Blockchain Based Access Control: A Review and Future Perspectives

Riqing Xu[1,2(✉)], Liang Shan[1,2], Xinlong Wang[1,2], and Gang Lei[1,2]

[1] School of Software, Jiangxi Normal University, Nanchang 330022, China
{richard,shanliang1981,leigang}@jxnu.edu.cn
[2] Jiangxi Provincial Engineering Research Center of Blockchain Data Security and Governance, Nanchang, China

Abstract. This paper reviews the state of the art in blockchain-based access control research. In the digital era, data security and access management are increasingly important. Traditional access control (e.g. RBAC, ABAC, CapBAC) faces various challenges in IoT, such as the risk of centralization and the threat of data leakage. To address these issues blockchain technology (with its properties such as distributed and tamper-proof) provides innovative solutions. This paper first introduces the three main-stream access control in IoT, then discusses the basic concepts of blockchain (including consensus mechanism, smart contract and cryptography), and analyzes the blockchain in access control applications (including authentication, privilege management and audit trail). It then discusses the advantages and challenges of block-chain access control and future research directions. Finally, the potential of block-chain in access control is summarized, emphasizing its importance for data security and privacy protection. Through this overview paper, readers can better understand the application of blockchain technology in access control and provide valuable insights for future research and practice.

Keywords: Access control · Blockchain · Data security · Privacy · IoT

1 Introduction

In the age of the internet, data security and privacy protection have become crucial challenges in our society and business life [1–5]. With the frequent occurrence of large-scale data breaches and the constant escalation of hacker attacks, we need a robust, secure, and reliable way to manage and protect our data. While traditional access control models such as Role-Based Access Control (RBAC) and Access Control Lists (ACL) perform well in specific contexts, they fall short when dealing with complex permission management requirements and cross-organizational collaboration. Previous research in this field has proposed various extensions and improvements, such as Attribute-Based Access Control (ABAC) and Capability-Based Access Control (CapBAC). However, these methods still face challenges related to centralization risks and single points of failure. Blockchain technology is an innovative solution to address these challenges.

Y. Cao and X. Shao (Eds.): DIONE 2023, LNICST 515, pp. 276–289, 2025.
https://doi.org/10.1007/978-3-031-80713-8_21

Blockchain technology, initially conceived as the underlying technology for Bitcoin, has rapidly evolved into a versatile tool that can play a role in various industries and domains. Its core features, including distributed ledger, decentralized control, immutability, and support for smart contracts, make it a promising access control method. Pal et al. [6] analyzed how blockchain can enhance IoT access control compared to traditional access control systems, and summarized five key characteristics of blockchain and IoT access control. This provides an outline for blockchain-based IoT access control.

This article aims to review the application of blockchain technology in the field of access control and explore its potential value in data security and privacy protection. In the second section, we introduce the fundamental concepts of access control, emphasizing their critical importance in the context of the Internet of Things (IoT). Next, we discuss the challenges faced by traditional access control methods and their limitations.

In the third section, we delve into the core principles and features of blockchain technology and how they relate to access control. By conducting an indepth examination of use cases where blockchain is applied in identity verification, permission management, and auditing, we demonstrate how it provides more robust, transparent, and secure access control mechanisms across various domains. In the fourth section, we analyze how the advantages of blockchain address current challenges in the access control field and offer insights into future prospects. Finally, we conclude this article.

2 Access Control

2.1 Background Knowledge

Access control is a security mechanism that ensures only authorized entities can reliably access resources (such as files and data) through access policies. Access policies rely on user identities, roles, attributes, and contextual information to determine which entities can access particular resources under defined conditions. Its goal is to protect systems and resources, making them accessible only to legitimate users, preventing unauthorized access, thereby maintaining the confidentiality, integrity, and availability of the system, and reducing the risks of security threats and data leaks, as shown in Fig. 1. Previous research has been dedicated to developing and improving various access control models and mechanisms to safeguard data and resources within systems from unauthorized access and misuse.

In the era of the proliferation of the IoT, access control is of paramount importance due to several key reasons.

