Blockchain-Based Authentication for Secure Data Access Control Measures with an Observation in IoT Device Implementation

Mario J. Montoya Torres
Master in Computer Science – Cybersecurity
Advisor: Nelliud D. Torres Batista, DBA
Polytechnic University of Puerto Rico
Graduate Project EXPO, May 2025

Abstract *— This paper explores implementing blockchain technology as an access control and identity management system to enhance security and data protection within organizations, particularly in environments with increasing IoT device deployments. The study reviews existing blockchain-based access control models, comparing transaction-based and smart contract-based approaches, highlighting their applicability to distributed and dynamic data environments. A proof-of-concept blockchain was developed using C++ and OpenSSL, focusing on trust-based access control for managing user authentication and authorization in a physical headquarters scenario. The paper also discusses scalability challenges and future directions, including integrating Inter-Planetary File System (IPFS) and Directed Acyclic Graph (DAG) technologies to optimize storage and transaction efficiency in large-scale IoT deployments1.*

Keywords *— Blockchain-Bases Access Control, Efficiency Optimization, Identity Management, IoT Devices, Scalability.*

INTRODUCTION

Organizations face significant challenges in implementing secure access controls to protect sensitive data while maintaining regulatory compliance and operational relevance. This project explores blockchain technology as a next-generation solution for access control and identity management systems. The researcher developed a prototype blockchain using existing libraries to analyze use cases, design considerations, scalability challenges, and limitations that inform future implementations.

The project also examines blockchain's potential for securing IoT ecosystems, particularly device authentication and physical access control. Organizations can implement robust security with reduced infrastructure overhead by leveraging decentralized networks, cryptographic protocols, and programming frameworks (Java/Python/C++). Subsequent sections detail IoT integration strategies, access control models, deployment observations, and final performance evaluations of the blockchain prototype.

RELEVANT WORK

What is a Blockchain?

A blockchain is the name of another kind of data structure for storing digital information of a computer professional's choosing, which is often important to a particular process, very similar to a linked list. Blockchain employs cryptographic techniques to maintain its security, and its data structure is, as the name implies, blocks that are chained together to create a "Blockchain." Blockchains work best when specific criteria surface, such as the need for nonrepudiation, preventing modification of stored data, high levels of security, and an effort to decentralize a current technology. A ledger keeps track of existing blocks within the blockchain and serves as a reference or proof that the current blockchain contains the mentioned transactions. Once the ledger is created, it will be copied and shared throughout a network, with each point of access or participant (also called a "node") holding on to a copy of it. Each node within this network is responsible for ensuring that ledgers remain authentic, and a consensus algorithm will agree on the validity of new blocks

when made. Figure 1 is a good visual of the blockchain lifecycle.

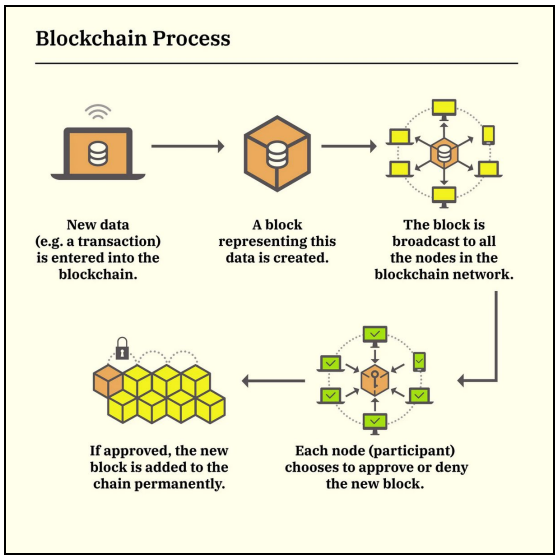

Figure 1
A Visualization of The Blockchain Process [1]

Application Research on Blockchain-Based Access Control

Researchers from the University of Aeronautics and Astronautics in Nanjing, China, are driven by the complexities that the era of big data brings and how it's changed the economic and social constructs humanity has come to know. Because of this surge in vast amounts of data and the continued creation of new data, researchers in China are exploring new opportunities to incorporate known technologies, such as blockchain, as a protective measure for storing big data. Their primary concern stems from current applications of access control models and their difficulty in merging into a distributed and dynamic environment of big data.

