into the knowledge graph, functional pathways, and qualitative logic among elements such as network trust, blockchain organization, user identity, big data, and information security in the digital economy era. Through an analysis of the endogenous and exogenous explicit management logic relationships among these elements, this study innovatively constructs three primary dimensions and nine secondary dimensions of digital identity attributes for users. Additionally, it establishes a collaborative management mechanism between government organizations and non-governmental blockchain alliances corresponding to identity attributes based on the delegated proxy mechanism. Furthermore, it reconstructs the big data chain management framework for user digital identity under the zero-trust model and establishes a management process for blockchain digital identity information security protection under the zero-trust model. These efforts provide innovative solutions with both research and application value for the "virtual-real integration" global security governance of the metaverse, digital economy, and digital government.

1. Introduction

In the era of the digital economy, blockchain users possess characteristics of multi-organizational management collaboration and synergies between digital technology and social organizational management. Especially, there exists a profound and strong linkage between big data technology and sudden public events. Consequently, in 2021, China successfully employed health QR codes based on blockchain user privacy data, as well as digital identity technology authentication management means, effectively controlling the spread of the COVID-19 pandemic, achieving remarkable global recognition. According to the release by Worldpay, a subsidiary of FIS, the global e-commerce market transaction volume exceeded $5.3 trillion in 2021, a 14 % year-on-year increase. In 2022, the digital payment transaction volume of China's import and export trade reached $372.71 billion, and by 2023, there were a total of 4.88 billion users active on social networks globally. According to the latest research data from risk prevention and solution company ClearSale Fraud Map, in the first half of 2022, the number of fraudulent orders in the Brazilian e-commerce market reached 2.8 million, with a total amount exceeding 2.9 billion Brazilian reais. A joint study by the Global Anti-Scam Alliance and data services company ScamAdviser revealed that global scams in 2021 resulted in a total loss of $55.3 billion. The "2023 Internet Crime Report" shows that various internet crimes resulted in a total loss of $12.5 billion, a 22 % year-on-year increase. Among the four largest types of network crimes causing the most economic losses in the United States (Business Email Compromise (BEC), investment fraud, ransomware technology/customer support, and impersonation of government scams), privacy breaches, information leaks, and financial fraud are all in critical areas, all related to digital identity.

With the application of digital technologies such as cloud computing, big data, and blockchain, the globalization of "Internet Plus" intelligent manufacturing and ecological industries is thriving. Digitalization is propelling the development of new forms of productive forces and high-level, high-quality value creation and management services (including remote work, secure authentication, identity recognition, digital security authorization, and crediting). The deep empowerment of digital technologies accelerates digital upgrading and transformation, drives industrial digitalization, and ensures the "virtual-physical integration" of the metaverse digital economy. In-depth research on digital security (online trust, digital identity, etc.) is of great significance for enhancing the high-quality development and application of digital currencies,

* Corresponding author.
E-mail address: 060902@hainnu.edu.cn (Y. Gai).

https://doi.org/10.1016/j.jksuci.2024.102031
Received 1 February 2024; Received in revised form 3 April 2024; Accepted 4 April 2024
Available online 9 April 2024

digital finance, smart enterprises, digital governments, and smart cities.

2. Related works

The traditional concept of information security, rooted in trust mechanisms, faces significant challenges in the era of the internet. Security information, which users rely upon, encounters immense challenges: office automation (OA), electronic government affairs, and the rise of digital economy e-commerce have transitioned directly into digital network trust models. The industrial revolution has progressed from 1.0 to the current Industry 4.0, leading to a significant reversal in societal management models due to technological advancements. The IT model of information security has undergone a cliff-like upgrade to a new theoretical paradigm of digital technology (DT). Incidents such as big data discrimination, worm viruses, and events like those involving Didi Taxi stem from vulnerabilities in digital trust and security (Wang et al., 2023), resulting in substantial losses. Digital identity serves as the infrastructure for e-commerce and mobile payments, necessitating the establishment of a completely new theoretical paradigm for digital security. This paradigm represents a binary fusion of digital technology and management (Yang, 2021), marking a new proposition for information security research under the previous purely IT support model.

Therefore, this study aims to firstly employ knowledge graphs to replace the traditional grounded theory for root cause analysis, conducting systematic and exploratory research on trust and information security. It aims to explore the endogenous logical relationships between blockchain information security and big data, organizational collaboration, information technology, identity authentication (Fu et al., 2023), and other factors. Secondly, qualitative research will be utilized for empirical analysis to uncover the endogenous mechanism elements framework of digital identity security management under the network trust model. This will address the management of digital identity security under the network trust model, exploring the mechanisms of collaboration in trust (Popa et al., 2023), technology, and information security across the digital society's government, businesses, and public sectors (Chen et al., 2024; Alhelaly et al., 2024). Finally, based on the exploratory analysis of knowledge graphs and information security, a management process for digital identity authorization, recognition, authentication, and security protection will be established.

2.1. Literature and knowledge graph analysis

Review of Literature Studies on Blockchain, Information Security, and Related Mechanisms and Frameworks: From 2000 to 2024(Fig. 1), we have examined a total of 18,988 papers from the CNKI database and 2,084 papers from the WOS database. After thorough screening, we have identified 2,230 research papers. The areas of research, keywords, and corresponding scholars are detailed in Table 1. Among these, there are

Table 1
Key Scholars and Field Keywords in Network Trust and Information Security Research.

Scholar	Field	Methods and paths
Wang Tao (2023); Li Huanhuan (2021); Liu G (2016); Cui Chuanjian (2017)	Public Information and Cybersecurity	Virtual network, multi-dimensional authentication zero trust
Zhang Yifeng (2019); Li Wenjuan (2018), Lian Yuming (2022), Ma Chao (2023)	network trust	Single sign-on and authentication
Du Jun (2023); Chen Li (2010), Liu Xun (2021)		CA/PKI/PMI application
Xu Yanhui (2023); Zhang Shunmei, Wei Shaojie (2007)		Trust Assessment BTMS Network ID
Li Yi, Feng Nan & Tan Shuncheng.(2019)		cross-domain data exchange
Khan A (2022); Gao S (2019); Li D (2017)		big data, blockchain, privacy
Li Weigang, Li Qiang (2021); Shang Kelong, Gu Qiang (2020); Wu Qi (2021)	Zero Trust Network	Dynamic Authentication, Encryption and Decryption \Zero Trust Security
Li Qiang (2016); Zhang Yq (2024)	open network	trust relationship, transitive computational model
Chen Y, Zhang K (2024); Popa M, Fu Yx, Wang L (2023)	Network trust, virtual robots	trust management model, trust measurement
Pang Jie, Tu Xuyan (2010); Xu Guangquan (2020)	Network Trust	Trust management, virtual robots
Singh M, Koprov P, Strauss S (2023); Upadhyay, S (2022)	Biometric Authentication	Face, fingerprint, iris, etc.

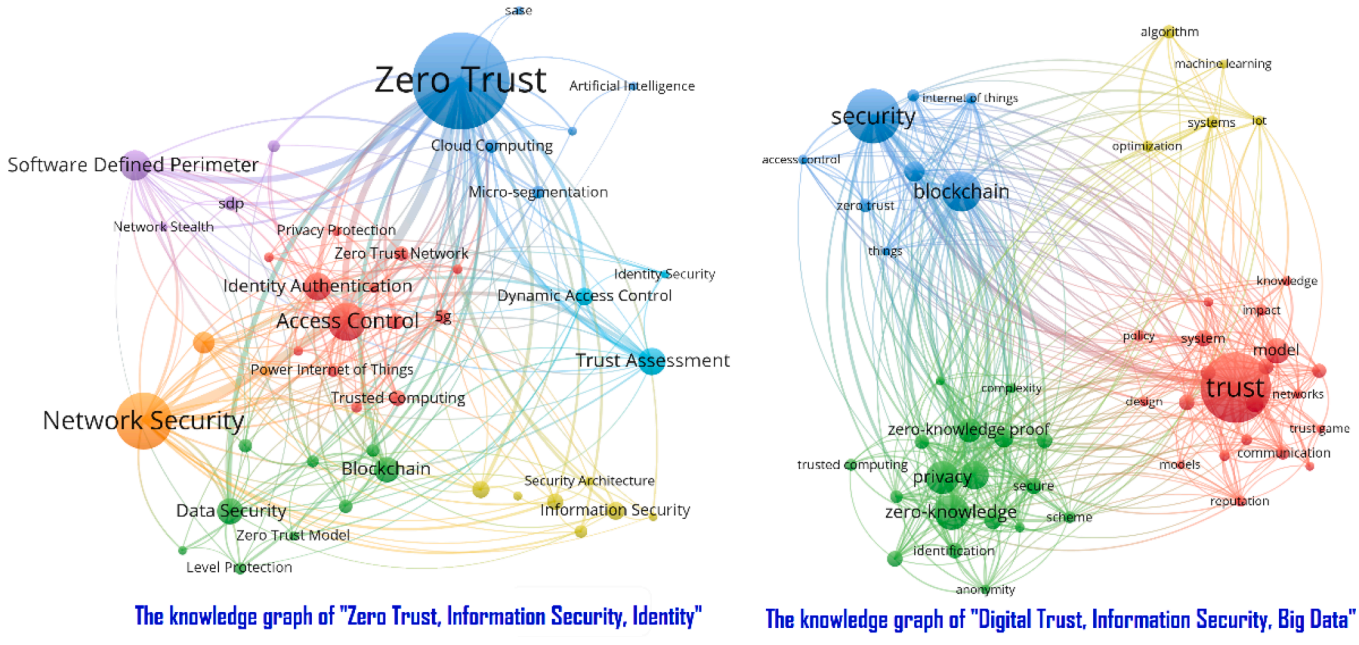

Fig. 1. Knowledge Graph Analysis of the Relationship between Trust Security and Management Framework (Data from CNKI, WOS).

294 research papers focused on digital trust, information security, and big data, while 170 papers address information technology. Notably, the proportion of research papers exploring the perspective of big data significantly surpasses those centered on information technology, indicating a clear upward trend.

Through the exploration and analysis of knowledge graphs in the fields of digital trust, information security, and big data, it can be observed that there are clear logical relationships among the dimensions of trust (zero trust), big data, smart contracts, information security, blockchain, and identity authentication (Fig. 1). Based on knowledge graphs and research literature data investigation, we constructed keywords such as blockchain trust security on WOS and other research literature, finding 5 major clusters and 20 keywords related to trust security topics. The first cluster: highlights the strong logical relationship between zero trust and access control, network security, blockchain, data security, smart contracts, and identity authentication; the second cluster: identity authentication has a strong research correlation with intrinsic security and network architecture identity authorization (Strauss, 2023); the third cluster: software protection has element-related logic with dynamic authorization, zero trust security architecture, blockchain, and IoT.

2.1.1. Information security and trust models

The social systems theory distinguishes trust into two major modes: interpersonal trust and systemic trust. Social trust includes interpersonal, institutional, digital, and network trust, among others. The earliest traditional trust systems were based on the PKI (Public Key Infrastructure) and CA (Certificate Authority) systems, which involved various encryption algorithms, keys, certification authorities, and authorization centers. However, with the digitization of society, there has been a significant shift in information security from traditional to digital modes. This transition has seen the evolution from traditional models to digitized networks and from informatization to digitalization. In the digital society, blockchain technology serves as a decentralized identity system, with trust systems built on "trust" technologies (Li et al., 2023), leveraging platforms such as the internet and blockchain to establish a "digital transaction security" model.

Traditional information security mainly concerns outward confidentiality, strategic concerns, and usability within single organizations. However, information security in the digital era encompasses data security, consensus security, privacy protection, smart contracts, and content security. In the era of information technology, traditional trust mechanisms struggle to meet the needs of digital security. Despite the proposal of blockchain 3.0, which introduces alliance constraints and security protocols spanning three organizational modes to enhance the technological level and hierarchical security control objectives of information security, large-scale data breaches, uncertainty about data rights and responsibilities, cybercrimes, network surveillance, and other threats are on the rise in the digital society. Consequently, while the level of societal network trust is gradually declining, it becomes evident that traditional information security and network trust cannot adequately address the security concerns of digital transactions.

In 2008, Satoshi Nakamoto introduced the decentralized blockchain model based on cryptographic functions like hashing. Through this innovation, a new generation of decentralized blockchain platforms integrating smart contracts for the first time fused the trust model of smart contracts (a form of digital trust model for organizational collaboration), extending blockchain digital security transactions to applications across the entire digital society (Fathalla et al., 2023; Yan et al., 2023). In 2010, prominent consulting firm Forrester proposed a novel network trust model: zero trust. In 2017, Google undertook a zero-trust security transformation of its internal network, validating the practical feasibility of the zero-trust security model in large-scale complex network environments. In August 2020, the National Institute of Standards and Technology (NIST) of the United States released the "Zero Trust Architecture," making zero-trust architecture and zero-trust networks hot topics in cybersecurity. In 2021, Forrester published a report titled "Introducing Zero Trust Edge Models for Security and Networking Services." Zero trust is a digitally driven security paradigm that continuously verifies and dynamically authorizes all users based on as many trust factors as possible, including access subject identity, network environment, and endpoint status. In 2023, the IGA released the foundational "Digital Identity Governance and Administration (IGA) Application Practice Guide" for enterprise digital identity management, business access, and next-generation security capabilities. Zero trust differs significantly from traditional security models, which evaluate entity risks through a "one-time verification + static authorization" approach (Kingo and Aranha, 2023), while zero trust builds enterprise security management on a model of "continuous verification + dynamic authorization.