The highly heterogeneous and extensive scale of IoT devices presents a series of challenges. The existence of a vast number of interconnected devices makes scalability a critical concern [7,8]. In this context, security and privacy requirements become particularly vital, necessitating the safeguarding of data and the confidentiality of user personal information. Since these devices can handle sensitive information, multiple aspects of security must be considered. Anonymity,

confidentiality, and integrity of data are of utmost importance. Firstly, data should be anonymized to prevent the leakage of personal identity information. Simultaneously, data confidentiality needs to be highly protected to prevent unauthorized access or theft. Additionally, data integrity must also be ensured to prevent tampering or corruption during transmission or storage. Furthermore, identity verification and authorization mechanisms are indispensable. These mechanisms prevent unauthorized users from accessing IoT systems, ensuring that only legitimate users can access and operate the devices. Trust is a crucial issue in the IoT environment. As different devices must process data according to user demands and rights, users must be able to trust these devices. Establishing trust hinges on robust security and privacy protection measures to ensure the proper protection of user data and rights.

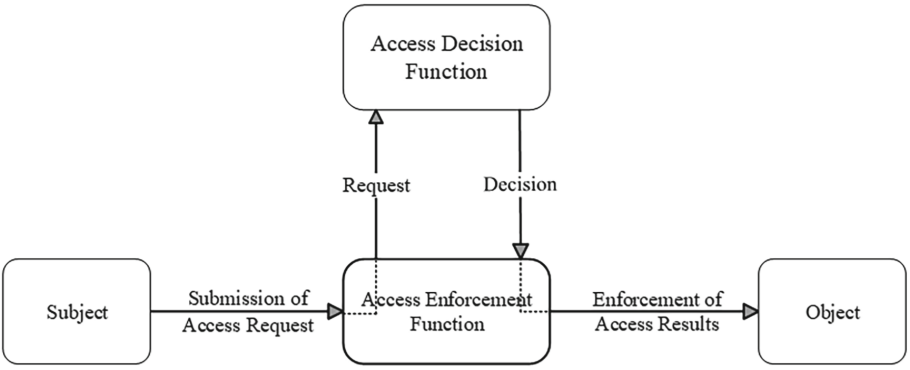

Fig. 1. Major components of an access control process.

In summary, the heterogeneity and scale of the Internet of Things introduce multi-faceted challenges, including scalability, privacy, security, and trust, among others. However, traditional access control methods such as RBAC, ABAC, and CapBAC face certain problems and limitations.

2.2 Role-Based Access Control

The RBAC model manages and controls access to system resources by associating users with roles and roles with permissions, granting access to specific roles, and assigning users to the corresponding roles. In the RBAC model, roles are defined based on the responsibilities and positions of users, and the system administrator assigns different roles to users, with each role having a set of permissions corresponding to its responsibilities. The core idea of the RBAC model is to simplify permission management by organizing users into roles. Traditional RBAC has limitations [9], including the role explosion problem, dynamic privilege management issues that do not consider context, and a lack of fine-grained access control, making it suitable for specific scenarios. Scholars have conducted

extensive research on this topic. Rajpoot et al. [10] consider contextual information and provide fine-grained access control, achieved by exploiting resource content in policies. Vistbakka et al. [11] define RBAC by extending the traditional static approach and propose and for-malize a dynamic RBAC model. Uddin et al. [12] propose an approach using the dynamic role-based access control model with dynamic separation of duties (SoD) and an authorization process workflow. However, in the complex IoT landscape, the number of connected devices is increasing dramatically. Formal dynamic RBAC is evidently not flexible enough to meet the fine-grained access requirements of multiple attributes in IoT. Furthermore, the central definition and management of roles and permissions lead to trust and extensible issues. The RBAC model is suitable for managing permissions within an organization, such as a corporate intranet.

2.3 Attribute-Based Access Control

Compared to the RBAC model, ABAC offers greater flexibility. In the ABAC model, access decisions are not manually assigned by system administrators but are determined based on entity attributes, such as user attributes, resource attributes, and environmental attributes. These attributes are defined through policy rules, and the system dynamically decides whether to grant users access to resources based on these rules. It then adapts access control dynamically based on the actual context and needs. The ABAC model allows for finer-grained control and can determine access based on combinations of multiple attributes, thus better accommodating complex access requirements. This model is commonly used in scenarios requiring highly customizable access control, such as cloud computing and healthcare systems. It provides robust flexibility in policy management but has some limitations in the context of the Internet of Things (IoT).

