Information Services & Use 44 (2024) 255–266
DOI 10.3233/ISU-240013
IOS Press

Exploration of the application of blockchain in e-government: Opportunities and risks coexist

Jian Yu*
School of Computer and Information Science, Hubei Engineering University, Xiaogan, China

Abstract. Blockchain technology provides a technical solution for the challenges faced by e-government, such as low efficiency, excessive energy consumption, and lack of trust mechanisms. It can promote the establishment of a more efficient and high-quality government service system, thereby enhancing the public trust of the government. Although blockchain technology provides theoretical innovation to traditional governance structures with its decentralization, consensus mechanisms, and enhanced trust, its impact and ability to transform existing governance structures still have limitations in practical applications. Based on an in-depth analysis of the concept and application boundaries of blockchain, this article explores its value in the field of e-government. At the same time, it systematically proposes strategic suggestions to promote the development of blockchain technology in the field of e-government from multiple aspects such as institutional construction, technical standardization, and professional talent cultivation, in response to its limitations and application risks. By accelerating technology research and development and standard construction, strengthening high-level promotion, optimizing promotion competition mechanisms, and conducting rooted research, the application and promotion of blockchain in government governance can be accelerated, laying a solid foundation for building a future intelligent and transparent government service model.

Keywords: Blockchain, e-government, application scenarios, government informationization, government management

1. Introduction

Developing and applying blockchain based e-government has become a strategic priority for many developed countries worldwide, aiming to promote modernization of government governance through technological innovation. Countries such as the UK and Singapore are particularly prominent in this regard, not only committed to technological breakthroughs in the basic network layer and intermediate protocol layer of blockchain, but also actively exploring new applications of this technology in the field of e-government, viewing it as a key to enhancing national competitiveness [1].

The report "Distributed Ledger Technology: Beyond Blockchain" released by the UK government clearly states that blockchain technology has the ability to reform the interaction mode between the government and citizens, bringing revolutionary changes to public services through data sharing, enhanced transparency, and trust. This indicates that the UK is actively seizing the potential of blockchain technology to achieve transparency and efficiency in government services. The Archangel project, jointly

*E-mail: yuj@hbeu.edu.cn.

developed by the UK National Archives and the University of Surrey, aims to use blockchain technology to prevent improper tampering of electronic video archives, thereby achieving permanent protection of electronic video archives [2]. In the United States, the Delaware Blockchain Initiative project aims to create a new way to preserve a company's shareholder list by storing it on a state operated blockchain rather than on a physical ledger [3]. Singapore has taken a dual approach in the fields of blockchain and artificial intelligence, incorporating them into its national strategic plan with the aim of building a smart government through these cutting-edge technologies, improving the efficiency and quality of public services, and addressing the challenges of international competition. Other countries are also taking active actions, such as the Netherlands using blockchain technology as electronic evidence storage in the judicial system, simplifying judicial procedures and improving work efficiency; Australia uses blockchain for election voting, enhancing the transparency and security of the voting process; The Swedish government has applied blockchain technology to land registration management, improving the transparency and security of land transactions [4,5]. These measures collectively demonstrate the enormous potential of blockchain e-government in simplifying administrative procedures, promoting government integrity, and improving service efficiency and quality, marking the world's move towards building a more efficient, transparent, and trustworthy government service model. Through blockchain technology, governments around the world are actively exploring new paths to modernize governance to meet the needs of the digital age [6,7].

The 2018 United Nations E-Government Survey Report (Chinese version) was released on the 21st at the Central Party School (National School of Administration). The report shows that China's online e-government services rank 34th in the world, reaching a leading level of global development. According to the report data, China's e-government development index is 0.6811, ranking 65th and above the global average. Among them, the online service index is 0.8611, ranking 34th and reaching a leading global development level. The report also shows that in terms of the Electronic Governance Development Index (EGDI) across all continents, Europe (0.7727) continues to lead, followed by the Americas (0.5898), Asia (0.5779), Oceania (0.4611), and Africa (0.3423). In response to this situation, the Chinese government has actively issued the Guiding Opinions on Accelerating the Construction of a National Integrated Online Government Service Platform, aiming to build an integrated national level e-government service platform and significantly improve the efficiency of e-government services [8].

