International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.7 July - August – 2023
DOI:10.46647/ijetms.2023.v07i04.082 ISSN: 2581-4621

Access Control Systems Based on Blockchain Technology

Gajanan Badhe[1], Dr. Maithili Arjunwadkar[2]
[1,2] *Progressive Education Society's Modern Institute of Business Studies, Pune -411044*
Corresponding Author Orcid ID : https://orcid.org/0009-0000-6749-2554

ABSTRACT
Now a days the need for decentralized applications is increasing and blockchain provides the foundational technology for creating and developing them. The security and integrity of the blockchain network and its resources are supported by access controls, which is a crucial component of blockchain-based applications. This paper presents a study of various access control mechanisms, including smart contracts, consensus algorithms, and cryptographic protocols, to assess their benefits and limitations in different contexts of applications. The purpose of the paper is to present various access control systems in blockchain-based applications and their applicability and effectiveness in various use case scenarios.
Keywords- decentralized applications, blockchain technology, cryptographic protocols, access control mechanism.

1. Introduction

Blockchain is distributed and decentralized ledger technology that enables the secure and transparent recording of transactions between numerous parties in a network. It uses a distributed and decentralized ledger for recording the transactions that are shared, duplicated, and constantly synced amongst peers run by users of a distributed network. It functions fundamentally as a database that is shared and synchronized among several network nodes, with no central hub or middleman in charge of managing the transactions [1]. The distributed ledger on the blockchain keeps track of all transactions that take place between users of the distributed network. For instance, all participants in the distributed network will treat the exchange of documents or data between members as a transaction record. Each entry in the blockchain ledger has a timestamp and a digital signature, making it possible to audit all transactions in the network and making it difficult to alter transaction records once they have been added to the ledger. The blockchain also increases the availability and efficiency of data delivery using decentralization [11]. The architecture of blockchain is shown in Figure1 as follows.

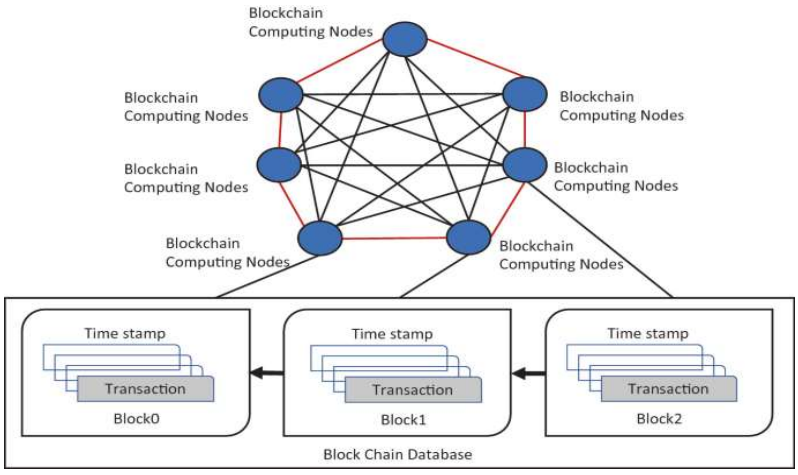

Figure 1. The Architecture of Blockchain

2. Access Controls:

DOI:10.46647/ijetms.2023.v07i04.082 ISSN: 2581-4621

Access control mechanisms are generally implemented using a combination of authentication that verifies user identity, authorization means determining user permissions, and audit mechanisms like logging and monitoring access attempts. Web application frameworks and platforms often provide built-in access control features, but custom access control solutions can also be developed based on the specific requirements of the application. Access control refers to the process of managing and regulating user access to specific resources or functionalities within the application. It ensures that only authorized users are granted the appropriate level of access based on their roles, permissions, and authentication credentials. Access control mechanisms are crucial for maintaining the security and integrity of any kind of web application by preventing unauthorized users from gaining access to sensitive data or performing unauthorized actions on the applications resources. There are various access control models and techniques used in web applications as follows-

Role-Based Access Control (RBAC): In this architecture, users are given responsibilities, and those roles determine the permissions they can access. Users are divided into various roles (administrator, manager, employee, etc.), and each role is given a set of access privileges. By regulating access based on user roles rather than specific permissions, role-based access control streamlines access control management [8].