Ying and Feng [2] point out that "Blockchain coincides with the needs of distributed deployment, audit mechanism, and trust mechanism that need to be addressed in the access control under the current big data environment, these needs have the characteristics of decentralization, transparent transaction and a trusted mechanism without third-party endorsement."

Their observations focus on analyzing blockchain-based access controls in three ways: what a combination of blockchain and access controls is, observing its first type of implementation as a transaction-based access control (BAC), and a second implementation as an intelligent contract-based access control.

A well-thought-out Blockchain-based access control measure has the advantages of being trustworthy, verifiable, automatic, and fine-grained.

Transaction-Based Access Control

Transaction-BACs take advantage of blockchain as a storage unit in the access control system, making it the sole security provider for the storage process. A transaction BAC grants and revokes access permissions using a central, authoritative server that publishes the transaction permissions. The blockchain pipelines will have to process additional information in the hashing process, such as timestamps, administrative, and subject information packaged within each transaction, on top of the transactions themselves.

Smart Contract-Based Access Controls

Smart contract BACs are implicitly explained as logical lines of code that are automatically executed at the expense of a user's change in data state and behavioral information. They are also considered part of the blockchain. Smart contracts provide supervision, management, information traceability, and policy update loggers capability through pre-determined conditions that users must satisfy for automatic ascension or granted access to an object.

Data Security in the IoT Environment

a) Transaction-BACs: In the case of Transaction-BACs, Ying et al. reference a new framework for transactions-BACs, named FairAccess [3], in which permissions are granted, acquired, delegated, and revoked based on Access Tokens. These Access Tokens are created when the user satisfies a policy stated by the resource owners' definitions. Token owners can pass or entrust access rights to a new owner by transferring existing tokens, though this is

dependent on each device establishing its access policy, challenging contract redundancy, and account management.

b) Smart Contract-BAC in IoT: Multiple smart contract implementations with recognizable mechanisms have been available to IoT, such as in studies referenced by Ying and Zeng, where ABAC and Hyperledger Fabric are combined, and studies done by Liu et al. [4]. Here, researchers deploy simple node access control systems with three primary types such as device contracts (DCs), policy contracts (PCs), and access contracts (ACs)

Table 1
Comparative Table of Transaction-BACs and SC-BACs

	Transaction-BAC	SC-BAC
Representative Models	FairAccess, ControlChain, BBDS.	BlendCAC, Fabric-IoT, Medrec, Ancile, Medshare.
Advantages	1) Transactions are hard to tamper with, providing the possibility to trace access. 2) Managing access tokens safely and decentralized. 3) Supporting access delegation.	1) Adopting automatically and flexibly, without human intervention. 2) Combining with machine learning algorithms to accomplish dynamic access control.
Disadvantages	1) The access decision is made by a single entity. 2) The access decision made by the resource owner and external entities may affect the time response.	Multiple access contracts' interaction may cause huge overhead.
Applications	Trusted storage, access permissions, access policies adoption, sensitive data protection and access operation records storage	Automatic access control, on-chain data management, automatic on-chain data integration, violation detection and access control determinations.

Blockchain-based Access Control Models in IoT Applications

In a similar discussion, researchers from the Department of Computer Science and Information and Logistics at the University of Houston, Texas, review access control frameworks using blockchain technology specifically for IoT devices. With current memory and computational limitations, a mainstream approach to the security and privacy of data is riddled with significant challenges for IoT systems. Traditional access control methods, such as role-based and attribute-based, are observed, and their high dependency on access control lists is observed directly [5].

- Access Control List: ACLs, or access control lists, are a set of rules or permissions that are used to determine who is allowed access to resources. The resources could be files, directories, devices, network segments, or locations, and an ACL is constructed by a large subset of previously defined entries with their permissible operations. Some entities within the entry are allowed to write, read, execute, or change the resource willingly if decided by the administrator of said ACL.