Blockchain technology has timely integrated into this transformation demand, and its inherent reliability, credibility, and openness make it an ideal tool for optimizing e-government services and promoting the integration of government informationization. China attaches great importance to the development of blockchain technology, listing it as a key area of national cutting-edge technology layout, and encouraging local governments to actively explore its application potential, aiming to use the characteristics of blockchain technology to improve the efficiency, transparency, and security of government services.

However, existing research on the functional definition of blockchain technology tends to be overly optimistic. On the one hand, excessive optimism may amplify the technological advantages of blockchain and thus amplify the risk of blindly launching blockchain. On the other hand, excessive concern about the impact of blockchain on existing governance structures may also inhibit its application in digital governments. Therefore, scientifically defining the function of blockchain is a prerequisite for accelerating the application of blockchain. This article combines the current development status of government data in China and the characteristics of blockchain technology itself to study the inherent logic of the role of blockchain technology in government data sharing mechanisms. Firstly, explain the development background and current situation of blockchain in the field of e-government. Secondly, define the technical concept of blockchain, including the blockchain technology architecture and the key technologies involved. Then, the role of blockchain technology in optimizing e-government mechanisms, potential

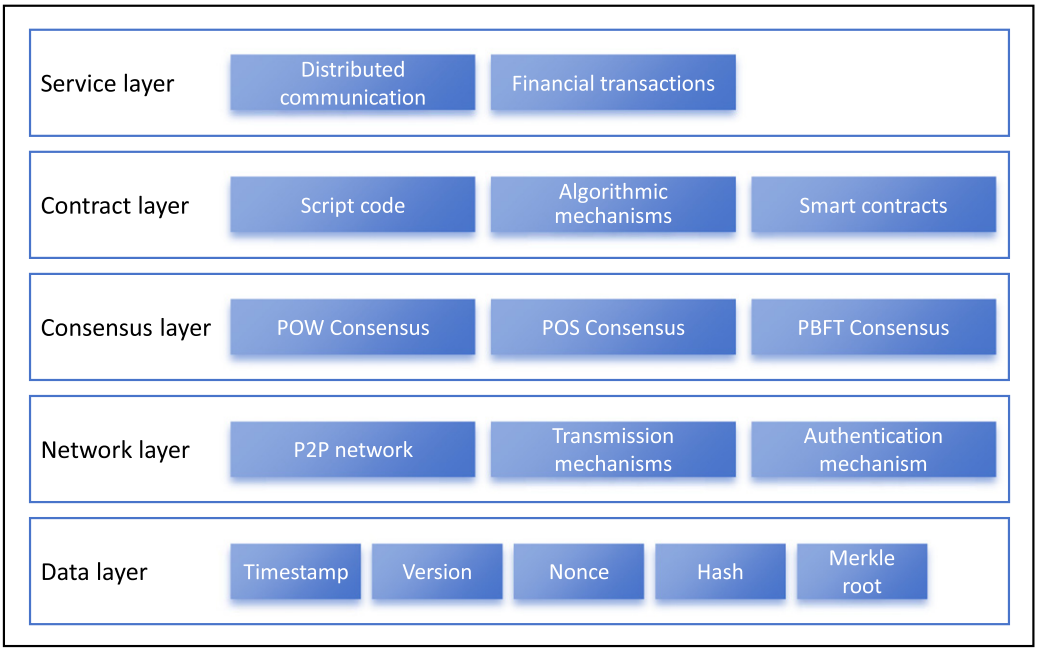

Fig. 1. Blockchain technology architecture.

risks, and the root causes of these risks were analyzed in detail. Finally, suggestions are made regarding the limitations and risks of the application of blockchain in the field of e-government, with the aim of benefiting the future development and application of blockchain technology.

2. Blockchain technology

The essence of blockchain technology is a comprehensive system that combines data management, value transfer protocols, and distributed computing. It achieves decentralized processing and immutability of input data through the use of consensus mechanisms, smart contracts, and advanced encryption algorithms, ultimately building a highly secure and trustworthy chain database system. This is both a way of storing information and a platform for executing value exchange rules [9,10].

In the technology architecture of blockchain, the three core levels clearly define the progressive relationship between technology and application, as shown in Fig. 1.