Limitations of ABAC in the IoT Context Include:

Lack of Policy Management Mechanism: ABAC does not provide built-in mechanisms to verify the required number of policies. This necessitates a policy management mechanism for effective management and verification, which can lead to increased complexity, potentially affecting system performance and scalability.

Accuracy and Trustworthiness of Attributes: ABAC relies on attributes for ac-cess decisions, but the accuracy and trustworthiness of these attributes cannot al-ways be guaranteed. If attribute information is tampered with or forged, the system may be vulnerable to security threats.

Difficulty in Attribute Standardization: Ensuring consistency of attributes across different systems can be challenging. This is because different systems may use varying attribute definitions and formats. Therefore, when applying ABAC across systems, the issue of attribute standardization needs to be addressed.

ABAC also involves challenges related to delegation, management, auditability, scalability, hierarchical representation, and others [13]. The inherent characteristics of blockchain technology naturally address the limitations of ABAC.

2.4 Capability-Based Access Control

'Capability' is one of the core concepts in the Capability-based Access Control (CapBAC) model, and it serves as a token or identifier used to represent access per-missions to resources. Specifically, a capability is a data structure that contains in-formation about the following:

Resource Identifier: Specifies the unique identifier of the resource or object to be accessed. This can be a file, a database record, a network service, and so on.

Operation: Defines the permitted operation or type of operation to be executed, such as read, write, delete, and others.

Subject: Identifies the entity with access privileges, typically a user, a process, or another system entity.

Optional Additional Information: Depending on requirements, capabilities may include other information related to access permissions, such as expiration time, access conditions, and more.

Unlike RBAC and ABAC, the CapBAC model employs a unique approach to access control. In CapBAC, access permissions are precisely managed through "capabilities" rather than relying on pre-defined roles or attributes [14]. This means that each entity is assigned or granted a set of capabilities, which explicitly specify the actions they can perform and the resources they can access. And CapBAC adopts a more entitycentric and personalized control approach.

The access control model of CapBAC exhibits broad applicability, enabling access control implementation across different device types and manufacturers. This is because capabilities represent access permissions in a universal manner, making them understandable and applicable regardless of device types or manufacturers. This scalability aids in improving cross-platform and cross-organizational interoperability, rendering CapBAC highly promising in addressing access control require-ments in comp lex environments like the Internet of Things (IoT). Additionally, CapBAC offers advantages in terms of lightweight and scalability, making it a potential solution to tackle the challenges posed by modern complex systems. While CapBAC is relatively new and has not yet gained widespread adoption. As technology evolves and the demand for finer-grained access control increases, the significance of CapBAC may gradually grow. CapBAC has the potential to offer finer-grained access control and more flexible token management compared to traditional access control. However, CapBAC is more complex than traditional access control models, making its implementation and maintenance more challenging. Nevertheless, this complexity can also be seen as a trade-off for providing higher security and precision in specific security requirements.

All in all, These three access control models each have their own advantages and applicable scenarios, with the choice of the appropriate model often depending on system requirements, complexity, and security needs. As shown in Table 1. RBAC is suitable for straightforward role management, ABAC is applicable in scenarios requiring more flexible permission management, and CapBAC

emphasizes the principle of least privilege, making it suitable for security-focused environments.

Table 1. Comparison of Access Control Models.

Feature/Model	RBAC	ABAC	CapBAC
Interoperability	Lower	Better	Better
Scalability	Lower	Better	Better
Dynamic	Lower	Better	Higher
Security	Basic	Better	Better
Privacy	weaker	Stronger	Stronger
Fine-Grained	Some level	Better	Higher
Manageability	Relatively easy	More complex	Some complexity