Because accessing ACLs is inevitable for looking up transaction updates, it is consequential that a lot of computational overhead is produced. Some implementations, such as the Bitcoin framework [6] and Ethereum, use Merkle Trees and Merkle Patricia Tries (MPTs) to combat this (see Appendixes A through C to learn more about these data structures). These allow the frameworks to efficiently handle data hashing for a long list of transactions within a block, keeping track of them in an efficient and limited way that can prevent DDoS attacks for the blockchain.

a) Trusted-Based Access Control method: It strictly depends on cryptographic methods such as verification and signing of digital signatures of the parties involved in the transactions. This system requests the verification of users' identities to grant permission to access the system. There have been additional discussions by other professionals in the field that propose control systems that address the right to transfer access from one user to another. Other works, like the one from Steichen et al. [7], solve the resource-sharing constraints while reducing the chain size effectively by developing an access control system using an Ethereum-based Interplanetary File System (IPFS). Other authors did something similar, such as Nguyen et al. [8]. but with Amazon cloud computing as their implementation. In the case of a separate paper by Wang et al. [9],

they promote trust on the chain through key management by smart contract policies from Ethereum.

b) Multi-layer Access Control: Multi-layer access controls distribute the computation using a hierarchical architecture that includes servers with more memory and computational resources. Other applications, such as Zhan et al. [10]. develop a contract-based access control management system that consists of a judge contract that receives misbehavior reports from the access control contracts about the subject attributes and dynamically validates the access control policies accordingly. Their AC methods and policies are managed using an Ethereum-based smart contracts platform.

METHODOLOGY FOR CREATING A PERSONALIZED BLOCKCHAIN

The foundation for any blockchain requires a handful of easily accessible key pieces, primarily a programming language. Thanks to its object-oriented programming features, C++ is a commonly used and powerful high-level language that allows developers to make precise memory management adjustments and create their data structures on the go. Secondly, an encryption scheme is necessary, and although there are multiple protocols that can perform this task well, the "OpenSSL" library has been a powerful security and privacy tool in the C++ landscape for some time now. In this implementation, ED25519 was the chosen asymmetric encryption schema for creating key pairs for wallets enrolled in the blockchain. There are already tens of use cases of blockchains on the web that are very well explained, though these are typically much smaller, simpler in scale, and with some present ambiguity.

Fletelli42, also known as Florian Letellier on GitHub [11], has a popular public repository titled "SimpleBlockchainImplementation" that perfectly serves the objectives of this capstone. The only downside to his codebase is that it was critically outdated. It was released two years ago, and many lines of code have been deprecated as of today. Much of the project's structure will be cited because the class relationships have an acceptable blockchain configuration that presents the following key features: adjustable scalability, functionality for the proposed context, and serves as a good introduction to the complexities of blockchain. By reviving this repository, proof is provided that a blockchain can be used for authentication control measures using open-source libraries and outdated code repositories. This could aid future developers by sharing the knowledge and tools for creating personalized approaches to data security.

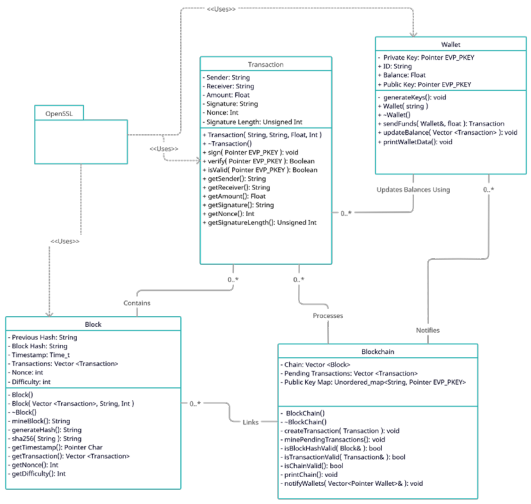

Figure 2
Blockchain's Backend Structure: A UML Class Diagram of The Hard Code

Key Influences on Access Controls Using the Proposed Blockchain

A blockchain based on access control efforts using identity and authentication management protocols is selective when taking in information about each identity, hoping to make each step where access is performed or granted auditable. This methodology proved to be an ideal scenario for users who can provide some form of authenticity and nonrepudiation whenever their wallet forms part of the network. Thanks to the flexibility of each class, which forms part of this blockchain, developers have complete control of