(1) The communication layer is the foundation of the entire system, which is divided into two parts: the network layer is responsible for the distributed propagation of data, ensuring that information can be transmitted quickly and securely in a decentralized network; The data layer encapsulates data into blocks and links them together through complex computational processes and encryption methods, forming an immutable blockchain structure.

(2) The protocol layer plays a bridging role, with the consensus layer ensuring that all participating nodes reach consensus on the authenticity of data, maintaining the integrity and consistency of the blockchain; On this basis, the consensus layer and contract layer incentivize network participants and ensure the

unambiguous execution of contract terms by setting rules and automatically executing protocols, further enriching the functionality and application potential of blockchain.

(3) The service layer is directly oriented towards practical applications, covering the practical implementation of blockchain technology in various fields and industries. This includes but is not limited to financial services, supply chain management, copyright protection, public services, etc. Each application is a concrete manifestation of the value of blockchain technology, driving the innovation of traditional business models and the development of the digital economy.

The core operational process of blockchain technology can be summarized as an interlocking chain, with the following specific steps: after the transaction is initiated, the information is broadcasted by nodes through a peer-to-peer network (P2P); After receiving transaction information, each node performs block calculation, which includes generating the hash value of the previous block to ensure data continuity and integrity; During this process, the nodes will continuously refresh to maintain the latest status; Subsequently, each node verifies the transaction to ensure its validity; Once verified, a new block is created, which contains the calculated block header hash value to ensure the immutability of the block content; After the completion of the new block construction, it will be added to the end of the blockchain and permanently stored in the system; This process repeats itself, constantly expanding the length of the blockchain. The key technical components that support this technological chain include:

- Peer to peer processing technology (P2P): Different from the traditional client server model, P2P technology enables each node in the network to be both a client and a server, and can directly interact with other nodes to exchange information, improving the decentralization and fault resistance of the system.
- Asymmetric encryption algorithm: using a pair of keys (public key and private key) to encrypt and decrypt information, ensuring the security of transactions and the verification of user identity, is the foundation of data encryption and verification in blockchain.
- Distributed processing technology: By involving multiple nodes in the network in data processing and storage, it enhances the stability and security of the system, ensuring the decentralized storage and synchronous updating of data.
- Consensus mechanism: Ensuring that all participating nodes reach consensus on the blockchain status, preventing double payments and malicious tampering, is the foundation of trust in blockchain networks.
- Smart contract: a computer program that automatically executes, controls, or documents legal events and behaviors, running on the blockchain, and can execute contract terms without third-party intervention, greatly improving transaction efficiency and security. It is a key tool for blockchain technology to achieve automated trust and value transfer.

Blockchain technology is mainly divided into three categories based on different access permissions and management methods: public chains, private chains, and consortium chains. Each type has its own unique participants, characteristics, advantages, and limitations, as shown in Table 1.

Public blockchains are open to everyone, allowing anyone to join, read data, send transactions, and participate in the consensus process. They embody the highest form of decentralization, where every node in the network has equal rights and responsibilities. The advantages of public blockchains lie in their high transparency and resistance to censorship, but they also face issues of high energy consumption and relatively low transaction efficiency.

In contrast to public chains, the permissions of private chains are restricted to specific organizations or individuals and are typically controlled by a single entity. This enables private chains to have better performance, such as low energy consumption, high efficiency, and stronger privacy protection capabilities, but their degree of decentralization is relatively low.

Table 1
Comparison of public chain, consortium chain, and private chain

	Public chain	Consortium chain	Private chain
Participant	Everyone	Alliance members	Internal members
Bookkeeper	All participants	Alliance administrator	Internal administrator
Consensus mechanism	PoW/PoS/PBFT	Distributed consistency algorithm	Distributed consistency algorithm
Incentive mechanism	Essential	Optional	None
Centralization	Decentralization	Multi centralization	Centralization
Privacy protection	Unprotected or Fully protected	Weak protection	Protecting privacy
Security	Vulnerable	Relatively safe	Very safe
Typical scenario	Virtual currency	Financial settlement	Copyright protection

As a compromise solution between public and private chains, consortium chains are jointly maintained by multiple pre selected entities, retaining a certain degree of decentralization while improving efficiency and security by limiting the number of participants, making them suitable for inter enterprise collaboration scenarios. Consortium chain is currently the most widely used type of blockchain in fields such as e-government and finance, combining the controllability of private chains with the partial openness of public chains.