Attribute-Based Access Control (ABAC): Access control choices are made using attribute-based access control, which takes into account a variety of properties, including user attributes, resource attributes, environmental factors, and relationships between entities. By developing policies based on these characteristics, it provides fine-grained access control [18].

Mandatory Access Control (MAC): A strict access control paradigm called mandatory access control bases access decisions on the user clearances and security labels given to resources. It is frequently employed in extremely secure settings, such as military or governmental systems.

Discretionary Access Control (DAC): In discretionary access control, users can manage access to their own resources. Access to a user's resources can be granted or denied at the user's discretion to other individuals or organizations. Discretionary Access Control is frequently used in simpler environments with highly trusted and accountable users.

3. Blockchain based access control mechanisms:

Access controls are critical in blockchain-based applications as they ensure that only authorized users can perform certain actions or access specific information. In this report, we will discuss access controls in blockchain-based applications and their importance. Access control is a process of selectively restricting access to resources or information based on an entity's identity and the permissions associated with that identity. In blockchain-based applications, access controls can be enforced through various mechanisms, such as smart contracts, consensus algorithms, and cryptographic protocols. Smart contracts are self-executing contracts with the terms of the agreement between the parties being directly written into lines of code [3]. They can be used to define access control rules for blockchain-based applications. For example, a smart contract can be programmed to only allow a specific set of users to access certain parts of the blockchain or perform specific actions, such as transferring tokens. Consensus algorithms, which are used to validate transactions and add them to the blockchain, can also be used to enforce access controls. For example, a proof-of-work consensus algorithm can require users to solve a computational puzzle to access certain parts of the blockchain, making it difficult for unauthorized users to gain access. Cryptographic protocols can also be used to enforce access controls. For example, public-key cryptography can be used to authenticate users and restrict access to certain parts of the blockchain. This can be done by requiring users to provide a digital signature that matches a specific public key before allowing access [2]. Access control plays an important role in protecting data privacy. However, traditional access control models such as RBAC and ABAC need to be built based on a central trusted server. Once the central trusted server is controlled by an adversary, it will pose a serious threat to data security. A blockchain-based access control schemes are required to be implemented, which uses the blockchain to replace the central trusted server and uses smart

DOI:10.46647/ijetms.2023.v07i04.082 ISSN: 2581-4621

contracts to complete access. Such a scheme solves the centralization problem of the traditional access control model used for web applications [15].

[11] proposed a blockchain-based access control scheme that employs the blockchain as the model's trusted center and uses smart contracts to carry out the access control policy. By executing smart contracts, the resource owner and resource visitor communicate with one another via the blockchain's nodes to complete the access process.

[10] Blockchain is particularly relevant to access control for network systems where authorization processes are based on subject and object attribute data, because of its enhanced security, adaptability, and scalability for management and the enforcement of access control data and procedures. Using function calls to track the status of the global access control system enhances an organization's capacity to check and audit access control operations.

Enigma [4] is a data management platform that is based on both off-chain storage and blockchain for access control. With data ownership, data transparency and auditability, and fine-grained access control, it addresses common privacy challenges. Only references to user data are kept on the blockchain for privacy purposes; the actual data is encrypted before being dispersed around a network of nodes at random and is controlled by a distributed hash table.

