IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Blockchain based identity and access management in Operating systems

S.NO	AUTHOR NAME	DESIGNATION	INSTITUTE NAME
1	MOHAMMED JAVED HUSSAIN	STUDENT	VIT VELLORE
2	MALLIPAAMU RAJKUMAR	STUDENT	VIT VELLORE
3	ELURI DINDI BHARADWAJ	STUDENT	VIT VELLORE

Abstract

This research paper explores the integration of blockchain technology into identity and access management (IAM) systems in operating systems. Traditional IAM systems face challenges related to centralised control, privacy, and security vulnerabilities. Blockchain, with its decentralised and immutable nature, has emerged as a potential solution for enhancing IAM capabilities. This paper reviews the existing literature on IAM and blockchain, highlighting the benefits and limitations of their integration. The research methodology includes a comprehensive literature review and analysis of case studies and implementations. The study evaluates how blockchain technology can improve identity verification, authentication, and access control in IAM systems. Additionally, the paper examines the benefits and challenges associated with blockchain-based IAM, addressing scalability, privacy, and regulatory considerations. Real-world case studies and successful implementations are analysed to provide insights and lessons learned. The research identifies future directions and research opportunities for advancing blockchain-based IAM systems. The findings contribute to the understanding of the potential of blockchain technology in revolutionising IAM in operating systems, paving the way for secure and decentralised identity management solutions.

Introduction

[1]A blockchain is a distributed, immutable, and decentralised ledger at its core that consists of a chain of blocks and each block contains a set of data. The blocks are linked together using cryptographic techniques and form a chronological chain of information. The structure of a blockchain is designed to ensure the security of data through its consensus mechanism which has a network of nodes that agree on the validity of transactions before adding them to the blockchain.

[2]Access Management: One source of truth for identity and associated access credentials — building visibility across department units and industries for better enterprise security.

Identity Management: The idea of "self-sovereign" identity — where users autonomously control their data and can prove its legitimacy on a turnkey basis, bypassing administrative third parties and bringing privacy to consumer data

Integration of Blockchain Technology into IAM Systems

3 10 ways blockchain improves IAM

There are several use cases where blockchain technologies -- or blockchain-inspired designs -- may improve IAM processes. These include the following :

1. Multiparty verification

Multiparty verification involves the replacement of a central identity service company with a group of entities, governed by a network and owned by a joint venture or consortium. This is the broadest vision for applying DLT to IAM systems for greater efficiencies, though complexity of coordination across parties has limited adoption at scale.

2. Verifiable credentials

According to the World Wide Web Consortium (W3C), "Verifiable credentials represent statements made by an issuer in a tamper-evident and privacy-respecting manner." They are a crucial component of identity verification, and DLT represents opportunities to "digitally watermark" a fixed claim. Just as blockchainbased non-fungible tokens have enabled artists to digitally watermark their original media, a similar capability can be applied to verifying identity credentials. That said, companies should not store personally identifiable information (PII) on-chain; they should only store the hash of the claim on-chain.

3. Distributing attributes

In public blockchain architectures, or hybrid architectures built on open source software, access is not limited and there is potential for global search and discoverability of attributes without requiring a central directory. Such transparency can threaten privacy principles, but with additional layers of privacy engineering, more accessible distribution has the potential to improve financial inclusion and help enfranchise those unable to prove their identity.

4. Accessing attributes

Attributes could be encrypted and smart contracts -- the terms of encoded logic and algorithms on a blockchain -- could be encoded to decrypt them when needed. To avoid storing PII or attributes themselves on a blockchain, only the signature of the hash of the attributes should be stored on the ledger, while the user presents the attributes from their device.

5. Attribute provenance

How do we know the origin and accuracy of identity attributes? After all, an attribute is only as reliable as our confidence in its source. Just as a shared ledger has improved transparency and efficiency in tracking food across the supply chain, a shared ledger could potentially create transparency in the timestamps of sources issuing identity attributes. This same capability could be useful for key lifecycle management, specifically for synchronous visibility into the lifecycle metadata of cryptographic keys -- i.e., who has access to what. The academic world is considering its use because it could assist with verification and authenticity of certifications and hiring credentials.

6. Data minimisation

What do service providers actually need to know to authenticate someone? Various DLT capabilities, such as smart contracts, zero-knowledge proofs or selective disclosure, can be configured to minimise which data or attributes are required for verification and which are never revealed.