In the field of e-government, the hybrid model of "consortium chain + private chain" is widely adopted to balance the needs of transparency, security, and efficiency. It not only promotes information sharing within the government, but also protects sensitive data, ensuring the effectiveness and security of services [11,12].

The rise of blockchain technology marks that mankind is moving from the era of information Internet to the era of value Internet, which helps to break information barriers and reduce the phenomenon of "data islands". However, with the booming development of the digital economy, finding a balance between promoting data openness and sharing, protecting personal privacy, and ensuring data security has become an important issue that urgently needs to be addressed in the development of blockchain technology. Therefore, strengthening data protection mechanisms and establishing an effective trust system have become key directions for the continuous evolution of blockchain technology.

3. The advantages and challenges of blockchain

3.1. Advantages of blockchain

Blockchain technology has brought unprecedented opportunities for the innovation of e-government, providing comprehensive and efficient solutions to long-standing problems such as low efficiency, information isolation, data vulnerability, and lack of trust in traditional e-government. From a reliability perspective, blockchain, as a decentralized distributed ledger, does not affect the normal operation of the entire system even if a single node fails. Compared to traditional centralized data processing models, it demonstrates higher system stability and reliability. In terms of credibility, although blockchain technology is open and transparent, it strictly protects personal data through encryption technology, ensuring that only authorized entities can access relevant data. This design, which combines cryptography and consensus mechanisms, greatly enhances the security and trustworthiness of information. In addition,

the openness of blockchain technology is reflected in its peer-to-peer accounting method, which can effectively improve the circulation and utilization efficiency of government information resources. After being confirmed by the consensus mechanism, the data of all participating parties can be broadcasted and viewed by other nodes. This process greatly promotes the sharing of government information, establishes a stable trust bridge between participating parties, and lays a solid foundation for building an efficient, transparent, and collaborative e-government ecosystem. Specifically, blockchain has reshaped the face of e-government through the following aspects [13–15].

Economic benefits: By simplifying processes and reducing intermediary links, blockchain technology reduces the cost of government processing, improves the economy of resource utilization, accelerates service delivery speed, and promotes efficient operation of government activities. Many local governments in China are using blockchain technology to optimize their government service processes, such as the "City Brain" launched by Hangzhou, which utilizes blockchain and other technologies to achieve "one-stop service", making it more convenient for residents and businesses to handle various government service matters, achieving "at most one visit" or even "no need to visit at all".

Information sharing: The data sharing mechanism supported by blockchain breaks down information silos while ensuring data privacy and security, achieving seamless information exchange across departments and levels, and enhancing information collaboration capabilities within the government and with the public. The distributed ledger feature of blockchain ensures the authenticity and immutability of data, while smart contracts can automatically execute data sharing rules, reduce human intervention, and improve data processing efficiency.

Data Security: By utilizing its tamper proof and encryption features, blockchain technology provides a robust defense wall for e-government data, effectively preventing illegal tampering or leakage of data and enhancing the information security defense line. In the judicial field, blockchain technology is used for the storage of electronic evidence, ensuring the authenticity and immutability of the evidence, accelerating the case handling process, and improving the fairness and efficiency of judicial rulings.

Transparent trust: The transparency and traceability of blockchain enable every government operation to have verifiable records, increasing the transparency of government actions and establishing a new type of relationship based on technological trust between the government and the public. This greatly enhances the public's trust and satisfaction with government decisions and public services. Blockchain technology is also used to enhance the transparency and accuracy of the social security system, ensure transparent allocation and effective use of poverty alleviation funds, and reduce corruption and abuse.

Blockchain digital identity: Through blockchain technology, a unified and secure identity authentication system can be created, allowing personal information to flow between different government departments without the need for repeated verification. Some regions in China have begun exploring the use of blockchain technology to issue digital identity cards, electronic business licenses, etc., to ensure the authenticity and privacy protection of identity and qualification information, improve work efficiency, and reduce the risks of forgery and fraud.