2.1.2. Digital identity and blockchain

Communication scholar Hecht (1993) argues that identity typically encompasses one's origin, social status, and position. The need for identity verification is often linked to rights, obligations, and responsibilities, reflecting an individual's status, qualifications, and treatment within society. Identity carries a sense of belonging and involves conceptual relationships between an individual's social status, societal roles, and personal attributes. Identity can be determined by an individual's social and situational status, where the identity associated with social status tends to be relatively stable (typically manifesting as expertise or qualifications), while the identity determined by situational status is more variable (such as abilities, employment, or wealth). Identity can be categorized into individual identity, interpersonal identity, and group identity (Yin and Wang, 2023). Zimmerman (1998) distinguishes identity into three dimensions: discursive identity, situational identity, and portable/accompanying identity.

The development of digital identity has transitioned from traditional paper-based identity to electronic information. With the advancement of internet technology, the scope of digital identity applications has expanded, evolving from simple login authentication to multi-factor authentication and biometric technologies, reflecting the evolving demands for authentication and advancements in information technology. With both domestic and international internet giants and emerging tech unicorns entering related industries, new technological paradigms such as Web3.0 and the metaverse are sweeping across the globe. Decentralized Identity (DID) is gradually gaining prominence, with the concept proposed by companies like Microsoft in 2015. In 2019, China established the Citizen Digital Identity Promotion Committee, where digital identity becomes an individual's second form of identification, and the Ministry of Public Security conducted research and development on network electronic identity (elD) technology and related standards systems. Business alliances provide blockchain-based digital identity solutions, such as "Verified" by Secure Key Technologies, "My Security Key Technologies" by R3 Corda Enterprise, and solutions built on open-source platforms like Life and Sovrin. Major technology vendors like IBM and Samsung are actively participating in blockchain-based digital identity initiatives. In March 2020, the Financial Action Task Force issued the "Digital Identity Regulatory Guide" to address money laundering issues.

Currently, the most prominent digital identity models revolve around blockchain-based digital identity systems, widely utilized for granting, managing, and verifying digital identities. Additionally, cross-chain technology plays a role in the digital identity field, facilitating interoperability and security of identity information by connecting different blockchain systems (Wang, 2023). The digital identity of blockchain users is explored through big data artificial intelligence models and biometric technologies, utilizing facial and fingerprint data for digital authentication: the digital identity model = "organizational management collaboration system + big data management + DT technology", enhancing the construction of two major trust systems for digital identity and blockchain big data circulation (Du et al., 2023). DID

systems built on blockchain possess characteristics of data authenticity, user privacy protection, and strong internet digital portability (Labati et al., 2023.).

2.1.3. Security algorithms and biometric recognition

Artificial intelligence technology has gradually become one of the most popular topics in today's society. The unique advantages of artificial intelligence play an increasingly important role and bring huge business opportunities in various fields such as healthcare, finance, education, and transportation. The artificial intelligence algorithm library provides security measures such as data encryption (Upadhyay et al., 2023), identity authentication, and access control. Data security encryption algorithms include not only AES, RSA/ECC, Diffie-Hellman, SHA-1/SHA-256, but also quantum cryptography, homomorphic encryption algorithms (fully homomorphic, partially homomorphic, and semi-homomorphic), multiparty computation cryptographic techniques, cellular automaton cryptography (Suhaimin et al., 2023), and so on. Artificial intelligence in the field of information security also includes biometric recognition, vulnerability detection, malicious code analysis, and many other aspects. In particular, biometric authentication and access control are the most successful areas of application in information security technology. Artificial intelligence technology centered on deep learning has greatly improved the accuracy of natural person identification using biometric technologies (Zhang et al., 2021) such as face, iris, voiceprint, palmprint, and vein recognition, with face recognition achieving an accuracy rate of up to 99 %. The Generative Adversarial Networks (GAN) proposed by Goodfellow et al. (2014) is currently one of the best methods for generating models. Using GAN for image generation relies heavily on the strong fitting ability of neural networks. Its performance in the field of biometric recognition is excellent. In visual tasks, GAN includes approximately 20 application models such as Pix2pix, Cycle-GAN, Disco-GAN, D2GAN, ACGAN, SRGAN, SeGAN, Perceptual GAN, etc. The application of GAN to improve network trustworthiness has vast research potential (Capocasale and Perboli, 2022; Zhang et al., 2024).

2.2. Analysis and summary

2.2.1. Summary of literature analysis

Through knowledge graph analysis, it is observed that 92.5 % of international research institutions focus on the network nature of blockchain and information security technology, while 7.5 % of research institutions concentrate on social management science, indicating a typical phenomenon of heavy emphasis on technology and light management.

There are three hotspots and innovative areas in digital identity and information security. Firstly, the security model of blockchain information data flow incorporates elements such as big data, user authentication, digital identity, and data key encryption. Network trust, digital identity, and zero trust exhibit strong correlations in the first cluster analysis, with the mainstream adoption of asymmetric encryption ECC security algorithm under the blockchain smart contract model. Secondly, core algorithms in blockchain information data exchange security, such as information anchoring, homomorphic encryption, edge computing (particularly in big data privacy aspects), information encryption algorithms, and anti-counterfeiting protection, dominate the mainstream hotspots. Thirdly, blockchain artificial intelligence technology: cloud computing and edge computing paradigms are widely applied through public and open-source code repositories and tools.

2.2.2. Current research gaps

Artificial intelligence is regarded as an advanced productive force with significant socio-economic benefits, but it also involves various crisis issues: national cybersecurity, confidential leaks, social privacy security, etc., including some ethical issues and major frauds, such as AI deepfake videos, voice impersonation, AI fraudulent transactions, financial account intrusion viruses, etc. There are many research gaps in network trust, especially in information security and digital identity authentication under the zero-trust model:

Firstly, in the digital age, data security still relies on the knowledge system and research theoretical paradigm of information security encryption. Network trust is mostly limited to the trust links of traditional single organizations and user account information links. Data islands and data rights issues lead to the loss of user information dominance, making cross-domain financial transactions and unified digital identity authentication extremely difficult. Thus, the foundation of information security will inevitably be shaken.

Secondly, there is a strong causal relationship and logical connection between network trust and information security, which is a major issue currently overlooked by many scholars. How network trust is transmitted and functions in the digital society, the dynamic and intermediary elements involved, and the discovery of inherent mechanisms and relationship frameworks are crucial for solving issues related to globalization of industrial chain upgrading and transformation, digital economy, major epidemic events, and other digital management aspects. Cross-domain digital network trust lacks digital trust coordination and correlation mechanisms among government, enterprises, and individuals.

Thirdly, the problem of blockchain information security theoretical paradigm. Although the blockchain security system appears relatively complete, in reality, blockchain information security is still in its infancy. Its security mechanisms have many shortcomings and defects: firstly, current blockchain research belongs to the information mode (information encryption, IT information theory-driven), and blockchain organizational research forms avoid the subdivision functions of government organizations, being overly singular and not adequately considering trust and cooperation relationships across industries and economic entities, and non-governmental organizations, such as corporate organizations, government finance, civil affairs, industry and commerce, legal and other national institutional organizations, virtual management functional organization, etc., hence smart contracts belong to the marginalized P2P mode, lacking third-party trust supervision mechanisms, leading to many cases of credit fraud in blockchain finance. Secondly, blockchain information security belongs to the social application mode of digital or big data, surpassing information technology and belonging to the architecture of big data digital management, with identity authentication and key security algorithms lacking user big data security management. Mainstream research on blockchain information security still follows the traditional digital algorithm mode of "ID number + password," with 99 % of projects lacking digital identity authentication, making it difficult to have a comprehensive digital knowledge system, thus it is difficult to be widely promoted and applied. Lastly, information security lacks cooperation and correlation with blockchain social and intergovernmental organizations, and research on digital identity loses its commercial value, and its application and promotion lose development space.

Fourthly, the lack of research on trust delegation and security agency services. In the era of big data, information asymmetry leads to IT outsourcing services, resulting in data islands, information islands, and stimulating management loopholes. Many users' data rights are monopolized and abused by software developers. Therefore, digital security transactions and payments lack third-party network trust delegation agents, risk warning, and other systemic integration and integration, especially social digital governments, enterprises' basic big data lack effective sharing, openness, and interface mechanisms, which are clearly related to third-party service developers, and the lack of many digital functional correlation studies also leads to management loopholes, thus information digital security lacks effective security trust supervision organizational services, and digital security will inevitably be filled with anomalies!

Fifthly, the problem of digital identity organization coordination and authentication. Government departments and "flying governments"

both have a significant influence on identity management. Blockchain trust solves the problem of credibility of online network natural persons, but it does not solve the problem of "virtual and real integration" of offline real identities, which is the current issue of information security and digital identity research. Although digital identity technology has made significant progress, it still faces many challenges, such as privacy protection, authenticity verification of dynamic identities, collaboration management mechanisms of government and "flying government" organizations, and cross-chain identity authentication problems.

In the realm of cybersecurity, blockchain-based organizational collaboration and the digitized process collaboration of functional elements (such as big data identity, organizational management contracts, information technology inheritance, dynamic identity authentication, secure privacy encryption, etc.) are involved. To achieve this, it is imperative to conduct exploratory research to dissect the digital drivers and mechanisms of managing network trust and information security. Utilizing information security and network trust elements, we explore the mechanisms of IT technology regulation and management intermediary integration, systematically analyze the intrinsic mechanisms of information security elements, conduct root cause management system analysis, establish a research management framework model, thereby enriching the theoretical paradigm of digital information security research. Scientifically customizing the digital relationship and trust security endogenous mechanisms of blockchain information security is conducive to enhancing and improving the interdisciplinary knowledge system, ensuring the healthy development of digital intelligence transformation and upgrading.

3. Hypotheses & methodology

3.1. Conceptual-theoretical model

Traditional information security models include information flow models, grid environment security information models, and the Role-Based Access Control (RABC) model that defines information flow policies; all of which are information technology models within a single organizational entity. However, for practical blockchain information security management, considerations must extend to issues such as organizational collaboration, trust, security levels, identity roles, etc. This is especially crucial given the heterogeneity of blockchain organizations, the hierarchical authorization of information, the dynamic encryption and decryption algorithms, and the impact of organizational environmental security collaboration.

The Technology Acceptance Model (TAM) explores the joint determinants of perceived usefulness and ease of use on behavioral intentions. Scholars' in-depth exploration of trust theory has revealed that trust not only directly influences behavior but also fosters cooperative relationships within societal behaviors such as production and consumption, banking transactions, security management (Wu and Pei, 2022), etc. Furthermore, individual behaviors indirectly facilitate the development of user big data and can also exert indirect effects by influencing risk and security perceptions. Novelty based on knowledge and trust among internet consumers can help reduce perceived risks and enhance security awareness, thereby indirectly influencing internet security behaviors.

Expanding upon the TAM model, we introduce the NOPI(Network trust, Organizational collaboration, Personal big data, Information technology) model, where these four dimensions are pivotal variables. We investigate the roles and impact mechanisms of each element within the blockchain information security management system. This model (Fig. 2) provides deeper insights into the mechanisms of digital identity security within blockchain information, thereby contributing to the refinement of both research theoretical paradigms and management frameworks in digital information security.