3 Blockchain Access Control

3.1 Background Knowledge

Blockchain is a distributed ledger technology that operates without reliance on a single central authority or server. It is built on top of a peer-to-peer (P2P) network, where data storage and validation are not under centralized control but are collectively maintained and verified by multiple participants in the network [15]. In a blockchain, transactions are recorded in blocks, with each block containing a certain amount of transaction data. These blocks are connected in chronological order, forming an ever-growing chain. Each transaction undergoes validation and confirmation to ensure its legitimacy before being added to the blockchain. This validation is achieved through encryption techniques and distributed consensus algorithms, ensuring the security and reliability of transactions. Consensus mechanisms are the rules and algorithms within the blockchain network used to achieve agreement and validate transaction validity. Encryption algorithms are employed to encrypt trans-action data in the blockchain, ensuring that only authorized participants can access and verify the information, thereby safeguarding data privacy and security. Smart contracts are another crucial concept [16], which are self-executing computer pro-grams that automatically execute contract conditions. They are deployed and executed on the blockchain network and automatically trigger and perform corresponding actions based on predefined conditions.

Blockchain is considered the optimal solution to the single point of failure prob-lem in centralized access control models and the security and trust issues in access control runtime environments [17].

3.2 Combined with Blockchain Access Control

RBAC Meets Blockchain

Kim et al. [17], implemented role-based access control (RBAC) on top of blockchain, proposing a mechanism for sharing images while preventing arbitrary third-party access. Specifically, it involves a central entity with dual roles: an administrator with no access to videos but the capability to manage access policies, and a video manager with permissions for video creation, modification, and deletion. When the administrator needs to modify the video manager's access policies, the management system sends an identity information request to the requester, who undergoes hash authentication. Smart contracts are used to request the identification key recorded in the management system to confirm that the block was created on the blockchain network by a legitimate user, thereby verifying the legitimacy of the block creator. The innovation in this paper lies in the dual-role central entity. However, the paper merely uses blockchain as a verification tool and does not integrate RBAC with blockchain. This approach ensures data integrity but does not effectively overcome the inherent limitations of RBAC, such as its lack of dynamism, granularity, and scalability, resulting in a relatively narrow scope of applicability and inflexible policy management.

Rahman et al. [18] proposed a context-aware, auditable, and dynamically loca-tion-aware role-based access control system based on Ethereum smart contracts. Resource owners send transactions to the blockchain to manage relationships be-tween roles and permissions. A location server is associated with an Ethereum ac-count that monitors user location information. However, the LRBAC smart contract is only deployed on the Ethereum blockchain and does not address the inherent limi-tations of RBAC, making it challenging to manage in scenarios with large amounts of data. Lackner et al. [19] introduced an RBAC model based on hierarchical roles and role-configurable management rules implemented through smart contracts. Permissions are not directly determined by the position of management roles within the hierarchical structure. Instead, roles are associated with corresponding manage-ment rules, and the granting and revoking operations require confirmation from multiple users. This model enables decentralized organizations with flexible man-agement constraints but has a relatively limited scope of application.

The integration of blockchain with RBAC opens a rift in centralized access control, where the system is no longer a single central entity but can have multiple central entities governing and managing each other. However, the inherent limitations of RBAC remain a historical challenge.

ABAC Meets Blockchain

Zhang et al. [20] proposed a payable multi-authority Attribute-Based Encryption (ABE) scheme with outsourced decryption, serving as a solution for sharing electronic health records in the edge computing environment. They specifically designed ciphertext-policy ABE (CP-ABE) with policy hiding to protect patients' sensitive information. They utilized blockchain to store public parameters, reducing the online time of other entities and improving system efficiency. Additionally, they employed smart contracts to facilitate fair payments between