policy assignment and access rights, determining which access control method is favorable. Previous works referenced on blockchain-BACs in IoT applications and current findings emphasize the dependency of a peer-to-peer network during deployment for a better understanding of why a trusted-BAC will likely be the choice for the proposed blockchain managerial tasks. For the blockchain network to be deployed at the IoT level, each IoT device must have the resources available to carry a copy of the digital ledger of transactions. Security comes from the collaboration of multiple devices with individual databases with the same static information or ledgers, but dynamic enough that each device can evaluate trust through certificates, reputation systems, or transaction histories. This allows for the convolution of tampering to flourish, preventing bypasses of the system's records and tricking devices into either accepting unauthorized users or changing existing ones.

Proposed Blockchain Against Relevant Studies

If the purpose of this blockchain is to track and manage user information throughout a physical headquarters with critical access points and restricted areas, using trusted BACs, then digital entities can be created for each player. This blockchain can provide transparency and security while tracking their movements throughout the site, with as little intrusion as possible, and ensuring physical security measures are carried out with minimal oversight and the capability of fraud. On the other hand, if the employee actors remain static for long and the landscape is rarely changed, it was observed that transactions can easily pile up, which is especially dependent on scalability. This means that ACLs might eventually be implemented. Zhang et al. [5], in their research on blockchain-based AC models for IoT, argue that looking up transaction updates is consequential and produces much computational overhead. Like their proposed observation, this blockchain methodology would thereon benefit greatly from Merkle Trees or Patricia Trie as a solution. As previously mentioned, these allow the frameworks to efficiently handle data hashing for a long list of transactions within a block, keeping track of them in an efficient and limited way that can prevent DDoS attacks for the blockchain and IoT devices, respectively.

Future Work and Consideration

A paper on blockchain-based Electronic Evidence Storage and Efficiency Optimization by researchers of the School of Computing at Qinghai Normal University, China [12], brings a valid discussion that is the solid groundwork for future deployments and research for the cybersecurity landscape since it encourages solutions to storage efficiencies of digital evidence by providing optimizations through acyclic graphs for on-chain storage. The proposed uses Inter-Planetary File System (IPFS) technology in a blockchain environment that benefits from storage models devised for electronic evidence. IPFS is explained in the following subsection.

Inter-Planetary File System

The IPFS is a content-addressable point-to-point distributed file storage system and transport protocol with nodes that form the distributed system and act as links in the form of encrypted hashes. Files are obtained through a distributed hash table from a network built by the IPFS. IPFS nodes can easily find content due to their distributed nature and expand the storage capacity of a blockchain.

Because IPFS is associated with low costs of data storage, fast download speed, distributed characteristics, and security, the paper introduces it as the primary storage model architecture of blockchain-based electronic evidence. As the number of users grows, the scalability of the blockchain must remain uncompromised, something that could promote itself as a challenge for deployments that require a larger environment with hundreds of IoT devices. IPFS thus solves the excessive amount of data and prevents any effects

on the consensus efficiency of the blockchain while reducing the efficiency of the resource access.

Evidence Storage Efficiency Optimization and Experimental Analysis

When scalability becomes a challenge, Zhikun et al. [12] address this by experimenting with and analyzing Directed Acyclic Graph technology as their project focus. They argue that present implementations bottleneck current blockchain technology. Transactions in traditional blockchains are processed sequentially, which is also correct for this Capstone's implementation, adding a large workload or proof of work calculations that are inefficient per block creation. A DAG implementation allows various new features not specific to blockchain technology and solves their storage and efficiency constraints. It does this thanks to its Directed Acyclic behavior of nesting the data; each transaction considers its data into a topology that defines a partial ordering protocol for the blocks.