3.2. Basic hypothesis

H11: Network trust has a positive effect on user Big Data

Social network trust plays a crucial role in mitigating the challenges of user big data scarcity and addressing the issues of "new users" and "new projects" within recommendation systems. Through big data analytics, personalized services and recommendations can be provided, leading to heightened user satisfaction and trust in network services. This perception of personalized and efficient service fosters increased trust in the platform (Taylor and Dargahi, 2020). The inherent virtual nature of cyberspace, coupled with the uncertainties surrounding user identities and behaviors, forms the foundational framework of network trust systems. The application of big data analytics helps in identifying potential risks and threats such as fraudulent activities and cyberattacks. By continuously monitoring and analyzing vast amounts of data, issues can be promptly detected and preventive measures implemented, thereby enhancing network trust. Furthermore, the encryption techniques employed in handling big data can significantly boost privacy and security protection, contributing to the establishment and

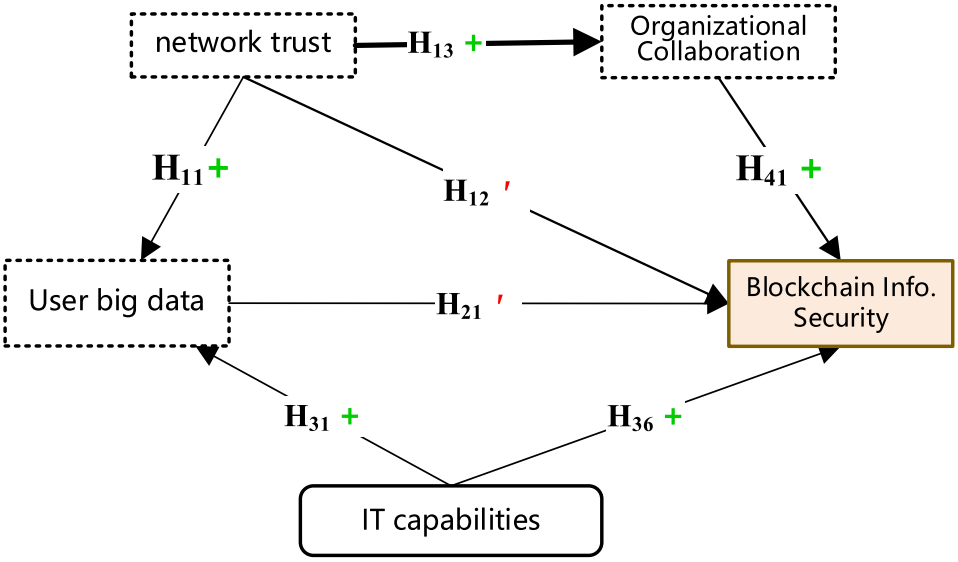

Fig. 2. Exploratory concept of NOPI model for blockchain.

maintenance of network trust, and subsequently reinforcing public trust in institutions. eID, leveraging algorithms like homomorphic encryption, provides privacy protection within the user big data environment (Dehghani and Ghiasi, 2021; Saxena et al., 2022), thereby fortifying the safeguarding of user information rights in network trust. Zero trust architecture presents a novel approach to network trust representation, establishing dynamically trusted secure access platforms to ensure the security and trustworthiness of subject-object business and data access.

H12: Network trust has a negative effect on blockchain information security

From a sociological perspective, the division of labor and the explosion of knowledge compel networked individuals to adapt to a complex knowledge network environment. Earle et al. (1995) attempted to obtain a simplified and rapid management model, benefiting from the ever-increasing opportunity costs, presenting a collaborative, contractual, agency, and delegation of individual and environmental organization. From a psychological standpoint, networked individuals aspire to establish a belief system that is honest, trustworthy, and reliable, achievable through cognitive and identity-based psychological processes. From an institutional perspective, administrative, governmental, and national political trust is the mainstream trust model of society (Berdik et al., 2021), while the fundamental approach to eliminating network political skepticism lies in governmental action. From an economic standpoint, network trust is essential for public market identity within the networked economy, while blockchain is built on the virtual, open, interactive, and decentralized nature of the internet, necessitating individuals to establish trust in unfamiliar organizations. In the digital society, it is transitioning from an information management model to a digital intelligent management model. Online trust is challenging, with numerous vulnerabilities and process pitfalls in digitalized corporate offices (Almakhour et al., 2022), and proxy psychological expectations formed by advertising, celebrities, experts, and market spokespersons easily masking significant insecure fraudulent behaviors. Additionally, uninformed merchants utilizing app proxies exacerbate the trust deficit, leading to a significant risk to blockchain information security.

Traditional cybersecurity assurances protect enterprise network boundaries, trusting within default boundaries. However, the emergence of new technologies and applications such as cloud computing, the Internet of Things (IoT), and mobile offices, along with digitized business processes, cloudification of resources, and decentralized big data, blur the boundaries between internal and external networks, leading to a plethora of security incidents and significant economic losses. Hence, borderless and zero-trust network security architectures are imperative. In conclusion, the risks associated with network trust incline towards over-reliance on technology, technical flaws leading to risks overflow, privacy breaches, legal and regulatory loopholes, and societal acceptance risks. New economic and management IT models may influence the stability of network trust.

H13: Network trust has a positive influence on Organizational collaboration

In the ecological development of social organizations, on one hand, network trust relationships can condense and stimulate the innovation and entrepreneurial drive of social organizations, optimizing team collaboration and resource allocation (Lumineau et al., 2021). On the other hand, complex platform organizations face increasingly severe platform governance challenges, with ecological conflicts continually erupting, and the uncertainty of innovative behavior rising. Therefore, encouraging participants to adopt network trust relationships, seeking symmetrical or balanced relationships, can help mitigate losses caused by blurred organizational boundaries, complex coordination, and competition.

H21: user Big Data has a negative impact on blockchain information security

User big data encompasses not only personal big data but also government big data, mobile communication big data, enterprise salary big data, and so forth (Aggarwal et al., 2021). These data are generated under the digital twin mode of intelligent terminals and sensors. The exponential growth of user big data directly impacts the security of privacy, life, property, etc., and even jeopardizes national and social security (e.g., national geographic information big data). Accompanied by the lack of self-protection awareness among individual subjects and the loss of data rights, the unlimited amplification of user app big data, along with excessive development, collection, leakage, and misuse, allows illegal information service providers and hackers to exploit for criminal activities. As the digital economy becomes increasingly interconnected, entering a period of explosive growth, information security issues are becoming more prominent, especially as blockchain information security faces unprecedented challenges (Alketbi et al., 2020).

H31: IT capability has a positive effect on user Big Data

Big data has become a crucial factor in the development of information-based societies, representing not only an inevitable product of information development but also a new stage of informatization (Han et al., 2019). In 2019, China issued the "Data Security Management Measures," which outlined the relevant standards and specifications for the collection, processing, utilization, and secure supervision of personal information and necessary data. The formulation of unique data security laws and personal information protection laws is a primary objective of informatization capability (Zhang et al., 2020). Under the requirement for confidentiality of user big data information, emerging IT technologies such as anonymization, smart contracts, encryption (Lykidis et al., 2021), etc., are expected to undergo significant development and undoubtedly find broader applications in the construction of big data sharing platforms (Liu et al., 2019).

H36: IT capabilities have a positive effect on blockchain information security

The transition of blockchain from 1.0 to 3.0 represents another new information revolution following internet technology. Xiang Hui (2020) believes it has made significant contributions in pandemic emergency management, industry applications, digital currencies, and other areas (Aggarwal and Kumar, 2021). Its applications have extended to every corner of society. According to Duan Siqi (2021), from the virtual economy to the entire spectrum (electronic information storage, copyright management and transactions, product traceability, digital asset transactions, Internet of Things, smart manufacturing, supply chain management, etc.), all rely heavily on the robust support of information technology capabilities (Alvi et al., 2022; Ahamad et al., 2022).

H41: Organizational Collaboration Has a Positive Impact on Blockchain Info. Security

Collaborative governance refers to cross-sector cooperation and joint governance between governments and other organizations, where multiple actors from public and private institutions jointly formulate, implement, and manage rules (Zhang et al., 2021). In 2007, the "Emergency Response Law of the People's Republic of China" proposed a emergency management system of "state-led, comprehensive coordination, classified management, and territorial management." Resource sharing and supply chain scheduling in emergencies, especially facilitated by big data information sharing, promote collaboration among various subsets. Government emergency organizations act as collaborative structures and core nodes in emergencies (Kouhizadeh et al., 2021). Organizations face numerous challenges such as supply chain visibility, process standardization, supply chain coordination and collaboration issues, and global disruptions. The functions of social organizations play a crucial role in systemic, policy, and collaborative governance theory aspects (Rathee and Singh, 2022).

3.3. Research design

3.3.1. Research object and data sources

The widespread digitization of social information security involves several elements such as digital identity policies, systems, and organizational collaboration. It constitutes a typical pain point in social domain management and belongs to interdisciplinary fields. It is

difficult to solely rely on computer technology to find answers directly. Therefore, it is necessary to not only investigate and interview IT experts but also consult IT management advisors. To achieve this, we employed three methods: interviews with IT experts, enterprise surveys, and online questionnaires, totaling 330 distributed. After excluding large-scale missing data, non-professional responses, and invalid data, we were left with 309 valid questionnaires, with an effective rate of 93.64 %. Characteristics of the respondents in this survey are as follows:

Job Type Distribution: IT Information Director 5.53 %, IT Development Engineer 46.25 %, IT Consultant Expert 14.56 %, Enterprise Senior Management Expert 6.84 %, Financial Investor 8.47 %, Computer Science Postgraduate 28.34 %; Gender Distribution: Male 74.81 %, Female 25.19 %; Educational Background Distribution: Doctorate and above 18.35 %, Master's degree 48.04 %, Bachelor's degree and below 44.60 %; Age Range: Over 50 years old 11.97 %, 30–50 years old 49.62 %, Below 30 years old 38.41 %.

Descriptive parameters were applied to questionnaire items across various dimensions: mean, standard deviation, skewness, and kurtosis. Statistical data indicate that skewness and kurtosis fall within a reasonable range, conforming to a normal distribution, suitable for subsequent analysis.

3.3.2. Reliability analysis

Internal consistency reliability analysis employs Cronbach's α as a reliability indicator. The analysis results indicate that the Cronbach's α values for each item range between 0.66 and 0.81. After deletion, α values range from 0.832 to 0.937, indicating that all items are worth retaining. The α coefficients for each dimension range from 0.863 to 0.942, exceeding 0.7. Therefore, the survey questionnaire in this study demonstrates good reliability.

3.3.3. Effectiveness analysis

(1) Exploratory Factor Analysis

Viewing the results of exploratory factor analysis from a top-down perspective, the Kaiser-Meyer-Olkin (KMO) value is 0.924, and Bartlett's sphericity test yields significant results (approximate chi-square: 6616.633; degrees of freedom: 595.000; significance: 0.000). This indicates that the data meet the prerequisites for exploratory factor analysis. Using the principal component method to extract factors, it is observed that five factors have eigenvalues greater than 1, cumulatively explaining 65.901 % of the variance. The scree plot flattens after the sixth factor, suggesting that five factors should be extracted (6–1) = 5. After extracting five factors, rotation is conducted using the maximum variance method. The results show that all items belong to their respective dimensions, exhibiting significant factor loadings and minimal cross-loadings with other dimensions. Thus, the questionnaire used in this study demonstrates good construct validity.

(2) Analysis of Deterministic Factors

Building upon exploratory factor analysis, confirmatory factor analysis of the scale-type measurement tool was conducted using AMOS 26. Composite reliability (CR) and average variance extracted (AVE) for each dimension were calculated based on standardized factor loadings. If CR > 0.7 and AVE > 0.5 (convergent validity), the measurement dimensions exhibit good convergent validity. The results (Table 2) indicate that all fit indices of the model meet the corresponding standards, indicating a good overall model fit.

Additional scrutiny was applied to assess the factor loadings, revealing (Table 3) standardized factor loadings spanning from 0.691 to 0.837, CR values ranging from 0.863 to 0.943, and AVE values falling between 0.549 and 0.650, all satisfying the requisite standards. Consequently, the questionnaire data demonstrates commendable convergent validity.

Table 2
Model variable fit.

Fit index	Critical value	Current value	Result
Chi-square		561.578	
Degrees of freedom		550	
Chi-square/Degrees of freedom	<3	1.021	√
RMSEA	<0.1	0.008	√
GFI	>0.9	0.911	√
RFI	>0.9	0.912	√
NFI	>0.9	0.919	√
IFI	>0.9	0.998	√
TLI	>0.9	0.998	√
CFI	>0.9	0.998	√

3.3.4. Structural validity analysis

The construct validity of the model data includes convergent validity and discriminant validity. In the testing method for discriminant validity, the square root of the AVE of each dimension is compared with the correlation coefficients and other dimensions. The results indicate that the correlation coefficients between any two dimensions are smaller than the square root of the AVE of each dimension itself (bold diagonal numbers), as shown in Table 4. Therefore, it is demonstrated that there is sufficient discriminant power among different dimensions, and concepts can be well distinguished.

3.3.5. Construct validity

The gender, occupation, industry, educational background, and job position of the survey respondents are included in the analysis as control variables for their significance in understanding network information security. The main variables (Table 5) involved in moderating effect analysis are centralized to reduce the impact of serial effects.

3.3.6. Correlation analysis

By calculating the average of each dimension to obtain scores, and using these scores for descriptive statistics and correlation analysis, we will obtain the results of dimension scores (Table 6), facilitating descriptive statistics and correlation analysis of the NOPI model.

3.3.7. Moderation analysis test

According to the regression statistics (Table 6), the hypothesis validation is correct, that will prove: this hypothesis of NOPI model is confirmed (Fig. 3).

Based on the above correlation analysis on the dimensions of the NOPI model of the Blockchain and the results of the Moderation Analysis Test between dimensions (Table 5, Table 7), it is proved that the logical relationship of NOPI model (Fig. 3) is significant and influential.