Smart contract processing sensitive information: Smart contracts can automatically execute contract terms without the need for third-party intervention, providing an efficient and secure way to handle government sensitive information and automatically enforce policy regulations. Blockchain technology is applied to public resource trading platforms, such as bidding and government procurement, to improve transparency, prevent opaque operations, and ensure fair and just transactions.

Electronic bills and certificates: Blockchain electronic bills can achieve fast circulation and verification, without being limited by physical location and office hours, improving the flexibility and efficiency of government processing. The tamper proof nature of blockchain provides strong protection for electronic

certificates, enhances public trust in government records, and reduces disputes and audit costs. By utilizing blockchain technology, tax departments can achieve full lifecycle management of invoices, with traceability from issuance to reimbursement, effectively cracking down on illegal activities such as issuing false invoices, simplifying the tax reporting process for enterprises, and improving tax management efficiency.

3.2. Risks and challenges

(1) The contradiction between algorithm security and efficiency: The security of blockchain mainly depends on its characteristics such as distributed ledger, encryption technology, and consensus mechanism. Through these features, blockchain can ensure the immutability of data and the reliability of transactions, thereby maintaining the security of the system. For example, each block in a blockchain contains the hash value of the previous block, and this chain structure makes it difficult to tamper with data once it is written. At the same time, blockchain uses encryption technology to protect the security and privacy of transaction data, ensuring that transaction data is not leaked. In addition, the consensus mechanism ensures consensus among nodes in the network, preventing attacks from malicious nodes. However, these security measures often sacrifice efficiency to some extent. For example, the Proof of Work (PoW) algorithm in consensus mechanisms requires a significant amount of computing power to solve complex computational problems, thereby ensuring the security of the network. But this algorithm has low efficiency and requires a lot of time and resources. In contrast, algorithms such as PoS (Proof of Stake) and DPoS (Delegated Proof of Stake) have improved efficiency, but there are still some scalability issues.

(2) The security risks of smart contracts: The application of smart contracts can be described as a win-win situation. Although it can enable both parties to reach a consensus of trust, related users are also prone to the loss of "trust benefits" caused by technical security risks. Although some legal regulations state that blockchain service providers need to have prerequisites related to providing services (such as technology, compliance with national standards, etc.), they are not sufficient to address the security risks of smart contracts. From the perspective of blockchain technology application security, relevant researchers are also in an awkward predicament. If security vulnerabilities related to blockchain technology applications are made public, it is easy to harm the rights and interests of blockchain service providers and some users. If they choose not to make them public, it will also allow some criminals to exploit vulnerabilities to invade the blockchain system, greatly reducing its security and stability, and even evolving into a "crash and paralysis" chain, thereby losing its due functional role.

(3) The risk of abuse of blockchain technology: Although blockchain technology has promoted the development of the digital society, if its application is not restricted, it will inevitably lead to its abuse, which will be backfired by the application of technology and result in the alienation of the digital society structure. Firstly, relevant users can utilize the decentralized technology characteristics of blockchain to conduct transactions without the supervision of centralized organizations such as banks and other financial institutions. Such a "vacuum zone" is likely to be a paradise for illegal activities such as drugs, money laundering, and gambling.

(4) The limitations of blockchain technology rules: Blockchain technology is also difficult to achieve the "complete decentralization and absolute neutrality" advocated by its technical rules in both theory and practice. From a theoretical perspective, blockchain technology faces issues such as inequality and isolation in regulating user behavior. The main reason for these problems is that they cannot completely break free from the control of "computing bias". Specifically, computational bias can be reflected in the consensus algorithms mentioned earlier. The operation of consensus algorithms is based on the principle of "minority obeying majority". If one can have the computing power of more than half of the nodes in the

blockchain, they can manipulate the data information on the "chain" at will, forming absolute dominance over the nodes and the blockchain system. However, this is not the essence of fairness and justice (absolute neutrality). If blockchain technology follows the principle of "minority obeying majority", it will only harm the interests of other nodes or related users, and even lead to the abuse of computing power [16].

4. Development strategy suggestions

The rapid development of blockchain technology under the government led model highlights the key role of the government in promoting technological innovation and regulating industry development. Although blockchain e-government faces some technical and conceptual challenges, its potential in improving government transparency, efficiency, security, and trust is enormous. By continuous technological innovation, improving laws and regulations, strengthening cross departmental collaboration, and enhancing public awareness and acceptance of blockchain technology, these disadvantages can be gradually overcome. Therefore, government support and control are particularly important, and it is recommended to start from the following aspects [17].