According to researchers, a successful DAG implementation can optimize the transactions processed per second (TPS), a system performance measurement, by about 30.4%. DAGs are considered a good, practical, and scalable alternative to current blockchain technologies when housing vast amounts of data.

CONCLUSION

It was concluded that the current versions of the OpenSSL library successfully adapted into an updated blockchain implementation, with most of its deprecated functions being replaced to serve their utility correctly. Updates such as the signing and verification of hashes for transactions and the key-generating schemas for asymmetric key pairs are important steps in providing security through encryption for each of the wallets participating in this blockchain. For the moment, the output is more concerned with usability than an intricate implementation of the chain in an IoT environment.

However, with the acquired references, experience, and knowledge from at least designing a functioning blockchain as the backbone of this project, such integrations into the proposed landscape and efficiencies in storage and digital evidence observed are accessible for future projects and professional enthusiasts alike. Current findings also highlight how a blockchain's architectural constraints can impact performance and efficiency in real-world deployments.

APPENDIX A

What is a Merkle Tree?

Merkle Trees were developed by Ralph Merkle in 1979 to hierarchically organize data by means of hashes. It’s primarily used to provide efficiency and security when verifying large datasets. Like the name implies the structure of this cryptographic data structure forms that of an upside-down tree, with components such as leaf nodes at the extremities, non-leaf nodes joining these extremities, and the Merkle tree root at the top. The leaf nodes contain hashes of individual data. In the case of this discussion, the data can be considered as one transaction in a blockchain, while the non-leaf nodes store a hash of their child nodes, and the Merkle root is the topmost hash representing the complete dataset. Each hash within a Merkle tree (its leaf nodes) is a transaction that can be referenced, paired, and combined, and that combination is rehashed iteratively until a single root (the Merkle root) is left. Hash verification is accomplished through computational steps that are logarithmically proportional to the dataset size.

In blockchain, a Merkle tree is ideal for providing data integrity through hashing algorithms, efficiency for transaction verification, and it serves as an optimal storage structure for blocks, thanks to only requiring each block to store a Merkle root rather than a large list of transactions.

APPENDIX B

What is Patricia Trie?

A Patricia trie is also known as a Patricia tree or a radix tree, though "Patricia" is really an acronym that stands for "Practical Algorithm to Retrieve Information Coded in Alphanumeric." A Patricia trie purpose is to provide a path to a node, where nodes that contain only one child are compressed into a single edge. This helps in reducing space and increasing search operations. Nodes form part of a string or binary key, and distinct branches of the tree are represented by a different set of key values. This greatly aids in the efficiency of searching, inserting, and deleting strings. Figure 3 provides a visual example of a Patricia trie.

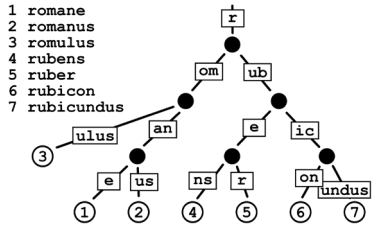

Figure 3
Graphical Representation of a Patricia Trie [13]

APPENDIX C

What is a Merkle Patricia Trie (MPT)?

Just as the name implies, Merkle Patricia Tries (MPTs) are simply the combination of Merkle trees and Patricia Tries to create a specialized data structure that takes advantage of both of their features to efficiently store key-value pairs. It uses the same hashing principle for data integrity as the Merkle tree, making node storage tamper-proof thanks to its quick detection and cryptographic verifications. Tampering would appear in the root hash of the tree if any of its underlying nodes are ever edited. The key-value storage aspect is supported thanks to Patricia tries because of scalable management of dynamic datasets and node compression that helps in minimizing redundancies.