3.4. Analysis of NOPI results

The NOPI model presents a pivotal and innovative framework for the establishment of a novel network trust paradigm. Supported by cutting-edge technologies like big data, zero-trust digital collaboration, and structural governance, it furnishes a scientifically efficient management structure for digital identities. User data permeates diverse digital landscapes of heterogeneous blockchain alliance entities, including direct-operated entities of governmental bodies (e.g., the Ministry of Health, Ministry of Public Security, Ministry of Education), government-delegated agents, and non-governmental entities operating under smart contracts (such as communities, banks, hospitals, police stations, enterprises, universities, and technical associations). At the heart of this ecosystem lie the intelligent contract data-chain relationships forged through user network trust and digital identity technologies. Digital trust encompasses secure connections and biometric authentication within various blockchain organizational processes. The overarching aim of this framework is to bolster the precision of user digital identity authentication, ensure the traceability of digital transactions, and foster

Table 3
Confirmatory factor analysis (standardized).

Dimensions	Measure variable		Loading	Z	p	SMC	CR	AVE
Name	Value Name	abbr.						
Network **t**rust	Administrative mode	Nt1	0.821	17.208	<0.001	0.674	0.918	0.650
	Contract mode	Nt2	0.796	16.412	<0.001	0.634		
Nt	Co-parasitic mode	Nt3	0.800	16.523	<0.001	0.640		
	Proxy model	Nt4	0.804	16.653	<0.001	0.646		
	Cognitive model	Nt5	0.824	17.282	<0.001	0.679		
	Zero-trust full verification	Nt6	0.793	16.309	<0.001	0.629		
Organizational **C**ollaborationOc	Open resource data	OC1	0.749	14.558	<0.001	0.561	0.863	0.558
	Alliance organization	OC2	0.766	15.036	<0.001	0.587		
	Criterion collaboration	OC3	0.729	14.032	<0.001	0.531		
	Management collaboration	OC4	0.747	14.498	<0.001	0.558		
	Business collaboration	OC5	0.744	14.432	<0.001	0.554		
User big dataUbd	Basic data	Ubd1	0.814	17.146	<0.001	0.663	0.943	0.646
	Identity data	Ubd2	0.817	17.251	<0.001	0.667		
	Household registration	Ubd3	0.789	16.385	<0.001	0.623		
	Asset data	Ubd4	0.796	16.601	<0.001	0.634		
	Transaction data	Ubd5	0.808	16.958	<0.001	0.653		
	Location data	Ubd6	0.785	16.244	<0.001	0.616		
	Medical data	Ubd7	0.792	16.467	<0.001	0.627		
	Employment data	Ubd8	0.794	16.537	<0.001	0.630		
	Social Security Data	Ubd9	0.837	17.917	<0.001	0.701		
Blockchain **i**nfo.	Info. Security Governance	BiS1	0.765	15.201	<0.001	0.585	0.880	0.549
SecurityBiS	Security Risk Assessment	BiS2	0.726	14.113	<0.001	0.527		
	General Security Management	BiS3	0.731	14.251	<0.001	0.534		
	Information system upgrade	BiS4	0.727	14.148	<0.001	0.529		
	Security Process Management	BiS5	0.739	14.462	<0.001	0.546		
	IT technology innovation	BiS6	0.757	14.967	<0.001	0.573		
IT capabilities	Data collection security	ITc1	0.771	15.667	<0.001	0.594	0.920	0.561
	Information data sharing	ITc2	0.762	15.417	<0.001	0.581		
	Security algorithm	ITc3	0.715	14.092	<0.001	0.511		
ITc	IT process management	ITc4	0.771	15.670	<0.001	0.594		
	network security protocol	ITc5	0.754	15.197	<0.001	0.569		
	User privacy includes	ITc6	0.758	15.288	<0.001	0.575		
	Accurate ID authentication	ITc7	0.691	13.471	<0.001	0.477		
	Cost efficiency	ITc8	0.740	14.793	<0.001	0.548		
	Intelligent decision	ITc9	0.774	15.763	<0.001	0.599		

Table 4
Discriminant Validity.

Variable term	1	2	3	4	5
1. User Big Data	**0.804**				
2. Network trust	0.296	**0.806**			
3. Organizational collaboration	0.173	0.357	**0.747**		
4 .Blockchain Info. Security	−0.274	−0.254	0.182	**0.741**	
5. IT capabilities	0.215	−0.053	0.110	0.382	**0.749**

Note: The bold numbers on the diagonal of the table are the square root of the average variance extraction ($(\sqrt{AVE})$) of the corresponding dimension, and the off-diagonal numbers are the correlation coefficients between dimensions.

Table 5
Correlation or Moderating Relationship of Dimensional Elements in NOPI Model.

Test variables	Tested	Statistics	Correlation (+or −)	Significance conclusion
Nt	Ubd	B = 0.292, t = 5.231, p < 0.001	Correlation +	√
Nt	OC	B = 0.316, t = 5.687, p < 0.001	Correlation +	√
ITC	Ubd	B = 0.265, t = 4.090, p < 0.001	Correlation +	√
Nt	BiS	B = −0.175, t = −4.138, p < 0.001	Correlation −	√
OC	BiS	B = 0.184, t = 4.610, p < 0.001	Correlation +	√
Ubd	BiS	B = −0.220, t = −5.393, p < 0.001	Correlation −	√
ITC	BiS	B = 0.306, t = 6.526, p < 0.001	Correlation +	√
ITC	ITC → Nt	B = −0.068, t = −1.369, p = 0.172	Moderating −	√
ITC	OC → BiS	B = 0.134, t = 3.875, p < 0.001	Moderating +	√
ITC	Ubd → BiS	B = 0.204, t = 6.130, p < 0.001	Moderating +	√
ITC	Nt → Ubd	B = 0.015, t = 0.407, p = 0.685	Moderating −	√

Note: + stand for positive − Stand for negative.

secure data sharing (Yanhui and Muzhe, 2020). Additionally, it encourages digital organizations to prioritize business digital interconnectivity and network collaboration. Furthermore, the NOPI model underscores the imperative of comprehensive research into blockchain information security, advocating for interdisciplinary integration and development across critical facets like big data, identity authentication, network trust, smart contracts, organizational collaboration, and digital transformation (Zhi et al., 2022). Such integration promises to expedite breakthroughs and innovative advancements in blockchain big data information security.

Zero Trust is a focal point in the realm of network trust research, with digital identity emerging as a pivotal research avenue for blockchain-driven Zero Trust security governance (Wang and Shan, 2020). This field is poised to initiate the digital management and simulation of digital twins, facilitating integrated intelligent management encompassing organizational collaboration in the digital society, secure governance of e-commerce transactions, and blockchain-based identity authentication for bolstering digital trust. This endeavor aims to recalibrate the network trust model of digital identity.

Within the Zero Trust paradigm, digital identity, underpinned by big data technology, stands poised to reshape the landscape of digital social

Table 6
Descriptive statistics and correlation analysis.

variable term	M	SD	1	2	3	4	5
1. Network trust	3.153	0.815	1.000				
2. Organizational collaboration	3.166	0.831	0.316**	1.000			
3. User Big Data	3.191	0.839	0.273**	0.155**	1.000		
4. Blockchain Info. Security	3.030	0.716	−0.226**	0.162**	−0.249**	1.000	
5. IT capabilities	2.959	0.713	−0.048	0.097	0.204**	0.340**	1.000

Note: The bold numbers on the diagonal of the table are the square root of the average variance extraction ($(\sqrt{AVE})$) of the corresponding dimension, and the off-diagonal numbers are the correlation coefficients between dimensions.

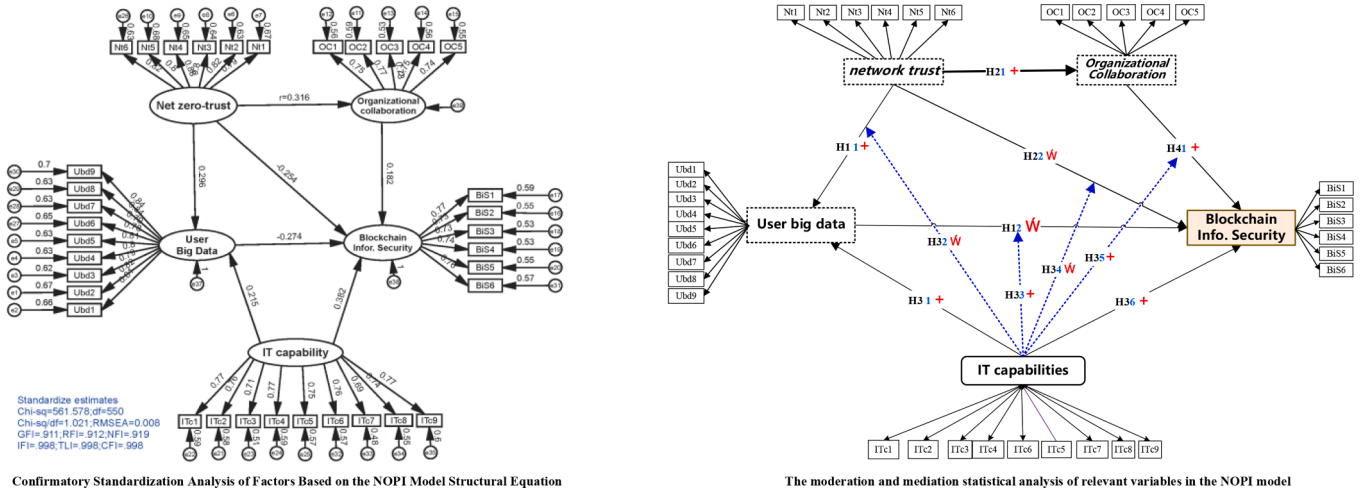

Fig. 3. Confirmatory factor analysis (standardized).

management (Saqib et al., 2022). It will catalyze secure, open sharing of resource data among blockchain consortium organizations (comprising government, enterprises, communities (Davis, 1989), etc.), thereby reshaping industrial Internet digital industry platforms and fostering the evolution of socially engaged commercial smart logistics supply chain platforms. This strategic maneuver seeks to augment the international competitiveness of industries.

The digitization journey of enterprises, cities, and societies hinges upon the seamless integration of big data technology and the management of digital identity. Consequently, within the digital trust model, process management of digital identity promises to furnish blockchain consortium organizations with robust technical frameworks and innovative management strategies, fostering network collaboration, smart contracts (Udokwu and Norta, 2021), and value co-creation.

4. Identity security authentication and process

4.1. Principles of digital identity trustworthiness

National government agencies (15 in the United States and 26 in China) empower the fusion authentication of citizens' digital and real identities, which is essential for ensuring the security of blockchain digital identities and is a foundational infrastructure for reshaping the core organization of digital social security.

Trusted identity platforms are applied in various scenarios such as e-government, e-commerce, internet finance, online education, etc. In e-government, users can utilize the CTID platform for online transactions, governmental services, public services, etc (Greulich et al., 2024). In e-commerce and internet finance, users can conduct online payments, transfers, financial management, etc. In online education, users can use the CTID platform for online learning, examinations, etc. The Digital Transformation Office (DTO) of Australia released the "Trusted Digital Identity Framework" (TDIF) in January 2021, aimed at facilitating governments, businesses, and individuals to exchange information and verify identities more securely and efficiently in the digital world. It provides convenience for the development of the digital economy and society and can be widely applied in fields such as e-government, e-commerce, internet finance, online education, etc. SingPass is a trusted digital identity for every resident of Singapore and serves as a platform connecting over 700 government agencies and private sector services. From checking provident funds to renewing insurance and even digitally signing documents, it enhances the efficiency of digital services. The United Nations ID4D initiative calls for joint efforts from governments, businesses, and civil society to promote interoperability and standardization of digital identities (Esposito et al., 2020).

Therefore, summarizing the goals, functions, and features of trusted digital identity management, the trustworthiness of digital identity follows these principles:

1) Covering citizens comprehensively across all levels, possessing inclusivity and expansiveness.
2) Identity possesses identifiability and recognizability.
3) Reflecting the characteristics of citizens' qualifications, abilities, rights, obligations, etc.
4) Fully covering various data elements of citizens' identities that can be audited and authorized.
5) Suitable for societal digitization and refined management, achieving authenticity and reliability.
6) Digital identity possesses real-time, dynamic, perceptual, authentic, authoritative, mobile, sensitive, and privacy-preserving characteristics.
7) Serving the national objectives and goals.
8) Complying with scientific management mechanisms of trust delegation and smart contracts.

Table 7
Regression analysis for Organizational collaboration, Blockchain Information Securities, and IT capabilities.