4.1. Promote the implementation of applications

Blockchain e-government is in a new stage of exploration and development, and the government plays a crucial role in this process. The government should clearly release relevant policies to encourage technological innovation and application attempts, provide necessary policy guidance and financial support for blockchain e-government projects, and create a favorable environment for innovative development. Select representative and feasible government areas as pilot projects for blockchain applications, such as document management, public services, data sharing, etc., and accumulate valuable practical experience by testing the feasibility and effectiveness of the technology through actual operation. Encourage government departments, research institutions, enterprises, and social organizations to participate and form a joint force to explore the best practices of blockchain e-government. Through cross-border cooperation, promote the deep integration of technology and government needs. During the pilot process, a feedback mechanism will be established to promptly collect opinions and suggestions from users, technical personnel, policy makers, and other parties. Based on the identified problems and shortcomings, technical adjustments and strategic optimizations will be made to ensure the continuous improvement of blockchain e-government projects. While promoting applications, it is necessary to strictly comply with data protection regulations, strengthen data encryption and privacy protection measures in blockchain systems, and ensure the security of personal information and sensitive data. On the basis of successful pilot projects, relevant technical standards and business specifications will be formulated to lay the foundation for the large-scale promotion of blockchain e-government, gradually expanding its application scope to more government fields.

4.2. Institutionalization of development

Although blockchain technology has shown great potential in asset ownership, information verification, and data management, its application still faces challenges such as insufficient legal protection and security risks. Clarify the legal status of data on blockchain, including ownership, usage, and disposal rights, to ensure that data rights involved in blockchain applications have legal basis and provide solid legal protection for data rights. Develop data protection and privacy regulations specifically for blockchain

technology, requiring the use of advanced encryption technology to protect on chain data, prevent data leakage, tampering, and illegal use, and establish emergency response mechanisms and compensation mechanisms for data leakage. Given that key security is crucial for blockchain systems, legislation should be enacted to clarify the responsible parties for key management, establish legal responsibilities and remedies for key loss or theft, and ensure the security of users' assets and data. In the process of data on chain, emphasis should be placed on the legality, legitimacy, and necessity of personal data processing, ensuring the data subject's right to know and choose. Any data collection, processing, and transmission should be based on the data subject's explicit consent. By utilizing the tamper proof nature of blockchain, a sound data traceability mechanism should be established. For behaviors such as data forgery and infringement of data rights, legal responsibilities should be clearly defined to ensure that the responsible parties can be traced back and held accountable in accordance with the law, and to maintain the fairness and order of the data environment. Given the cross-border mobility of data and the global nature of blockchain, it is necessary to strengthen real name management and international cooperation, enhance legal coordination and cooperation on data protection and privacy rights between countries, jointly build a legal framework for cross-border data flow, and protect the rights and interests of global users.

4.3. Establish a standard system

One of the major challenges facing the development of blockchain e-government is the lack of unified industry technical standards and application systems, which leads to many projects being easily trapped in patterned replication or blindly following trends during implementation, without fully considering the unique needs and feasibility of specific government scenarios. To solve this problem, it is crucial to establish a scientific and reasonable standardized system for programmatic application technology. We should conduct in-depth research on the needs of different government fields, clarify the specific requirements and technical challenges of e-government in application scenarios such as digital identity, electronic proof, and government auditing, and ensure that the construction of standard systems can be targeted. Due to the involvement of numerous government departments and business processes in e-government, establishing cross departmental working groups to promote information sharing and resource integration is the foundation for developing a widely applicable and compatible standard system. Based on thorough research, we will begin to develop technical standards and operational guidelines, including data formats, interface specifications, security standards, privacy protection, smart contract templates, etc., to ensure interoperability and data consistency between different blockchain platforms. Select representative application scenarios to carry out pilot projects, verify the feasibility and effectiveness of the standard system through practice, collect feedback in a timely manner, iteratively optimize the standards, and ensure that they can effectively guide practical applications. Along with the establishment of technical standards, corresponding laws and regulations are also needed to clarify the legal status, responsibility attribution, and data protection requirements of blockchain e-government, providing legal protection for technological applications. In addition, with the continuous development of technology, the standard system also needs to be constantly updated and improved, while strengthening the integration with international standards, promoting mutual recognition and cooperation of blockchain e-government on a global scale.