REFERENCES

[1] G. Rodriguez Cruz, "What is Blockchain?," in *Money Group LLC,* June 2, 2022. [Online Article] Available: https://money.com/what-is-blockchain/. [Accessed: November 13, 2024].

[2] Y Zhu and F. Xu, "Application Research on Blockchain-Based Access Control," in *2021 2nd Int. Conf. on Comput. Sci. and Manage. Technol. (ICCSMT)*, Shanghai, China. Nov. 13, 2021. [Online Library]. Available: https://ieeexplore.ieee.org/document/9786969. [Accessed: November 15, 2024].

[3] A. Quaddah, A. Ouahman, A. Elkalam. "Fairness: A New Blockchain-based Access Control Framework for The Internet of Things." in *Secur. and Commun. Netw. LLC, Research Gate,* February 02, 2017. [Online Publication]. Available: https://www.researchgate.net/publication/313847688_FairAccess_a_new_Blockchain-based_access_control_framework_for_the_Internet_of_Things_FairAccess_a_new_access_control_framework_for_IoT. [Accessed: November 15, 2024].

[4] L. Han, H. Dezhi, and L. Dun. "Fabric-IoT: A Blockchain-based Access Control System in IoT." in *IEEE Access*, vol. 8, January 21, 2020. [Online Library]. Available: https://ieeexplore.ieee.org/document/8964343. [Accessed: November 15, 2024].

[5] Y. Zhang, A. Memariani, and N. Bidikar. "A Review on Blockchain-based Access Control Models in IoT Applications," in *IEEE 16th Int. Conf. Paper*, Singapore. October 9-11, 2020. [Online Library]. Available: https://ieeexplore.ieee.org/document/9264499. [Accessed: November 17, 2024].

[6] S. Nakamoto. "Bitcoin: A peer-to-peer Electronic Cash System," in *White paper*, October 31, 2008. [Online Article]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: November 15, 2024].

[7] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State. "Blockchain-based, Decentralized Access Control for IPFS," in *2018 IEEE Int. Conf. on IoT (iThings) and IEEE Green Comput. and Commun. (GreenCom) and IEEE Cyber, Physical and Social Comput. (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, July 30, 2018. [Online Library]. Available: https://ieeexplore.ieee.org/document/8726493. [Accessed: December 1, 2024].

[8] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne. "Blockchain for Secure EHRs Sharing of Mobile Cloud-Based E-Health Systems" in *IEEE Access,* vol. 7, May 17, 2019. [Online Library]. Available: https://ieeexplore.ieee.org/document/8717579. [Accessed: December 1, 2024].

[9] S. Wang, X. Wang, and Y. Zhang. “A Secure Cloud Storage Framework with Access Control Based on Blockchain” in *IEEE Access,* vol.7, July 23, 2019. [Online Library]. Available: https://ieeexplore.ieee.org/document/8770246. [Accessed: December 1, 2024].

[10] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan. “Smart Contract-Based Access Control for the Internet of Things” in *IEEE Internet of Things Journal*, vol. 6, no. 2, June 15, 2018. [Online Library]. Available: https://ieeexplore.ieee.org/document/8386853. [Accessed: December 10, 2024].

[11] F. Letellier. “Simple Blockchain Implementation” in *GitHub Repository*, August 29, 2023. [Online]. Available: https://github.com/fletelli42/SimpleBlockchainImplementation. [Accessed: February 20, 2025].

[12] Z. Miao, C. Ye*, P. Yang, Y. Chen, and Y. Chen. “Blockchain-based Electronic Evidence Storage and Efficiency Optimization” at *2022 6th Int. Conf. on Cryptography, Secur. and Privacy (CSP),* Tianjin, China, January 14-16, 2022. [Online Library]. Available: https://ieeexplore.ieee.org/document/9845257. [Accessed: February 20, 2025].

[13] Alchemy Doc. “What are Patricia Merkle Tries?,” in *Alchemy Insights, Inc.*, 2023. [Online Article]. Available: https://docs.alchemy.com/docs/patricia-merkle-tries. [Accessed: April 20, 2025].