Variable	M1		M2		Variable	M3		M4		M5		Variable	M6		M7		M8	
	B	t	B	t		B	t	B	t	B	t		B	t	B	t	B	t
constant	−0.567	−1.472	−0.362	−0.983		−0.18	−0.451	0.110	0.295	0.101	0.273		3.086	9.256***	3.189	11.210***	3.394	13.130***
gender	0.136	1.409	0.107	1.170	gender	0.131	1.338	0.074	0.794	0.079	0.854	gender	0.112	1.345	0.088	1.236	0.045	0.701
IA	−0.012	−0.109	−0.029	−0.270	IA	−0.076	−0.661	−0.081	−0.749	−0.080	−0.748	IA	0.071	0.731	0.078	0.946	0.039	0.527
IF	−0.026	−0.261	−0.047	−0.494	IF	0.064	0.628	0.039	0.407	0.046	0.475	IF	−0.036	−0.411	−0.010	−0.134	−0.032	−0.480
AR	0.091	1.646	0.079	1.508	AR	−0.035	−0.612	−0.04	−0.761	−0.038	−0.723	AR	−0.026	−0.538	−0.040	−0.981	−0.061	−1.668
Edu	0.082	1.500	0.078	1.497	Edu	0.004	0.080	−0.01	−0.189	−0.012	−0.233	Edu	0.002	0.043	−0.027	−0.679	−0.041	−1.128
Jt	−0.024	−0.585	−0.027	−0.683	Jt	0.003	0.070	0.002	0.057	0.000	−0.010	Jt	0.019	0.529	0.029	0.955	0.036	1.312
CI	0.025	0.439	0.006	0.114	CI	0.012	0.206	−0.02	−0.347	−0.022	−0.391	CI	−0.063	−1.253	−0.075	−1.759	−0.088	−2.278
												Nt			−0.172	−3.690***	−0.175	−4.138***
												Oc			0.209	4.663***	0.187	4.610***
												Ubd			−0.267	−6.043***	−0.220	−5.393***
												ITc			0.375	7.432***	0.306	6.526***
					Nt			0.293	5.228***	0.292	5.231***	**ITc × Nt**					0.015	0.407
					ITc			0.252	3.927***	0.265	4.090***	**ITc × Oc**					0.134	3.875***
Nt			0.316	5.687***	**ITc × Nt**					−0.068	−1.369	**ITc × Ubd**					0.204	6.130***
R^2	0.024				R^2	0.01		0.129		0.134		R^2	0.016		0.306		0.438	
			0.119															
F	1.062				*F*	0.447		4.899***		4.609***		*F*	0.715		11.888***		16.387***	
			5.069***															
ΔR^2					ΔR^2			0.118		0.005		ΔR^2			0.289		0.133	
			0.095															

Note: *p < 0.05, **p < 0.01, ***p < 0.001, two-tailed test. Variable abbreviation as follows:
IA = Industry attributes; IF = Internet fraud;AR = age range; Edu = Education; Jt = Job type; CI = Cybersecurity Importance;Nt = Network trust;OC = Organizational collaboration;Ubd = User Big Data;BiS = Blockchain Information Securities; ITc = IT capabilities.

4.2. Identity structure and authentication institutions

Digital identity must be governed by national legal constraints as the guiding principle; monetary, financial, and regulatory government credits as the criteria, and social rights (civil affairs: marriage, elderly care, medical insurance, etc.), responsibilities (judicial: elections, self-governance, etc.), and obligations (business: tax payment, employment) as the binding relationships. Therefore, the government is the stable ballast and foundational identity function authority in the economic development of the digital age. Non-governmental organizations and enterprises and institutions also have a significant impact on identity (Khan, 2022; Nazir et al., 2024; Haiou, 2014). These organizations, through their respective functions and activities, jointly shape the identities of individuals and enterprises in society and exert a significant influence on them. This includes international organizations such as the United Nations (UN), the World Bank, the International Monetary Fund (IMF), etc., which operate globally and have an indirect impact on the policies and identity management of member countries. Authentication and standardization institutions such as the International Organization for Standardization (ISO), IBM, the Big Four accounting firms, etc., whose certifications and standards have a significant impact on the professional qualifications and service capabilities of enterprise products and practitioners. Others include industry associations and chambers of commerce, educational institutions, professional associations, and labor unions, etc. Simon points out that identity analysis needs to consider three levels: the micro level, the macro level, and the meso level. With the help of the above analysis, we summarize the three major attributes of identity (Table 8).

4.2.1. Basic attributes

Basic attributes include personal foundational big data: foundational data (age, gender, birthday, ID number, etc.), marital status, family members, place of residence (linked to property residence). Basic attributes belong to the foundational determination attributes of citizens. Most of the foundational identity data attributes are dynamic and environmental attributes, especially marital status and family members (changes due to birth and death) (Yuanpei, 2020).

Identity basic attribute data association process: includes birth, establishment, update, and elimination. Birth institutions include: hospitals, health commissions, and household registration offices jointly reviewed; marital status update institutions (courts, civil affairs bureaus, police stations) (Berawi and Sari, 2021; Wang et al., 2022; Lykidis et al., 2021), family members by marriage registration offices, hospitals, crematoriums, police stations; place of residence by real estate offices, police stations, etc.

4.2.2. Public attributes

Public attributes (Table 7) usually have specific identity attributes under the constraints and protection of national laws. The state endows citizens with rights and obligations that are relatively stable as long as they do not violate the law (Runze, 2021). Therefore, public attributes are often prone to loopholes due to inadequate supervision and inability to update in a timely manner, leading to fraud incidents, such as: tax attributes, tax attributes reported by enterprises, audited by tax bureaus and industrial and commercial bureaus, because personal income big data cannot be supervised, enterprises also conceal and disperse individual incomes, leading to inadequate supervision by industrial and commercial, tax departments, causing frequent tax evasion incidents (Jiahui, 2020).

4.2.3. Private attributes

The private attributes of identity typically reflect personalized and privacy-sensitive characteristics. The private attributes of identity are usually formed through individual efforts, exhibiting personalized differences that carry social recognition. These differences mainly manifest in two major attributes: employment (social labor) and social

Table 8
Digital Identity Attributes, Authentication Institutions, Authorized Agencies, and Review Institutions.

ID Elements	Attribute	Authentication Institution	Authorized Agency Organization	Review Institution
Basic Attributes	Household Registration	Ministry of Public Security	Police stations, etc.	Hospitals, civil affairs depar., Public Security, Discipline Inspection Commission, company, Public Security, Courts, Judiciary, etc.
Public Attributes	Political participation	State Council	CPPCC, government, community, etc.	
	Healthcare	Ministry of Health	Health Department, hospital, company, etc.	
	Education	Ministry of Education	Education Bureau, university, etc.	
	Residence	Ministry of Housing and Urban-Rural Development	Real Estate Bureau, etc.	
	Taxation	Ministry of Finance	Tax Bureau, banks, etc.	
	Military Service	Military Service	Ministry of National Defense	
Private Attributes	Scientific Research	Science & Technology Ministry, HR Ministry, Finance Ministry, Administration for Industry and Commerce, Tax Bureau, etc.	Academic institutions, HR Department, Education Ministry, Medical Insurance Bureau, hospitals, financial companies, banks, courts, etc.	Courts, Discipline Inspection Commission, Public Security, etc.
	Work			
	Entrepreneurship			
	Investment			
	Social: Driving	Ministry of Transport/ Tourism/Public Security, etc.	Police stations, courts, travel agencies, vehicle administration bureaus, banks, etc.	
	Social: Transport			
	Social: Tourism			

interactions (private life consumption, etc.). The employment attribute includes four types: scientific research (academic research institutions), employment (enterprises and institutions), entrepreneurship (start-up companies), and investment (financial investments) (Wang and Jiyan, 2017). Due to its personalized characteristics, private attributes possess a certain level of concealment, making it difficult for social public organizations and certification agencies to obtain real-time access. Various review and regulatory agencies are prone to information asymmetry due to cross-industry collaboration, cumbersome processes, and complexity, which easily lead to loopholes and exploitation, resulting in counterfeiting and fraudulent incidents (Alketbi, 2020). For example, an investor's investment attribute may lead to bankruptcy and loss of investment capability due to debts or crimes. Verification agencies (banks, financial institutions, public security, courts, etc.) require significant time to determine and provide evidence, leading to delays in publicly disclosing societal information. As a result, other criminals take advantage of the situation to continue their activities, while victims fall into new traps due to the inability to obtain real-time information on the identity attributes of fraudsters (Tiancheng, 2021).

4.3. Digital identity security audit

The framework for the digital identity structure of users in the digital society comprises four parts. First, there are the trusted identity management attributes. Second, there are authoritative organizations capable of proving the reliability of identities, which carry out digital authorization and audit, confirmation, and other management tasks for citizen identity attributes (Zhang et al., 2022). Third, due to the dynamic changes in citizen identity attributes, there are third-party organizations capable of conducting real-time dynamic audits. Fourth, because of information asymmetry, especially the distributed nature of organizations confirming all identity elements, the audit and update of identities require the digitalization, processual interconnection(Fig. 4), integration, and collaborative management of all organizations to ensure reliability, security, timeliness, and precision, ensuring the scientific and efficient dynamic audit and authentication of identities (Bradatsch et al., 2023).

The authoritative organizations for identity determination are scattered throughout various corners of society. Therefore, based on the blockchain management model and blockchain consortiums, they are

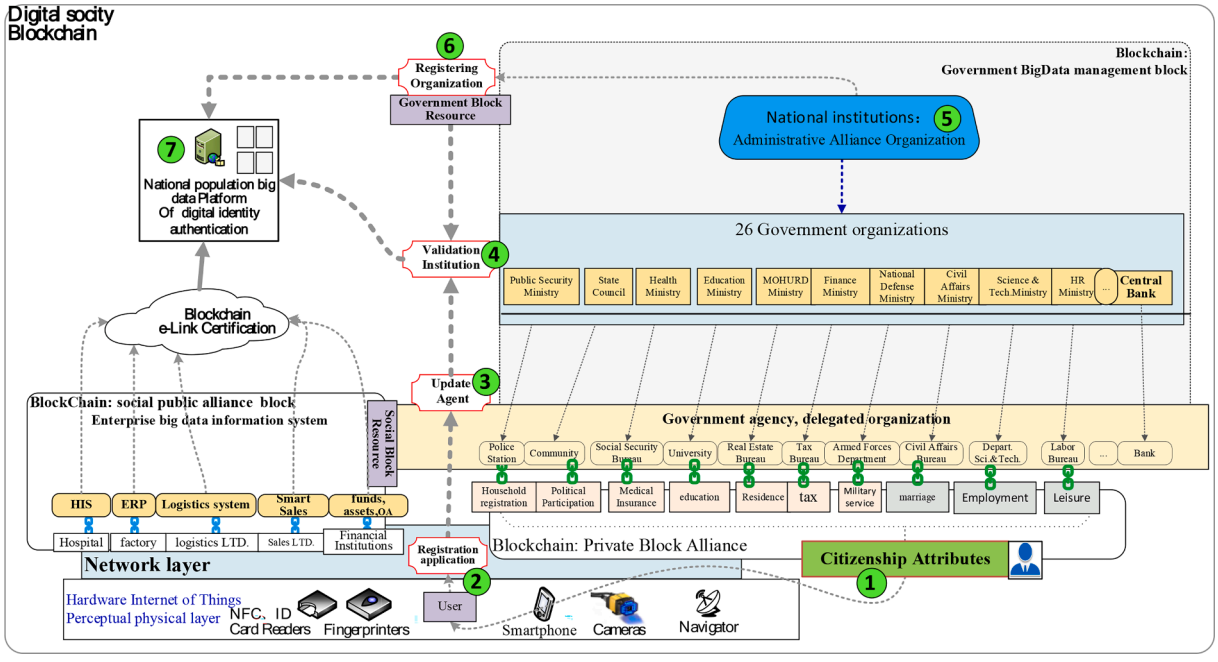

Fig. 4. Zero Trust Blockchain Dynamic Management and Audit Mechanism for Digital Identity.

divided into three main parts:

(1) Blockchain Consortium of National Administrative Organizations: China has established 26 first-level administrative organs of the State Council, including the Ministry of Public Security and the Ministry of Health. Following the delegation and agency system of national functions, this structure is gradually extended to six levels: province, city (municipality directly under the central government), county, district, town, and village (Fig. 4) (Jq, 2021). These are the core state institutions for citizen identity authentication and also include a six-level judicial supervision review and approval mechanism. Due to the digital divide and IT outsourcing services, state institutions issue digital identity management strategies and policies, which are then handed over to the administrative blockchain consortium for the digital release of identity management. IT supply development organizations and vendors are tasked with the integration and construction of the blockchain-based big data platform for digital identities.
(2) Blockchain Public Consortium for Social Public Services and Management: This consortium is composed of research institutions, medical facilities, academia, financial institutions, and IT companies. It supports the digital identity process services for society and is related to organizations such as universities that provide citizens with educational qualifications and professional capabilities (teacher qualifications, technical consulting, and other professional skills) (Zhaohui, 2021). The public blockchain consortium is responsible for submitting, auditing, and updating the authentication of digital identities. It may even use digital collection and algorithmic IT systems provided by IT development vendors to audit and determine changes in user identity information, carrying out identity attribute changes, and pushing for online network integration, publication, and sharing.
(3) Family Private Blockchain Consortium: This consortium is the provider of big data information for digital identities, taking on the change, collection, and perception of digital identities. Through apps or digital system interfaces provided by the IT development supplier consortium, it facilitates the creation, alteration, and update applications of identity information attributes.