Access controls are critical in blockchain-based applications. They can be enforced through various mechanisms, such as smart contracts, consensus algorithms, and cryptographic protocols. Proper access controls ensure that only authorized users can access sensitive information or perform specific actions on the blockchain, preventing unauthorized access and maintaining the integrity of the blockchain. Access control is a critical aspect of blockchain-based applications that determines who has access to specific information or functionality. Access control in the context of online web-based applications refers to the process of determining and restricting access to resources or functionalities within the application based on a user's identity and permissions. It ensures that only authorized users can access and perform certain actions within the application while preventing unauthorized users from accessing sensitive information or performing potentially harmful actions. Access control mechanisms in web-based applications can take various forms, such as login credentials, user roles, and permissions. Users are typically required to provide a username and password to log in to the application. Once authenticated, they may be assigned specific user roles or permissions that determine their access level within the application. For example, an admin user may have access to all functionalities within the application, while a regular user may only have access to specific pages or features. Access control is an essential aspect of web-based applications, especially those that handle sensitive information or perform critical functions. It helps ensure the confidentiality, integrity, and availability of the application and its resources. Additionally, access control mechanisms can help prevent unauthorized access or malicious attacks, which can lead to significant financial and reputational damage.

Access control in the context of blockchain-based applications refers to the process of selectively restricting access to the blockchain's resources or information based on an entity's identity and the permissions associated with that identity. In blockchain-based applications, access control is enforced through various mechanisms, such as smart contracts, consensus algorithms, and cryptographic protocols.

3.1 Public and Private Key Authentication:

Public and private key authentication is a widely used access control mechanism in blockchain-based applications. This mechanism is used to verify the identity of users and secure transactions. For instance, in the Bitcoin blockchain, public and private keys are used to generate digital signatures to validate transactions [1]. Multi-Factor Authentication: Multi-factor authentication is used to provide an extra layer of security to blockchain-based applications. It can include biometric authentication, smart cards, or tokens. For instance, in the Ethereum blockchain, multi-factor authentication is used to secure user accounts. Role-based access control is used to grant access to blockchain-based applications based on a user's role and it is implemented using smart contracts to automate the process of granting permissions to users based on their roles. For example, in the

DOI:10.46647/ijetms.2023.v07i04.082 ISSN: 2581-4621

Hyperledger Fabric blockchain, Role-Based Access Control is used to control access to network resources [17]. Attribute-Based Access Control Attribute-based access control is used to grant access to blockchain based applications based on the user's attributes. It is implemented using smart contracts to automate the process of granting permissions based on attributes such as job title, department, and location. For example, in the Ripple blockchain, Attribute-based access control is used to manage access to financial data [18]. A method for developing, managing, and enforcing access control policies that makes use of blockchain technology. The two key benefits of this method are that the access privileges can be easily changed from one user to another through a blockchain transaction and that the policy is published on the blockchain and therefore visible to the scenario's subjects.

3.2 Smart Contracts:

Smart contracts [8] are self-executing contracts that can be used to implement access control mechanisms in blockchain-based applications. Smart contracts can be used to automate the process of granting and revoking permissions to users based on their roles or attributes. For example, in the Ethereum blockchain, smart contracts are used to implement access control mechanisms for decentralized applications. Permissioned blockchain [9] is used to control access to the blockchain-based application. It allows only authorized users to participate in the blockchain network and access data based on permissions. Permissioned blockchain is used in enterprise blockchain applications, where access control is critical. For example, in the Corda blockchain, permissioned blockchain is used to control access to financial data. [8] have designed a platform for role based access control to utilize across multiple organizations using Ethereum blockchain and Solidity smart contracts. It has implemented a smart contract to initialize the roles and the challenge-response protocol to authenticate the ownership of roles and user verification. ChainAchor is a blockchain platform that enforces access control for users who submit transactions. This paper introduces ChainAchor as a platform to solve the problem of identity and access control in the shared permissioned blockchains. Shared permissioned blockchain is a permissioned blockchain that is shared between multiple distinct organizations. Identity privacy, access control, and optional disclosure & transaction privacy are challenging issues in shared permissioned blockchains. ChainAnchor consensus method looks for the public-key of the sender of the transaction in a database including all the identities information and it forces access control based on that. The identities of the users are anonymous completely and cannot be disclosed by anyone in the system [12].