mobile edge computing (MEC) servers and users. Experimental results demonstrated that blockchain technology addressed the trust issues between MEC servers and users but did not consider attribute revocation and management. Yan et al. [21] have integrated blockchain technology with attribute-based searchable encryption to propose an innovative solution for distributed data sharing. This solution supports policy concealment and attribute revocation, enabling fine-grained searchable access to encrypted cloud data. Specifically, the approach involves storing data ciphertext in the distributed Inter Planetary File System (IPFS) and securely distributing metadata ciphertext through blockchain smart contracts, ensuring data integrity and confidentiality. Additionally, they have designed smart contracts with search auditing capabilities, allowing for dynamic management of access permissions based on user access behavior and access periods. Qin et al. [22] have proposed a blockchain-based multi-attribute authorization access control scheme designed for data sharing. They leverage smart contracts to establish mutual trust among multiple permissions and have devised four smart contracts to facilitate cross-domain collaboration for multiple permissions. By introducing a secret sharing scheme and an authorization block-chain, they have successfully achieved cross-domain management for each attribute. This eliminates the single-point bottleneck present in existing multi-attribute CP-ABE (Ciphertext-Policy Attribute-Based Encryption) schemes while also reducing computational and communication overhead between users and multiple attribute permissions. Additionally, they record access logs on a trusted and immutable block-chain, allowing data owners to easily monitor user access behavior. Wu et al. [23] also presented a strategy and attribute-concealing access control scheme that combines block-chain technology and the ABAC model. This scheme aims to establish access control that can be audited and preserves privacy in data-sharing scenarios. It utilizes smart contracts to assess whether attributes conform to certain policies and employs an additive homomorphic Dynamic Threshold Public Key Cryptosystem (DT-PKC) cryptographic system to encrypt attributes and policies. Multiple blockchain nodes collectively decrypt the data and use zero-knowledge proof technology to ensure the correctness of the decryption results. This approach effectively prevents attackers from inferring private information or gaining unauthorized access through information on the blockchain. However, it introduces complexity in terms of auditing and monitoring, making it challenging to provide comprehensive traceability of access activities. Therefore, striking a balance between privacy protection and trace-ability remains a challenge in blockchain technology. Li et al. [24] combined traditional RBAC and ABAC models to manage access policies in the supply chain. Specifically, they adopted the ABAC model as the overall framework, defining entities and attributes, encapsulating various operations among different entities into roles, and incorporating roles as entity attributes within ABAC. They designed three smart contracts on Hyperledger Fabric for managing information, storing access control, and implementing access control policies. Experimental results demonstrated that this approach leverages the flexibility of ABAC to achieve fine-grained and dynamic permission management while

simplifying system permission administration with RBAC advantages. By utilizing the traceability, tamper-resistance, and decentralization features of blockchain technology, it addresses trust and information silo issues between transaction parties, ensuring the security and privacy of medical device information in the supply chain.

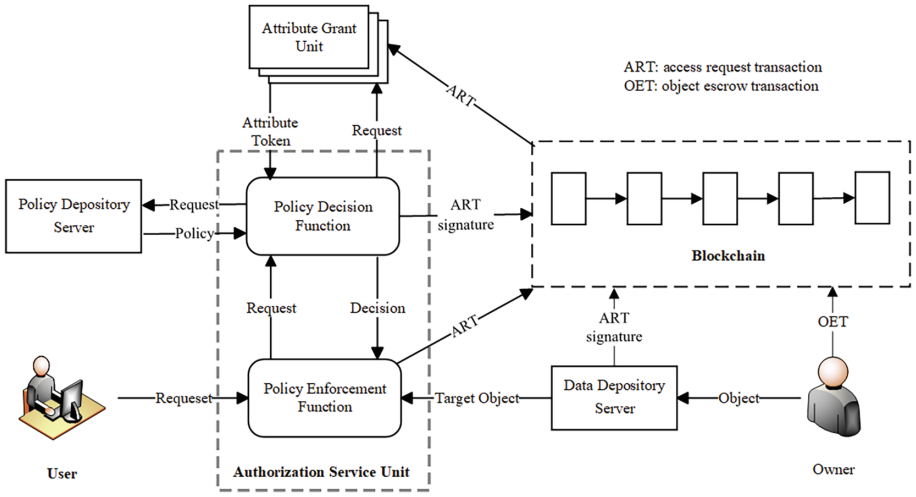

Fig. 2. Major components of an access control process.

Implementing blockchain-based ABAC can be achieved through two main approaches: transaction-based access control and smart contract-based access control [23]: In transaction-based access control, access policies are stored on the blockchain in the form of transactions. Users retrieve the necessary information from the blockchain and make authorization decisions. The authorization results are then communicated back to the blockchain through transactions. As shown in Fig. 2. [32]

In smart contract-based access control, attributes and policies are transmitted to smart contracts. When a user's attributes align with the specified policies, the smart contract automatically grants access authorization. As shown in Fig. 3.