4.4. Zero trust dynamic security mechanism

4.4.1. Zero trust principles

Zero Trust is a security model whose core management principles are based on the concept of "never trust, always verify." Here are some key management principles of the Zero Trust model:

Default Deny: In the Zero Trust model, any unverified access request should be denied by default. Only users, devices, or services that have undergone rigorous verification should be granted access to resources.

Least Privilege Principle: Users, devices, or services should only have the minimum set of privileges necessary to accomplish their tasks. This means that even if users or devices are granted access, they can only access resources necessary for their work or functionality (Zhaohui, 2021).

Identity-based Access Control: Access control decisions should be based on the identity of users, devices, and applications rather than on network location. This means that regardless of whether users are on the internal network or external network, they need to go through an authentication and authorization process.

Continuous Monitoring and Assessment: The Zero Trust model requires continuous monitoring and assessment of all network traffic. This includes real-time monitoring of user behavior, device status, and network activities to promptly detect and respond to anomalies.

Dynamic Security Policies: Security policies should be dynamically adjusted based on the real-time status of users, devices, and applications. For example, if abnormal user behavior or device infection is detected, their access permissions should be adjusted immediately.

Micro-Segmentation: Networks should be segmented into multiple secure zones or micro-segments to restrict the ability of attackers to move within the network. Each micro-segment should have its own security controls and access policies.

Encryption: All network communications should use encryption technologies to protect the confidentiality and integrity of data. This includes data in transit (e.g., via VPN-SSL) and data at rest (e.g., data stored on servers).

Multi-Factor Authentication: To enhance security, users should be required to provide multiple authentication factors such as passwords, biometrics, or security tokens when accessing sensitive resources.

Automation and Integration: The Zero Trust model should leverage digital technology tools and integrated security solutions to streamline management processes, improve response times, and reduce human errors.

User and Device Education: Organizations should educate users and device administrators about the importance of Zero Trust principles and provide necessary training to ensure they understand and comply with relevant security policies and practices (Safi et al., 2022).

4.4.2. Zero trust security management mechanism

Zero Trust authorization is relatively complex, primarily involving: access subject identity attributes and authorization operations, access object attributes, and delegated proxy authorization policies. Access authorization mandates that all access must be authorized by an access controller before accessing application systems or other resources. Complex authorization is based on element granularity to construct dynamic security policies (Fig. 5):

(1) Technical Validation: Security authentication in the user's privacy domain (such as AI identity algorithms, technical recognition, etc.), login access detection and control of big data provisioning devices (USB, PC clients, apps, etc.), SSL channel access control of professional VPNs, sensitive information protection of user identity attributes (collaborative authorization encryption of delegated proxy agencies, anti-copying of sensitive data, etc.), and construction of digital identity platform technology architecture. Digital identity utilizes digital twinning, biometric AI technology, and big data technology to construct personal identity 3-dimensional attribute big data (Table 8) platforms (Liu et al., 2023). User identity verification is based on the qualification verification of the user's primary identity attribute information data. Therefore, zero-trust blockchain digital identity integrates security protection and attribute update processes to ensure the integrity, dynamism, and timeliness of digital identity across the entire big data realm (Bicer et al., 2023; Zhou et al., 2015). Residents with legitimate identity qualifications undergo digital identity registration, and new IT technologies are used to AI model personal biometric big data such as fingerprints and faces, followed by secure encryption and authentication using digital algorithms, before issuing digital electronic credentials, authentication templates, and identifiers for electronic verification and identity comparison.
(2) Identity Identification: Accessing subject users are given unique identifiers within the determined boundaries of the system, addressing the issue of user identity attribution.
(3) Identity Verification: Utilizing blockchain big data to verify the existence of smart contracts and determine the validity of user identity, permissions, qualifications, and capability status features.
(4) Identity Authorization: Obtaining identity authorization, permissions, qualifications, and other specifications from the blockchain big data digital identity platform to determine which resources users can access and the operational permissions for

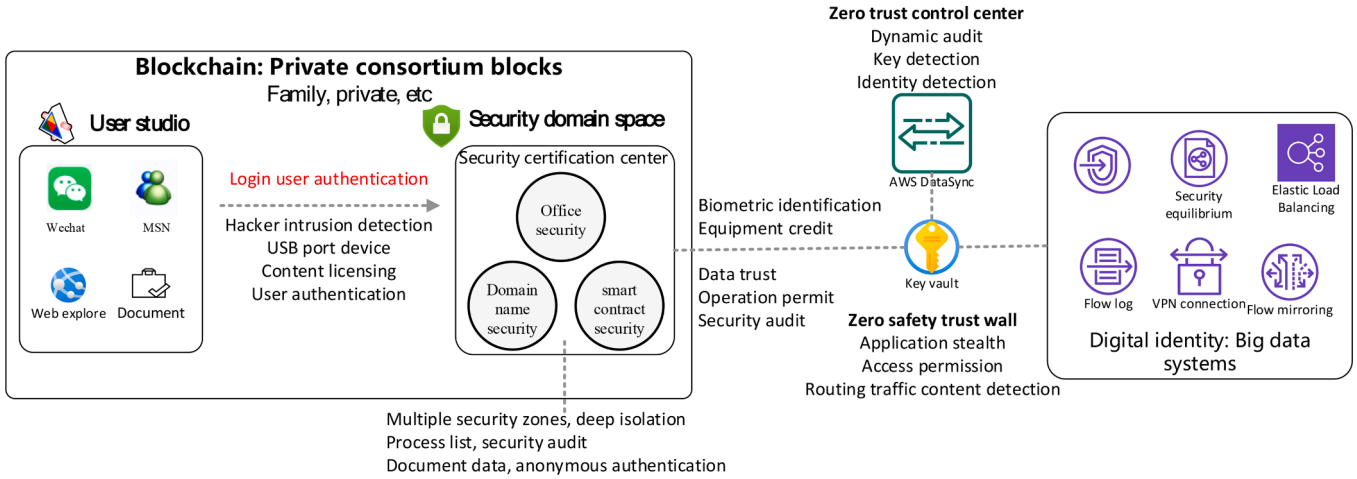

Fig. 5. Zero Trust Blockchain Digital Identity Space Security Strategy.

resources (read, write, delete, etc.), resolving user business content authorization.

(5) Audit Records: Archiving user access behavior records for subsequent accountability or system improvement.

4.4.3. *Digital identity security collaborative mechanism*

The concept of zero trust enables a fully dynamic and real-time digital authentication of all elements. Numerous user events (such as career transitions, changes in family members, and violations) cause variations in identity attributes at different levels. In the digital era, the digitization of these events, along with the real-time updating mechanism of digital twins, replaces IT information silos and IT management paradoxes. Digital twins form ten types of big data chains of user identity (such as household chains, family member chains, and maternal-child chains) (Fig. 6). Big data technology drives the collaboration of blockchain consortiums, making it possible for blockchain organizations to collaboratively ensure the timely updating of identity big data attributes under smart contract mechanisms. This is the engine behind the collaborative management and business convergence mechanisms of blockchain organizations. Digital twins trigger changes in user identity and application for push services. Intelligent agents of digital identity push change requests to proxy service agencies of blockchain public consortium organizations for identity change verification. Subsequently, based on the validation of government administrative consortium blockchain organizations, identity agent approval is submitted to the national population digital identity big data platform, ensuring the timeliness, legitimacy, and authority of digital identity information, thus achieving the management of identity changes and updates across the entire Internet.

5. Information security protection process

Zero trust digital identity possesses seven characteristic attributes: trustworthiness, uniqueness, attribution, validity, dynamism, effectiveness, and specificity. Under the Internet mode, the zero trust digital identity authentication mechanism meets the management coordination of departments such as household registration, social security, industry and commerce, civil affairs, achieving risk elimination and verification security for the seven major characteristics of user identity. Therefore, blockchain digital identity integrates big data IT technology and the collaborative protection of blockchain alliance organizations, matching the following principles:

The organization of blockchain digital identity constructs smart contracts for the collaborative update of identity information, completing the real-time creation, updating, improvement, and publication of primary background identity big data after identity

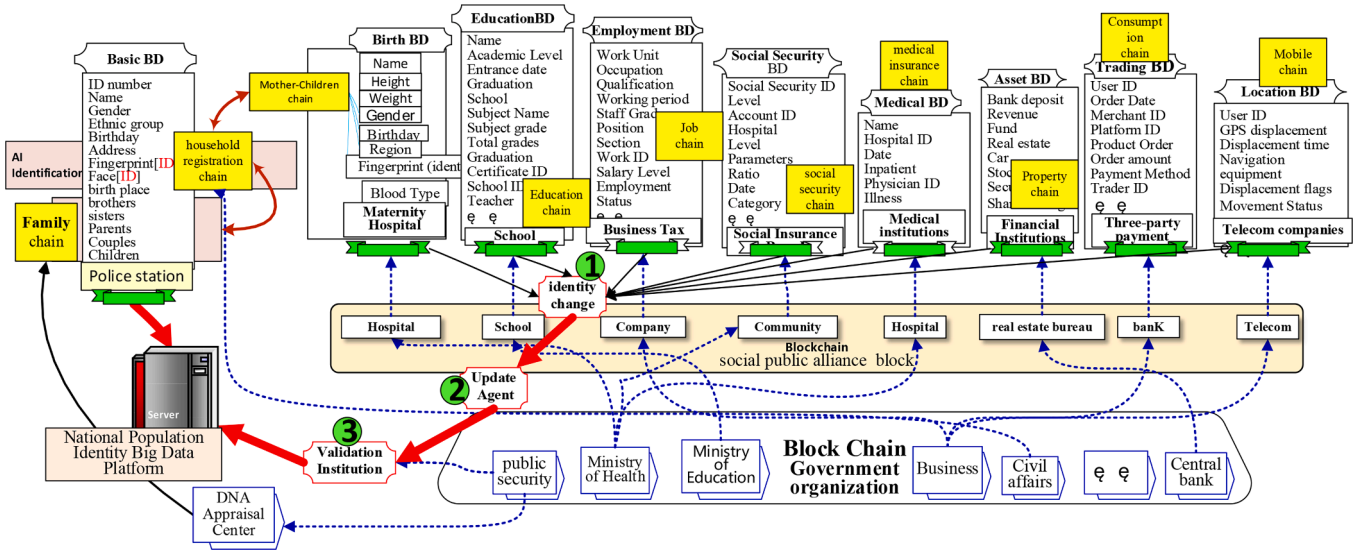

Fig. 6. Enhancing User Digital Identity Management in Big Data Chains through Blockchain Organizational Collaboration.

authentication, and does not allow expired or useless identity information data to exist.

Blockchain user data meets information perception, with a certain objective CPS physicality, with an identification rate of <0.0001 %.

Accurate real-time identity authentication should be true, immediate, and unique. Fingerprint or facial biometric recognition AI technology can uniquely match applicants with the big data population database template, ensuring that on-site applicants can successfully pass one-to-one identity consistency tests with the national population database, with a rejection rate of <0.0001 %.

Blockchain information should have security classification, authorization classification, and effective domain authorization.

Anonymous automatic authentication requires dynamic high-strength encryption algorithms and high-strength security authentication, adopting dynamic algorithms and dynamic key mechanisms, rejecting SSO password mode links to avoid the risk of brute force attacks.Zero-trust high-intensity blockchain information security typically requires establishing three security protections (SSL-VPN encrypted channels, encryption and decryption protection processes with dynamic key mechanisms, automatic identification and authentication of digital identities), with digital identity anonymous authentication referring to the utilization of user biometric features for digital vector modeling, replacing traditional password authentication, to conduct dynamic key and real-user on-site comparison recognition, enhancing security. Thus, based on the zero-trust user digital identity, the blockchain anonymous dynamic information security protection process is as follows:

5.1. Establishing digital identity database

National Ministry of Public Security is mainly responsible for building the block chain population digital identity database: first, large personal identity data, mainly providing digital identity AI intelligent recognition model based on user's fingerprint, face, DNA and other data, and opening and sharing to the public at different levels according to their access rights. Second, the Cyber Physics data provided by employment companies, social security, assets, education and other institutions related to personal qualifications and abilities (such as qualifications, academic qualifications, credit, legal and other abilities), these related enterprises and institutions are entrusted by the State to provide applications for alteration in user identity data. These institutions need to abide by the contractual commitments: to ensure that the identity information is true and effective, and modification submitted is in qualifications.