3.3 Consensus mechanisms:

Consensus mechanisms are used to ensure that only authorized users can make changes to the blockchain-based application. Consensus mechanisms can include proof-of-work, proof-of-stake, and Byzantine fault tolerance. These mechanisms help to prevent unauthorized changes to the blockchain and ensure the security and integrity of the data stored on the blockchain. For example, in the Bitcoin blockchain, proof-of-work consensus mechanism is used to validate transactions. Consensus algorithms are used to validate transactions and add them to the blockchain, and can also be used to enforce access controls. For example, a proof-of-work consensus algorithm can require users to solve a computational puzzle to access certain parts of the blockchain, making it difficult for unauthorized users to gain access. Cryptographic protocols can also be used to enforce access controls. For example, public-key cryptography can be used to authenticate users and restrict access to certain parts of the blockchain. This can be done by requiring users to provide a digital signature that matches a specific public key before allowing access. The importance of access controls in blockchain-based applications cannot be overstated. Without proper access controls, unauthorized users can gain access to sensitive information or perform actions that can compromise the integrity of the blockchain. This can lead to significant losses and damage to the reputation of the blockchain-based application. Therefore, access control mechanisms are crucial in maintaining the security and integrity of blockchain-based applications.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.7 July - August – 2023
DOI:10.46647/ijetms.2023.v07i04.082 ISSN: 2581-4621

Following table includes an analysis of different access control mechanisms in blockchain-based applications, their advantages, and limitations, and their effectiveness in different scenarios.

Table 1. Access control mechanisms in blockchain-based applications

Access Control Mechanism	Advantages	Limitations	Effectiveness in Different Scenarios
Smart Contracts	Can be used to enforce complex access control policies. Can be customized to suit specific use cases	Requires significant development effort to implement. Smart contract vulnerabilities can be exploited by attackers.	Effective for controlling access to blockchain resources based on user roles or permissions. Useful for enforcing access controls for decentralized applications.
Consensus Algorithms	Offers a high level of security and resilience. Can be customized to suit specific use cases	Requires significant computational power to execute. Limited scalability in certain scenarios	Effective for controlling access to blockchain resources based on computational effort. Useful for enforcing access controls for proof-of-work and proof-of-stake blockchains.
Crypto - graphic Protocols	Offers a high level of security and confidentiality. Can be used to enforce granular access control policies.	Requires significant computational power to execute. Difficult to implement and manage.	Effective for controlling access to blockchain resources based on user identity or digital signatures. Useful for enforcing access controls for public-key cryptography-based blockchains.

An analysis of different access control mechanisms in blockchain-based applications, their advantages, and limitations, and their effectiveness in different applications. The findings of this study demonstrate that each access control mechanism has its advantages and limitations, making them suitable for specific use cases. For example, smart contracts are useful for enforcing access controls for decentralized applications, while consensus algorithms are effective for controlling access to blockchain resources based on computational effort. Cryptographic protocols are useful for enforcing access controls for public-key cryptography-based blockchains. The study highlights the importance of access control mechanisms in blockchain-based applications, as they play a critical role in maintaining the security and integrity of these systems. The results of this study can be used to inform the design and implementation of access control mechanisms in blockchain-based applications, improving their overall security and integrity.

CONCLUSION

DOI:10.46647/ijetms.2023.v07i04.082 ISSN: 2581-4621

The paper provides an analysis of various access control mechanisms in blockchain-based applications. The study presented and examined three main access control mechanisms, including smart contracts, consensus algorithms, and cryptographic protocols, to evaluate their strengths, weaknesses, and effectiveness in different use case scenarios. This study provides insights into access control mechanisms in blockchain-based applications, which can help blockchain to design and implement effective access control mechanisms that meet the specific needs of various new use cases. This research will contribute to the existing literature on access control mechanisms in blockchain-based applications by analyzing various access control mechanisms and its effectiveness in different applications. In the next step we are planning to present a service-oriented architecture for blockchain based access control.