From a privacy perspective, storing access policies and user attributes directly on the blockchain ledger is not appropriate. Therefore, we need to explore a method that strikes a balance between privacy and traceability, such as employing privacy protection techniques to conceal sensitive information. This issue holds significant significance in blockchain research.

CapBAC Meets Blockchain

Xu et al. [25] introduced a decentralized capability-based access control scheme utilizing blockchain, referred to as BlendCAC. This scheme defines two types of

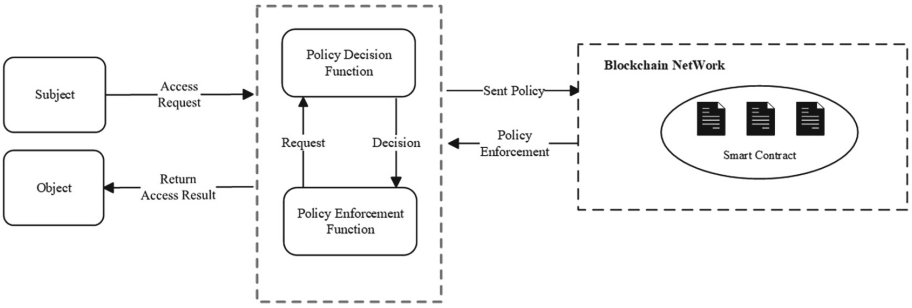

Fig. 3. Smart contract-based access control.

tokens: Identity-Capability (ICap) tokens, which record subject-specific authorization operations, and Identity-Delegation-Certificate (IDC) tokens, which document delegation relationships between subjects. Nakamura et al. [26] introduced a delegation graph as an alternative to delegation trees, addressing two limitations related to BlendCAC: authorization inconsistencies and the synchronous updat-ing of permissions. Liu et al. [27] have proposed a capability-based access control architecture for managing the identity and access control of IoT devices, utilizing blockchain and decentralized identifiers (DIDs). Specifically, the access control module collaborates with on-chain smart contracts. Each DID uniquely corresponds to a blockchain account and allows DID owners to configure recovery delegation and thresholds. Device owners can use ownership credentials to manage ownership relationships of their devices, enabling them to revoke and reissue credentials to enhance device security and privacy. This approach offers scalable and lightweight access control, ensuring the security and trustworthiness of interactions between devices and servers through protocol specifications. However, ensuring user privacy and managing DIDs can be challenging.

4 Discussion

4.1 Access Control Advantages of Blockchain

Compared to traditional models, blockchain-based access control models offer several advantages, including immutability, smart contracts, and distributed control.

Immutability Ensures Data Security: One of the greatest strengths of blockchain is its immutability. Once information is written into the blockchain, it is nearly impossible to alter or delete. This means that once access permissions are granted or revoked, the corresponding records are permanently stored, ensuring data integrity and trustworthiness. This is particularly valuable for protecting sensitive information and facilitating audit trails.

Smart Contracts Enable Automated Access Control: Smart contracts on the blockchain are self-executing computer programs that can automatically execute predefined actions based on specified conditions. In blockchain-based access con-trol, smart contracts can be used to implement automated access decisions [27,28]. For example, when a user requests access to a particular resource, a smart contract can verify the user's identity and permissions, automatically granting access if the conditions are met. This automated access control not only enhances efficiency but also reduces the risk of human errors.

Distributed Control Enhances Availability: Blockchain is a distributed system where permission information is stored across multiple nodes. This distributed nature ensures high availability of access control because there is single point of failure that could cause the entire system to collapse. Even if some nodes experience failures, other nodes can continue to execute access control tasks.

Transparency and Traceability: Blockchain's transparency means that anyone can view the data and access control rules on the blockchain. This transparency helps build trust since users can clearly understand how access control decisions are made. Furthermore, the blockchain records the history of every access request and authori-zation, making audit tracking more accessible and reliable [29].

4.2 Challenges and Future Prospects

With the continuous development of blockchain technology, it will continue to have a positive impact on the field of access control. Here are some future prospects:

Standardization and Interoperability: In the future, we may see more standards and protocols related to blockchain access control to facilitate interoperability be-tween different systems. This will make it easier to integrate various blockchain solutions into existing access control systems.

Privacy Protection: Implementing stronger privacy protection measures on the blockchain will be an important direction. This may involve the application of privacy computing to ensure that users' sensitive information is not disclosed [30].