5.2. Establishing SSL-VPN network channels

Remote Secure Access Channel SSL-VPN is based on the Secure Socket Layer (SSL) protocol, which provides secure access to the digital channel for blockchain applications.

5.3. Public plain text data

Social organization generates unencrypted data: PubText (Fig. 7-(3)).

5.4. Blockchain user digital identity authentication

The user's actual fingerprint or 3D dynamic real-world face image data is compared with the data of the national population record (Fig. 7-(4)), which can identify the user on-site and the template user in the national population database for comparison and identification: the real identity "person – card" comparison and identification, the process is as follows:

First, the Ministry of Public Security will establish a nationwide foundational household registration big data for digital population identity (including user facial and fingerprint image model data). Blockchain public consortium organizations will verify and update other attribute big data, initiate periodic process audits, and incorporate additional attribute big data of user identities into the blockchain big data platform. In the blockchain big data platform, user identity card attribute data will be associated with digital images such as faces and imported into the user identity standard library database. Simultaneously, utilizing AI techniques such as Faster R-CNN for facial

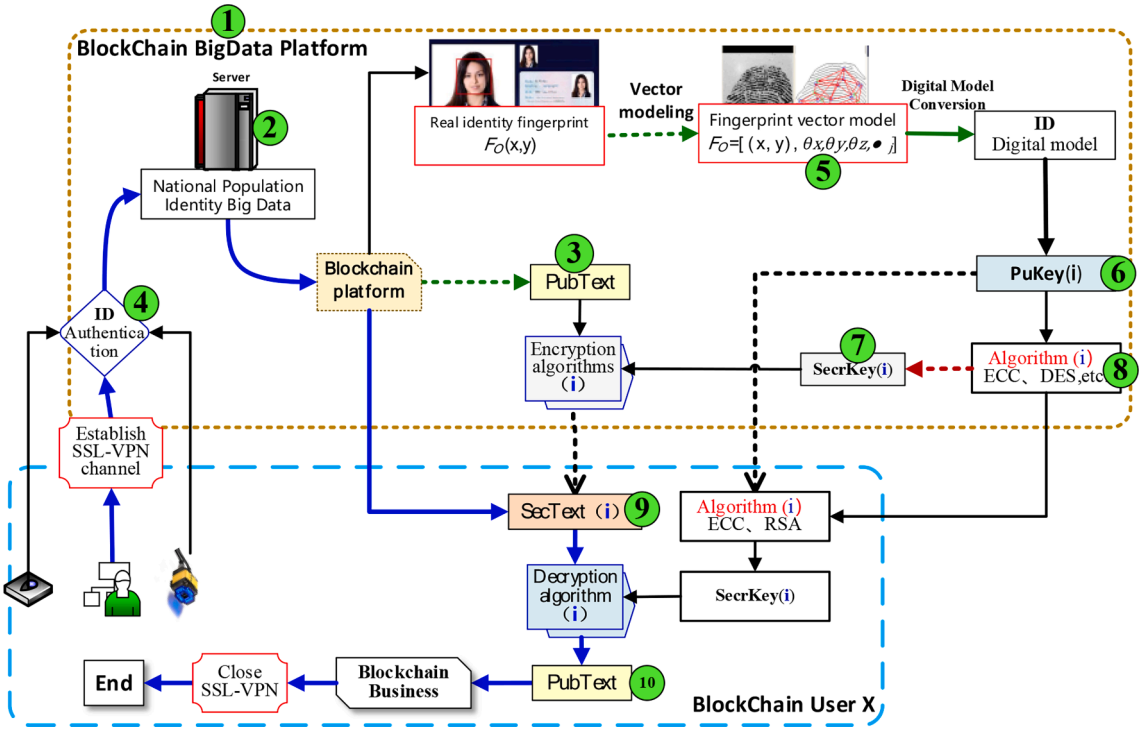

Fig. 7. User Big Data Zero-trust Digital Identity Blockchain Security Process.

localization and identifying key facial landmarks (such as eyes, nose, and mouth), an identity mapping model will be established. Additionally, 3DMM (Three-Dimensional Morphable Model) learning will be employed for modeling, utilizing dataset Pdata(x) to generate Blockchain's 3D facial template images in DB(x).

Second, integrating specialized scenarios, harnessing complex large-scale datasets to train advanced facial recognition models. Employing a cascaded CNN technique with 3DMM model for progressive parameter regression analysis, ensuring accurate localization of facial landmarks. Synthetic data generated by the model serves for 3D deep learning and calibration, catering to scenarios like side profiles and closed-eye recognition.

Third, the remote devices, such as smartphones and computers, are utilized to capture real-time user facial images denoted as Gd(z). These images serve as three-dimensional contextual auxiliary information for cached data P(z).

Finally, the generation of the adversarial GAN network data and the determination results. Gd and Db in Equation (5) represent the neural network's user template digital identity image and the actual face image taken in real life. z refers to the input Gd network noise training template graph, E refers to the mathematical expectation, x refers to the real image and y (target image).

Db() refers to the network training to learn to generate a Db(x) image to represent the probability that the network will determine whether the image is actual or not. The equations for the loss functions of Dd and Gd are shown below.

3DMM learning modelling was used to generate a DB(x) template map of the 3D face of Blockchain with the data set Pdata(x){Fd_{model}, At_{model}},Representation of Each User's Textured 3D Facial Model Using Digital Modeling Formulas:

$$Fd_{model} = \mathrm{Fd}^2 + \sum_{i=1}^{m-1} \alpha_i \, \mathrm{Fd}_i \tag{1}$$

$$At_{model} = \mathrm{At}^2 + \sum_{i=1}^{m-1} \beta_i \, \mathrm{At}_i \tag{2}$$

Fd: facial Average Shape and At: average Texture Sections,Fd^2 and At^2 represent the average shape and average texture components of the face, which are the core of the 3DMM. They represent the linear combinations of discriminative facial features, sorted in descending order of eigenvalues of the covariance matrix. Fd^2 and At^2 respectively denote the eigenvectors of the covariance matrix according to the facial feature values. The distributions of these two sets of coefficients follow $p(\alpha)\ \exp[-\frac{1}{2}\sum_{i=1}^{m-1}(\alpha_i/\sigma_i)^2]$, where σ_{i} is the eigenvalue of the shape covariance matrix. α and β follow a multivariate normal distribution.

The equations for the loss functions of Dd & Gd respectively are:

$$Loss(Db) = -Ex\ Pz[Db(x)] + Ex\ Pz[Db(x)] \tag{3}$$

$$Loss(Gd) = -Ex\ Pz[Db(x)] \tag{4}$$

Gd(z) and the template library Db(x) are fed into the CNN algorithm for circular iterative matching. If Gd(Db(z)) = 0.5, then the equation for comparison verification can be interpreted by Mathematical Formula (5).

In order to produce a noticeable comparative effect on user facial features, train a conventional GAN model to have the discriminator network (Db) judge whether the real user's face matches the effect of the generator function's image. The determination of whether the result is a real human face image is expressed by the following formula (6).

$$\min_{Gd}\ \max_{Db} V(Db, Gd) = E_{x\ Pdata(x)}[logDb(x)] + E_{z\ P_z(Z)}[log(1 - Db(Gd(z)))]. \tag{5}$$

$$Disc_{gan}(Gd, Db) = E_y[logDb(y)] + E_{x,y}[log(1 - Db(Gd(x, z)). \tag{6}$$

Then calculate the facial recognition result based on the process (Fig. 8) and equation (6), If the result of discriminator is 0, that means the recognition has failed; If the result is 1, it means that the person and the certificate are identical, and the verification of the real identity is successful. Generally speaking, GAN can achieve a verification accuracy of up to 99 % in biometric recognition.

5.5. Dynamic protection of information security

(1) Determination of dynamic invocation rules for the security algorithm of a Blockchain smart contract (i): The security system is generated by default with two 256-bit keys, which include a public key (PuKey) (Fig. 7-(6)) and a private key (SecrKey). After the digital model of the user fingerprint is converted into a digital model with setting FO = [(x,y),θx,θy,θz,∮j], the fingerprint digital model generates PuKey set FO(SecrKey) obtained by asymmetric algorithm.

(2) Establish and verify the reliability of the encryption and decryption algorithm library Algorithm(i)with security algorithm dynamic invocation rules: Algorithm(i) algorithm library includes DES, 3DES, AES (symmetric algorithm); ECC, RSA, DSA (asymmetric algorithm) etc. i represents the algorithm library serial number. The algorithm library needs to follow the blockchain user, inter-organizational smart contract rules: strictly ensure synchronous updates and collaborative consistency.

(3) Calculate and get the private key(i), and transfer Pukey into the function Algorithm(i)to get the private key SecrKey(i).

(4) Information data encryption and decryption: get the blockchain ciphertext SecText after encrypted by Encryption algorithms(i) and SecrKey, send the block encrypted data SecText, PuKey(i) to the user, the user gets the blockchain parameter data, use PuKey

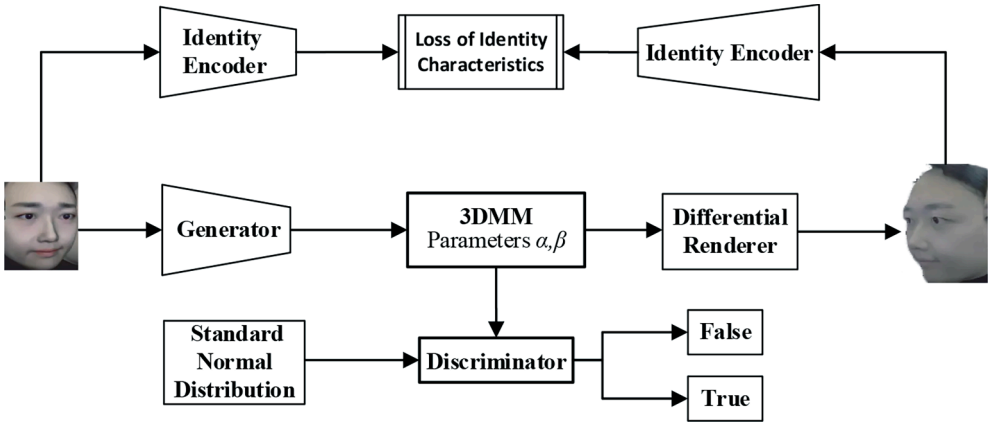

Fig. 8. 3DMM and adversarial networks facial recognition process.

and (i) number symmetric decryption algorithm, Algorithm(i) can decrypt to get private key SecrKey(i), then input ciphertext SecText, SecrKey(i) and the decryption algorithm(i) to get data PubText (Fig. 7-(10)).

5.6. Get the initial text PubText

According to their business management, users get the initial blockchain information text PubText and perform data exchange, operation, modification, etc. Users upload their encrypted data, generate blockchain node information, and complete the blockchain data share.

5.7. Task completed

Verification and authentication of identity information completed, along with encryption protection tasks, and SSL-VPN channel closed.

6. Conclusions

Cross-disciplinary research in fields like digital identity and network trust is limited, lacking a robust knowledge base. This study integrates and innovates across disciplines such as social psychology of trust, data management, and computer science of information security by NOPI model. It examines the relationships between network trust, blockchain organization, user identity, big data, and information security. The study proposes precise user digital identity attributes and big data management chains, reshaping blockchain information security. It introduces dynamic security mechanisms and collaborative processes for blockchain governance, providing effective solutions for digital identity governance. Research on digital identity technology enables reliable integration into financial services and enhances employment opportunities. Governments and enterprises benefit from fraud prevention, quality services, and inclusive taxation. Collaborative identity management boosts office efficiency, particularly in cross-border transactions and international cooperation, fostering trust and cooperation between nations.

7. Future work

Digital twins will empower the data collection, content perception, and intelligent management of digital identities, enriching the knowledge management system and research theoretical paradigm of digital identity big data. The zero-trust approach based on the CPS system will deeply enhance the digital social security governance framework. The digital identity identification and collaborative authentication of blockchain users will be a key focus in the next stage of digital society development, becoming a cornerstone of the national digitalization development strategy and digital security infrastructure. In this regard, the digital government will improve the grading and sharing of big data, promote the digital and intelligent upgrade and transformation of metaverse (Meta systems), organizations (enterprises, governments, nations, etc.), and enhance global economic cooperation and high-quality development.

Author contributions

Conceptualization (network trust, zero trust, digital identity, blockchain, etc.), overall framework, methodology, reversion, review and editing: Feng Wang; Data collection, computation, and analysis of the survey questionnaire, investigation, resources: Yongjie Gai; information security and process protection: Haitao Zhang. All authors have read and agreed to the published version of the manuscript.

CRediT authorship contribution statement

Feng Wang: Writing – review & editing, Writing – original draft, Supervision, Software, Resources, Methodology, Investigation, Conceptualization. **Yongjie Gai:** Writing – review & editing, Writing – original draft, Visualization, Validation, Resources, Data curation, Conceptualization. **Haitao Zhang:** Writing – review & editing, Writing – original draft, Visualization, Funding acquisition, Formal analysis.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Acknowledgement

This article was supported by the National Social Science Foundation of China (No. 21BTQ058).