4.4. Strengthen technological research and integration

The practical implementation of blockchain technology is an important goal of its research and development, and the key to achieving this goal lies in continuously optimizing and innovating core

technologies such as P2P transmission, consensus mechanisms, smart contracts, etc., to better adapt to diverse application scenarios. At the same time, in response to the difficulty of balancing algorithm security and efficiency, technical strategies need to be adopted to ensure legal implementation, thereby eliminating the risks that algorithms may induce and providing technical support for effective governance. Events such as the Agama wallet data breach highlight the severe challenges faced by the blockchain security field, reminding us to continuously improve the security protection capabilities of blockchain systems, including but not limited to strengthening permission management, upgrading encryption algorithms, and improving privacy protection mechanisms, in order to effectively respond to increasingly complex network security threats. For example, the "S-money" theory proposed by the University of Cambridge in the UK, based on advanced ideas of quantum theory and relativity, provides new theoretical support for the security of cryptocurrencies, especially for the study of private key security, which is of great significance for protecting the account security of data subjects [18].

The integration and development trend of blockchain technology with cutting-edge technologies such as artificial intelligence (AI), the Internet of Things (IoT), and Big Data is evident. The combination of these technologies can complement each other's advantages, jointly break down data silos, and promote the free flow and efficient utilization of information. AI can provide more intelligent data analysis and prediction capabilities for blockchain, and the massive data generated by IoT devices can be securely stored and transmitted through blockchain. Big data technology can help improve the processing efficiency and decision-making accuracy of blockchain networks. Therefore, in the future, blockchain e-government should fully utilize the integration advantages of these technologies. It is not only necessary to strengthen the research on the integration of technologies themselves, but also to pay attention to the integration of cross domain knowledge, ensure that technology applications can better serve the public, improve the transparency, efficiency, and convenience of government processing, and truly achieve the goal of convenience and benefit for the people. In this process, it is necessary to continuously explore regulatory frameworks and legal systems that are adapted to the new environment, ensuring technological progress and social stability and harmonious development.

4.5. Pay attention to talent cultivation

As an emerging and rapidly developing industry, blockchain has an extremely urgent demand for professional talents. Currently, the application of blockchain technology has expanded from the initial digital currency to multiple fields such as finance, logistics, healthcare, and government affairs, with an increasing demand for interdisciplinary and versatile talents. Therefore, strengthening the cultivation of blockchain talents is not only an important support for promoting industrial development, but also a key factor in maintaining the country's leading position in global technological competition.

IBM and other global tech giants have launched blockchain education programs, reflecting the industry leaders' emphasis on talent cultivation. By injecting enterprise resources and practical experience, it helps to quickly cultivate practical talents who understand both technology and business. This collaborative model not only provides students with learning opportunities that combine theory with practice, but also helps to shorten the distance between theoretical learning and practical application, accelerating talent output. Local governments and higher education institutions in China are also actively responding, such as Guangzhou's promotion of blockchain related professional construction and targeted classes, as well as Tongji University's blockchain DBA teaching program, which aims to cultivate high-end professional talents to meet the industry's urgent demand for high-level and specialized talents. These measures not

only enrich the connotation of domestic blockchain education, but also provide valuable experience and reference for other regions and universities.

5. Conclusion

Blockchain is an emerging technology generated by the collection of various high-tech digital information technologies. Its decentralized, tamper proof, and traceable technical characteristics enable it to be widely used in government services, economic reform, people's livelihood development, social governance, and other fields, greatly improving the production efficiency of society. Blockchain based e-government not only changes the service model of the government, making it more flexible and responsive, but also significantly improves the efficiency and quality of public management, promoting the level of government public services towards a smarter, more efficient, and lower cost direction. The application technology of blockchain has shaped the coexistence of stakeholders. From different perspectives, governments, enterprises, and individuals all have their own interests and demands. However, on the one hand, people need to be inclusive towards new things, respect the inherent logic of digital change, and hope that it can bring us positive changes; On the other hand, it is necessary to enhance the research and development capabilities of technologies such as artificial intelligence and blockchain applications, overcome ethical and network autonomy issues caused by technological defects and even misuse, and create a pioneering technological development environment guided by legal procedures and free values. The application prospects of blockchain are broad, and it is necessary to strengthen research from the perspectives of technology, society, and the rule of law, to leverage the technological advantages of blockchain, and thus achieve the modernization of the national governance system and governance capacity with the help of blockchain.