Performance Optimization: Blockchain's performance issues have always been a challenge, especially in large-scale access control scenarios. Future research and development may focus on improving the performance and scalability of blockchain to meet high-demand requirements.

Multi-Chain and Cross-Chain Solutions: Multi-chain and cross-chain solutions can provide greater flexibility for access control, allowing assets and permissions to be more easily interoperable and transferable between different blockchains [31].

5 Conclusion

This article delves deep into the fundamental concepts of access control and its pivotal role in today's digital landscape. We underscore the challenges and constraints confronting traditional access control methods, including their static nature, complexity, capability management, and security vulnerabilities. Subsequently, we explore how blockchain technology addresses these challenges and elucidate its potential advantages in the realm of access control, such as immutability, smart contracts, distributed control, transparency, and security. Blockchain technology introduces novel solutions and possibilities to the field of access control. Its immutability and distributed nature enhance the credibility and availability of access control. Smart contracts automate access decisions, while transparency and traceability foster trust, and security fortifies data and permission protection. Nevertheless, blockchain technology itself grapples with performance, scalability, storage costs, and privacy issues, necessitating thoughtful consideration and resolution in real-world applications. Looking to the future, we anticipate ongoing development and innovation within blockchain technology in the access control domain. Standardization and interoperability will facilitate integration across diverse systems, privacy protection techniques will bolster the security of personal data, and performance optimization will enhance blockchain's usability in high-load environments. Multi-chain and cross-chain solutions will provide support for greater flexibility, catering to the needs of various organizations and application scenarios.

In conclusion, blockchain technology brings fresh hopes and opportunities to the access control field, promising to enhance security and manageability in the digital landscape. Nevertheless, it demands continuous research and improvement to over-come its inherent challenges and realize its full potential.

References

1. Jain, P., Gyanchandani, M., Khare, N.: Big data privacy: a technological perspective and review. J. Big Data **3**(1), 1–25 (2016). https://doi.org/10.1186/s40537-016-0059-y
2. Zhang, J., Chen, B., Zhao, Y., Cheng, X., Hu, F.: Data security and privacy-preserving in edge computing paradigm: survey and open issues. IEEE Access **6**, 18209–18237 (2018)
3. Tabrizchi, H., Kuchaki Rafsanjani, M.: A survey on security challenges in cloud computing: issues, threats, and solutions. J. Supercomput. **76**(12), 9493–9532 (2020). https://doi.org/10.1007/s11227-020-03213-1
4. Sun, P.J.: Privacy protection and data security in cloud computing: a survey, challenges, and solutions. IEEE Access **7**, 147420–147452 (2019)
5. Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H.: A survey on security and privacy issues in Internet-of-Things. IEEE Internet Things J. **4**(5), 1250–1258 (2017)
6. Pal, S., Dorri, A., Jurdak, R.: Blockchain for IoT access control: recent trends and future research directions. J. Netw. Comput. Appl. **203**, 103371 (2022)
7. Sicari, S., Rizzardi, A., Grieco, L.A., et al.: Security, privacy and trust in internet of things: the road ahead. Comput. Netw. **76**, 146–164 (2015)