References

Aggarwal, S., Kumar, N., 2021. Blockchain Technology for Secure and Smart Applications across Industry Verticals. Elsevier Academic Press Inc, San Diego, pp. 345–354.
Aggarwal, S., Kumar, N., 2021. Blockchain for enterprise. In: Aggarwal, S., Kumar, N., Raj, P. (Eds.), Blockchain Technology for Secure and Smart Applications across Industry Verticals. Elsevier Academic Press Inc, pp. 345–354.
Ahamad, D., Hameed, S.A., Akhtar, M., 2022. A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization. J. King Saud Univ.-Comput. Inf. Sci. 34 (6), 2343–2358.
Alhelaly, Y., Dhillon, G., Oliveira, T., 2024. Mobile identity protection: the moderation role of self-efficacy Gurpreet Dhillon. Aust. J. Inf. Syst. 28 https://doi.org/10.3127/ajis.v28.4397.
Alketbi, A., et al., 2020. Novel blockchain reference model for government services: Dubai government case study. Int. J. Syst. Assur. Eng. Manage. 11 (6), 1170–1191. https://doi.org/10.1007/s13198-020-00971-2.
Alketbi, A., Nasir, Q., Abu Talib, M., 2020. Novel blockchain reference model for government services: Dubai government case study. Int. J. Syst. Assur. Eng. Manag. 11 (6), 1170–1191.
Almakhour, M., Sliman, L., Samhat, A.E., Mellouk, A., 2022. A formal verification approach for composite smart contracts security using FSM. J. King Saud Univ.-Comput. Inf. Sci. 35 (1), 70–86.
Alvi, S.T., Uddin, M.N., Islam, L., Ahamed, S., 2022. DVTChain: a blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. J. King Saud Univ.-Comput. Inf. Sci. 34 (9), 6855–6871.
Berawi, M.A., Sari, et al., 2021. Developing a blockchain-based data storage system model to improve government agencies' organizational performance. Int. J. Technol. 12 (5), 1038–1047. https://doi.org/10.14716/ijtech.v12i5.5237.
Berdik, D., Otoum, S., Schmidt, N., et al., 2021. A survey on blockchain for information systems management and security. Inf. Process. Manag. 58 (1), 28.
Bicer, C., Murturi, I., Donta, P.K., Dustdar, S., 2023. Blockchain-based zero trust on the edge, doi: 10.48550/arXiv.2311.16744.
Bradatsch, L., Miroshkin, Kargl, F., 2023. ZTSFC: a service function chaining-enabled zero trust architecture. IEEE Access 11, 125307–125327. https://doi.org/10.1109/ACCESS.2023.3330706.
Capocasale, V., Perboli, G., 2022. Standardizing smart contracts. IEEE Access 10, 91203–91212. https://doi.org/10.1109/ACCESS.2022.3202550.
Chen, Y., Yang, Q., Li, X., 2024. A new identity authentication and key agreement protocol based on multi-layer blockchain in edge computing. IEEE Access 12, 3274–3291.
Davis, F.D., 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. 13 (3), 319–340.
Dehghani, M., Ghiasi, M., et al., 2021. Blockchain-based securing of data exchange in a power transmission system considering congestion management and social welfare. Sustainability 13 (1), 21.
Du, J., Wang, Y., Zheng, K., Jia, S., 2023. Innovative development and application practice of trusted computing 3.0. Inf. Secur. Res. 9, 179.
Esposito, C., Tamburis, O., Su, X., et al., 2020. Robust decentralised trust management for the internet of things by using game theory. Inf. Process. Manag. 57 (6), 16.
Fathalla, E.S., Azab, M., Wu, H.Y., et al., 2023. pt-ssim: a proactive, trustworthy self-sovereign identity management system. IEEE Internet Things J. 10 (19), 17155–17169.

Fu, Y.X., Shao, J., Feng, W.Z., 2023. Non-transferable blockchain-based identity authentication. Peer-to-Peer Netw. Appl. 16 (3), 1354–1364. https://doi.org/10.1007/s12083-023-01481-1.
Greulich, M., Lins, S., Pienta, D., Thatcher, J.B., Sunyaeva, A., 2024. Exploring contrasting effects of trust in organizational security practices and protective structures on employees' security-related precaution taking. Inf. Syst. Res. https://doi.org/10.1287/isre.2021.0528.
Haiou, L., 2014. Mobile SNS trust model for big data knowledge service recommendation. Library Forum 34 (10), 68–75.
Jiahui, Z., 2020. Research on the impact of new government media responsiveness on government trust in online public opinion events. J. Guiyang Municipal Party School 06, 27–36.
Jq, Z., 2021. Research on information security risk assessment of CBTC system based on blockchain. Inf. Comput. 33 (11), 230–233.
Khan, A., 2022. Integrating blockchain technology into healthcare through an intelligent computing technique. CMC-Comput. Mater. Continua 70, 26. https://doi.org/10.32604/cmc.2022.020342.
Kingo, T., Aranha, D.F., et al., 2023. User-centric security analysis of mitid: the Danish password less digital identity solution. Comput. Secur. https://doi.org/10.1016/j.cose.2023.103376.
Kouhizadeh, M., Saberi, S., Sarkis, J., 2021. Blockchain technology and the sustainable supply chain: theoretically exploring adoption barriers. Int. J. Prod. Econ. 231.
Labati, Rd., Piuri, V., Scotti, F., 2023.. multicardionet: interoperability between ecg and ppg biometrics. Pattern Recogn. Lett. 175, 1–7.
Li, B.H., Song, X.Y., Cai, K., et al., 2023. Trust management strategy for digital twins in vehicular ad hoc networks. IEEE J. Sel. Areas Commun. 41 (10), 3279–3292.
Liu, R.Y., Yu, X.F., Yuan, Y., Ren, Y.J., 2023. BTDSI: a blockchain-based trusted data storage mechanism for Industry 5.0, J. King Saud Univ.-Comput. Inf. Sci. 35 (8) https://doi.org/10.1016/j.jksuci.2023.101674.
Lumineau, F., Wang, W.Q., Schilke, O., 2021. Blockchain governance-a new way of organizing collaborations? Organ. Sci. 32 (2), 500–521.
Lykidis, I., Drosatos, G., Rantos, K., 2021. The use of blockchain technology in e-government services. Computers 10 (12), 17.
Lykidis, I., Drosatos, G., Rantos, K., 2021. The use of blockchain technology in e-government services. Computers 10 (12), 168. https://doi.org/10.3390/computers10120168.
Nazir, A., He, J.S., Zhu, N.F., Ullah, F., 2024. Collaborative threat intelligence: enhancing IoT security through blockchain and machine learning integration. J. King Saud Univ.-Comput. Inf. Sci. 36 (2) https://doi.org/10.1016/j.jksuci.2024.101939.
Popa, M., Stoklossa, S.M., Mazumdar, S., 2023. Chain discipline - towards a blockchain-iot-based self-sovereign identity management framework. IEEE Trans. Services Comput. 16 (5), 3238–3251.
Rathee, T., Singh, P., 2022. A systematic literature mapping on secure identity management using blockchain technology. J. King Saud Univ.-Comput. Inf. Sci. 34 (8), 5782–5796.
Runze, Hu., 2021. The impact of online participation on government trust–an empirical analysis based on data CSS2017. J. Texas Coll. 37 (04), 58–65.
Safi, S.M., Movaghar, A., Ghorbani, M., 2022. Privacy protection scheme for mobile social network. J. King Saud Univ.-Comput. Inf. Sci. 34 (7), 4062–4074.
Saqib, M., Jasra, B., Moon, A.H., 2022. A lightweight three factor authentication framework for IoT based critical applications. J. King Saud Univ.-Comput. Inf. Sci. 34 (9), 6925–6937.
Saxena, S., Shao, D., Nikiforova, A., Thapliyal, R., 2022. Invoking blockchain technology in e-government services: a cybernetic perspective. Dig. Policy Regul. Govern. 24 (3), 246–258. https://doi.org/10.1108/DPRG-10-2021-0128.
Strauss, S., et al., 2023. The body as permanent digital identity? Societal and ethical implications of biometrics as mainstream technology. Tecnoscienza-Ital. J. Sci. Technol. Stud. 14 (1), 59–76.
Suhaimin, M.S.M., Hijazi, M.H.A., Moung, E.G., et al., 2023. social media sentiment analysis and opinion mining in public security: taxonomy, trend analysis, issues and future directions. J. King Saud Univ.-Comput. Inf. Sci. 35 (9), 25.
Taylor, P.J., Dargahi, T., et al., 2020. a systematic literature review of blockchain cyber security. Digit. Commun. Netw. 6 (2), 147–156.
Tiancheng, Z., 2021. Research on industrial internet information security in the big data era. Shanghai Manag. Sci. 43 (06), 110–2+9.
Udokwu, C., Norta, A., 2021. Deriving and formalizing requirements of decentralized applications for inter-organizational collaborations on blockchain. Arab. J. Sci. Eng. 46 (9), 8397–8414.
Upadhyay, S., Kumar, M., Singh, S., et al., 2023. Digital image identification and verification using maximum and preliminary score approach with watermarking for security and validation enhancement. Electronics 12 (7). https://doi.org/10.3390/electronics12071609.
Wang, T., 2023. analysis and countermeasures of computer network security issues under the background of big data. Sci. Inf. 5, 88–90.
Wang, F., Jiyan, Z., et al., 2017. Research on mobile commerce payment management based on the face biometric authentication. Int. J. Mob. Commun. 15 (3), 278–305.
Wang, F., Shan, G.B., et al., 2020. Identity authentication security management in mobile payment systems. J. Glob. Inf. Manag. 28 (1), 189–203. https://doi.org/10.4018/jgim.2020010110.
Wang, L., Yuan, Y., Ding, Y., 2023. Analysis and design of identity authentication for Iot devices in the blockchain using hashing and digital signature algorithms. Int. J. Distributed Sensor Netw. https://doi.org/10.1155/2023/2524051.
Wang, Z.Y., Li, et al., 2022. Business innovation based on artificial intelligence and blockchain technology. Inf. Process. Manag. 59 (1), 102759 https://doi.org/10.1016/j.ipm.2021.102759.
Wu, D., Pei, Y., 2022. Blockchain technology and its research in the field of information security. China New Commun. 24 (01), 40–41.
Yan, Z., Qu, H.P., Lin, X.J., et al., 2023. Identity-based proxy matchmaking encryption for cloud-based anonymous messaging systems. J. Syst. Archit.
Yang, X., 2021. Research on Attribute σ Protocol and Identity Recognition. Minnan Normal University. doi: 10.27726/d.cnki.gzzsf.2021.000275.
Yanhui, S., Muzhe, H., 2020. Research on scientific data custody model of institutional knowledge base integrating blockchain technology. Mod. Intell. 40 (01), 101–109.
Yin, S., Wang, X., et al., 2023. Research on adversarial network image dehazing fusion of multiple models. Comput. Sci. Appl. 13, 1807.
Yuanpei, H., 2020. Research on security system construction under network security level protection 2.0. Wireless Internet Technol. 17 (08), 32–33.
Zhang, J., Li, Y.J., Xiao, W.D., 2021. Integrated multiple kernel learning for device-free localization in cluttered environments using spatiotemporal information. IEEE Internet Things J. 8 (6), 4749–4761. https://doi.org/10.1109/JIOT.2020.3028574.
Zhang, J., Li, Y.J., Li, Q., Xiao, W.D., 2024. Variance-constrained local–global modeling for device-free localization under uncertainties. IEEE Trans. Ind. Inf. https://doi.org/10.1109/TII.2023.3330340.
Zhang, C., Wang, C., Sun, L., 2021. Blockchain system risk classification and security standards. Inf. Technol. Stand. 9, 12-4+20.
Zhang, Y., Zhang, L.Y., Wu, Q., Mu, Y., 2022. Blockchain-enabled efficient distributed attribute-based access control framework with privacy-preserving in IoV. J. King Saud Univ.-Comput. Inf. Sci. 34 (10), 9216–9227. https://doi.org/10.1016/j.jksuci.2022.09.004.
Zhaohui, Du., 2021. Research and application of borderless zero trust network in the context of "Internet +". Mod. Inf. Technol. 5 (06), 153–157.
Zhi, K.Y., Tan, Q.R., Chen, S., 2022. How does social security fairness predict trust in government? The serial mediation effects of social security satisfaction and life satisfaction. Int. J. Environ. Res. Public Health 19 (11). https://doi.org/10.3390/ijerph19116867.
Zhou, P.Y., Xu, Z.J., Li, Y.B., et al., 2015. Research on identity authentication management in mobile commerce based on ECC and dynamic fingerprint key. Int. J. Mob. Commun. 13 (5), 535–548.