References

[1] J. Sharma and H. Taherdoost, *Impact of Blockchain Technology on the Development of E-Businesses,* 2022, pp. 391–396. ISSN 23674512. doi:10.1007/978-981-16-8403-6_35.

[2] Archangel: Securing our national archives with AI and blockchain [EB/OL]. [2022-11-30]. https://www.surrey.ac.uk/news/archangel-securing-our-nationalarchives-ai-and-blockchain.

[3] Quinn H., What ever happened to the Delaware blockchain initiative? [EB/OL]. [2022-12-10]. https://technical.ly/civic-news/delaware-blockchain-initiative/.

[4] C. Diego, C. Judith, F.D. Daniel et al., Blockchain for public services: A systematic literature review, *IEEE ACCESS* (2021), 913904–913921.

[5] L. Ioannis, D. George and R. Konstantinos, The use of blockchain technology in e-government services, *Computers* **10**(12) (2021), 168.

[6] S. Ølnes, J. Ubacht and M. Janssen, Blockchain in government: Benefits and implications of distributed ledger technology for information sharing, *Government Information Quarterly* **34**(3) (2017), 355–364.

[7] E.N. Surya, A.H. Nizar, A. Ria et al., Survey of smart contract framework and its application, *Information* **12**(7) (2021), 257.

[8] U. Nations. *United Nations E-Government Survey 2018,* United Nations, 2018, https://www.un-ilibrary.org/content/books/9789210472272.

[9] Y. Li, D.A. Su and A. Mardani, Digital twins and blockchain technology in the industrial Internet of Things (IIoT) using an extended decision support system model: Industry 4.0 barriers perspective, *Technological Forecasting and Social Change* **195** (2023). doi:10.1016/j.techfore.2023.122794.

[10] C. Qian, Y. Gao and L. Chen, Green supply chain circular economy evaluation system based on industrial internet of things and blockchain technology under ESG concept, *Processes* **11**(7) (2023), 1999.

[11] H. Sa'ari, M.M. Amin, M.S. Abbas, A.F. Ismail, A.H.H. Fadzilah and M. Nordin, Transforming Industrial operations with blockchain: the healthcare application health-chain. in: *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE),* IEEE, 2023, pp. 1175–1179.
[12] J. Yu, F. Xu and Y. Li, Research and design of student archives management system based on consortium blockchain, *Journal of Computational Methods in Sciences and Engineering* **23**(5) (2023), 2313–2322. doi:10.3233/JCM-226825.
[13] A.K. Koshariya, V. Kumar, V. Ahmad, B.H. Babu, B. Umarani and S. Ramesh, Blockchain technology for agricultural data sharing and sustainable development of the ecosystem. in: *Artificial Intelligence, Blockchain, Computing and Security Volume 1,* CRC Press, 2024, pp. 272–276.
[14] K. Gadallah, The potential role of blockchain technology in addressing development challenges in developing countries. in: *Conference on Sustainability and Cutting-Edge Business Technologies,* Springer, 2023, pp. 226–236.
[15] H. Hou, The application of blockchain technology in E-government in China. in: *2017 26th International Conference on Computer Communication and Networks (ICCCN),* IEEE, 2017, pp. 1–4.
[16] H.J. Zheng and Y. Cao, Governance of risks in the application of blockchain technology: logic, principles, and means, *Journal of Hefei University of Technology (Social Sciences Edition)* **37**(3) (2023), 42–50.
[17] I. Lykidis, G. Drosatos and K. Rantos, The use of blockchain technology in e-government services, *Computers* **10**(12) (2021), 168.
[18] K. Adrian, S-money, *Proceedings: Mathematical, Physical and Engineering Sciences* **475**(2225) (2019), 1–25.