8. Qiu, J., Tian, Z., Du, C., et al.: A survey on access control in the age of internet of things. IEEE Internet Things J. **7**(6), 4682–4696 (2020)
9. Franqueira, V., Wieringa, R.: Role-based access control in retrospect. Computer **45**(6), 81–88 (2012)
10. Rajpoot, Q.M., Jensen, C.D., Krishnan, R.: Attributes enhanced role-based access control model. In: Fischer-Hübner, S., Lambrinoudakis, C., Lopez, J. (eds.) TrustBus 2015. LNCS, vol. 9264, pp. 3–17. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-22906-5_1
11. Vistbakka, I., Troubitsyna, E.: Modelling and verification of dynamic role-based access control. In: Atig, M.F., Bensalem, S., Bliudze, S., Monsuez, B. (eds.) VECoS 2018. LNCS, vol. 11181, pp. 48–63. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-00359-3_4
12. Uddin, M., Islam, S., Al-Nemrat, A.: A dynamic access control model using authorizing workflow and task-role-based access control. IEEE Access **7**, 166676–166689 (2019)
13. Servos, D., Osborn, S.L.: Current research and open problems in attribute-based access control. ACM Comput. Surv. **49**(4), 1–45 (2017)
14. Gusmeroli, S., Piccione, S., Rotondi, D.: A capability-based security approach to manage access control in the internet of things. Math. Comput. Model. **58**(5–6), 1189–1205 (2013)
15. Tschorsch, F., Scheuermann, B.: Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutor. **18**(3), 2084–2123 (2016)
16. Omohundro, S.: Cryptocurrencies, smart contracts, and artificial intelligence. AI Matters **1**(2), 19–21 (2014)
17. Lo, S.K., Liu, Y., Chia, S.Y., et al.: Analysis of blockchain solutions for IoT: a systematic literature review. IEEE Access **7**, 58822–58835 (2019)
18. Rahman, M.U., Guidi, B., Baiardi, F., Ricci, L.: Context-aware and dynamic role-based access control using blockchain. In: Barolli, L., Amato, F., Moscato, F., Enokido, T., Takizawa, M. (eds.) AINA 2020. AISC, vol. 1151, pp. 1449–1460. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-44041-1_122
19. CraĂ, S., Lackner, A., Begic, N., Mirhosseini, S.A.M., Kirchmayr, N.: Collaborative administration of role-based access control in smart contracts. In: 2022 4th Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS), Paris, France, pp. 87–94 (2022). https://doi.org/10.1109/BRAINS55737.2022.9909116
20. Zhang, Y., Wei, X., Cao, J., et al.: Blockchain-enabled decentralized attribute-based access control with policy hiding for smart healthcare. J. King Saud Univ.-Comput. Inf. Sci. **34**(10), 8350–8361 (2022)
21. Yan, L., Ge, L., Wang, Z., et al.: Access control scheme based on blockchain and attribute-based searchable encryption in the cloud environment. J. Cloud Comput. **12**(1), 1–16 (2023)
22. Qin, X., Huang, Y., Yang, Z., et al.: A blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing. J. Syst. Architect. **112**, 101854 (2021)
23. Wu, N., Xu, L., Zhu, L.: A blockchain-based access control scheme with hidden policy and attribute. Futur. Gener. Comput. Syst. **141**, 186–196 (2023)
24. Li, J., Han, D., Wu, Z., et al.: A novel system for medical equipment supply chain traceability based on alliance chain and attribute and role access control. Futur. Gener. Comput. Syst. **142**, 195–211 (2023)

25. Xu, R., Chen, Y., Blasch, E., Chen, G.: BlendCAC: a smart contract enabled decentralized capability-based access control mechanism for the IoT. Computers **7**(3), 39 (2018)
26. Nakamura, Y., Zhang, Y., Sasabe, M., Kasahara, S.: Exploiting smart contracts for capability-based access control in the internet of things. Sensors **20**(6), p1793 (2020)
27. Liu, H., Han, D., Li, D.: Fabric-IoT: a blockchain-based access control system in IoT. IEEE Access **8**, 18207–18218 (2020)
28. Zhang, Y., Zheng, D., Deng, R.H.: Security and privacy in smart health: efficient policy-hiding attribute-based access control. IEEE Internet Things J. **5**(3), 2130–2145 (2018)
29. Zhang, X., Du, W., Moshayedi, A.J.: A traceable and revocable multi-authority attribute-based access control scheme for mineral industry data secure storage in blockchain. J. Supercomput. 1–37 (2023)
30. Wu, G., Wang, S., Ning, Z., et al.: Privacy-preserved electronic medical record exchanging and sharing: a blockchain-based smart healthcare system. IEEE J. Biomed. Health Inform. **26**(5), 1917–1927 (2021)
31. Duan, L., Sun, Y., Ni, W., et al.: Attacks against cross-chain systems and defense approaches: a contemporary survey. IEEE/CAA J. Automatica Sinica **10**(8), 1647–1667 (2023)
32. Zhu, Y., Qin, Y., Gan, G., et al.: TBAC: transaction-based access control on blockchain for resource sharing with cryptographically decentralized authorization. In: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), vol. 1, pp. 535–544. IEEE (2018)