References

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org. 2008.
2. Li X., Jiang P., Chen T. et al. A Survey on the Security of Blockchain Systems. Future Generation Computer Systems. 2018; 82:307-324.
3. Buterin V. A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum Foundation. 2014.
4. Zyskind Oz, G., Alex ', N., & Pentland, S. '. (2015). *Enigma: Decentralized Computation Platform with Guaranteed Privacy*.
5. Rouhani, S., & Deters, R. (2019). Security, performance, and applications of smart contracts: A systematic survey. *IEEE Access*, *7*, 50759–50779. https://doi.org/10.1109/ACCESS.2019.2911031
6. Zheng Z., Xie S., Dai H. et al. Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services. 2018; 14(4):352-375.
7. Puthal D., Malik N.M., Mohanty S.P. et al. The Blockchain as a Decentralized Security Framework. IEEE Consumer Electronics Magazine. 2018; 7(2):18-23.
8. Jason Paul Cruz, Yuichi Kaji, and Naoto Yanai. 2018. RBAC-SC: Role-Based Access Control Using Smart Contract. IEEE Access 6 (2018), 12240–12251.
9. Thomas Hardjono and Alex Sandy Pentland. 2016. Verifiable Anonymous Identities and Access Control in Permissioned Blockchains. manuscript in preparation (2016).
10. Hu, V. C. (2022). Blockchain for access control systems. https://doi.org/10.6028/NIST.IR.8403
11. Jiang, X. (2021). A Blockchain-based Access Control Scheme. Journal of Physics: Conference Series, 1955(1). https://doi.org/10.1088/1742-6596/1955/1/012088
12. Le, T., & Mutka, M. W. (2018). Capchain: A privacy preserving access control framework based on blockchain for pervasive environments. Proceedings - 2018 IEEE International Conference on Smart Computing, SMARTCOMP 2018, 57–64. https://doi.org/10.1109/SMARTCOMP.2018.00074
13. Laurent, M., Kaaniche, N., Le, C., & Plaetse, M. vander. (2018). A blockchain based access control scheme. ICETE 2018 - Proceedings of the 15th International Joint Conference on -Business and Telecommunications, 2,168–176. https://doi.org/10.5220/0006855601680176
14. Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., & Yu, K. (2020). AuthPrivacyChain: A Blockchain-Based Access Control Framework with Privacy Protection in Cloud. IEEE Access, 8, 70604–70615. https://doi.org/10.1109/ACCESS.2020.2985762
15. Liu, B., Xiao, L., Long, J., Tang, M., & Hosam, O. (2020). Secure Digital Certificate-Based Data Access Control Scheme in Blockchain. IEEE Access, 8, 91751–91760. https://doi.org/10.1109/ACCESS.2020.2993921
16. Namane, S., & ben Dhaou, I. (2022). Blockchain-Based Access Control Techniques for IoT Applications. In Electronics (Switzerland) (Vol. 11, Issue 14). MDPI. https://doi.org/10.3390/electronics11142225
17. Ferraiolo D, Cugini J, Kuhn D R. Role-based access control (RBAC): Features and motivations[C]//Proceedings of 11th annual computer security application conference. 1995: 241-48.

DOI:10.46647/ijetms.2023.v07i04.082 ISSN: 2581-4621

18. Yuan E, Tong J. Attributed based access control (ABAC) for web services[C]//IEEE International Conference on Web Services (ICWS'05). IEEE, 2005.
19. Ouaddah A, Abou Elkalam A, Ait Ouahman A. FairAccess: a new Blockchain-based access control framework for the Internet of Things[J]. Security and communication networks, 2016, 9(18): 5943-5964.
20. Pinno O J A, Gregio A R A, De Bona L C E. Controlchain: Blockchain as a central enabler for access control authorizations in the iot[C]//GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE, 2017: 1-6.
21. Maesa D D F, Mori P, Ricci L. A blockchain based approach for the definition of auditable Access Control systems[J]. Computers & Security, 2019, 84: 93-119.
22. Ding S, Cao J, Li C, et al. A novel attribute-based access control scheme using blockchain for IoT[J]. IEEE Access, 2019, 7: 38431-38441.