7. Audit trails

In many enterprise contexts, creating a log of interactions is not only an operational and security best practice but a requirement for regulatory compliance. While a blockchain is not compulsory when logging information for an audit -- e.g., a user is enrolled, a user logs in, a user requests permissions or a user is deactivated -- it can be useful for synchronisation across parties, maintaining log integrity and reducing the potential for tampering or fraud.

8. Compliance verification

Another use case enabled through shared audit trails is compliance verification, as auditors can be permission-based stakeholders within the shared ledger network. Many enterprise identity use cases also require compliance verification, such as know your customer (KYC) in financial services. In this example, the IAM-blockchain convergence would not remove the need for the central authority -- in the case of KYC, a government authority -- but could offer greater efficiency for both individuals and banks. A bank could "see" and attest that other banks have conducted KYC due diligence and verified the customers' identities, all while reducing the bank's costs.

9. Self-sovereign identity (SSI)

Though the concept of full self-determination and shifting control of all attributes back to the end user long predates blockchain and IAM, DLTs have inspired several innovative designs to enable greater self-determination around personal data. Examples include consensus algorithms specifically designed for attribute reliability. Despite the potential for SSI, some higher-risk enterprise use cases -- for example, in healthcare or financial services -- may always require an external authority to validate identity claims.

10. Decentralised identifiers (DIDs)

DIDs are identifiers controlled entirely by the identity owner, independent of centralized authorities or providers. These are a component of SSI, designed to be user-controlled, unable to be reassigned and resolvable. This means they contain documentation of public keys, authentication protocols and verifiability via cryptography or an issuing authority's signature.

Benefits and challenges of Identity and Access Management Systems

4 Key Benefits of Identity and Access Management Systems

1. **Eliminating weak passwords**—research shows over 80% of data breaches are caused by stolen, default, or weak passwords. IAM systems enforce best practices in credential management, and can practically eliminate the risk that users will use weak or default passwords. They also ensure users frequently change passwords.

2. **Mitigating insider threats**—a growing number of breaches is caused by insiders. IAM can limit the damage caused by malicious insiders, by ensuring users only have access to the systems they work with, and cannot escalate privileges without supervision.

3. **Advanced tracking of anomalies**—modern IAM solutions go beyond simple credential management, and include technologies such as machine learning, artificial intelligence, and risk based authentication, to identify and block anomalous activity.

4. **Multi-factor security**—IAM solutions help enterprises progress from two factor to three factor authentication, using capabilities like iris scanning, fingerprint sensors, and face recognition.

Challenges faced by blockchain based identity and access management in operating systems

1. System Integration

[5]System Integration is defined as the process of bringing together the component sub-systems into one system (an aggregation of subsystems cooperating so that the system is able to deliver the overarching functionality)

2. Resource Consumption

Blockchain networks typically require significant computational resources, including processing power and storage capacity. Implementing a blockchain-based IAM system within an operating system may increase resource consumption, potentially impacting system performance and efficiency.

3. Access Control Granularity

Traditional operating systems offer fine-grained access control mechanisms that allow administrators to define access rights at various levels (e.g., file, folder, network). Designing a blockchain-based IAM system that preserves this level of access control granularity while leveraging blockchain's decentralised nature can be challenging

4. Authentication and Identity Verification

Operating systems often rely on traditional authentication methods such as passwords, biometrics, or cryptographic keys. Integrating blockchain-based identity verification mechanisms into the operating system, such as decentralised identity (DID) models or self-sovereign identity (SSI), requires careful consideration of compatibility, security, and user experience

5.System performance and Impact

The additional computational overhead and data storage requirements introduced by blockchain-based IAM systems may impact the overall performance of the operating system. It is crucial to strike a balance between the security benefits offered by blockchain and the efficient operation of the operating system.

6. Upgradability and Maintenance

Blockchain technology evolves rapidly, with frequent protocol updates and security patches. Ensuring the upgradability and maintenance of a blockchain-based IAM system within an operating system environment requires robust mechanisms to handle updates, compatibility, and data migration.

Case study

[6]According to the case study There are a few issues with using blockchain

Issue 1: usability

First, it heavily is based on the consumer proudly owning and securing their private key. This is often a usability hurdle – there's a want to recognize what a private secret is inside the first area, the user wishes to put in writing down healing phrases or hazard dropping their account as there's no centralized account recovery. There's obviously the cloud key storage offerings which ideally depend upon a password-based key to encrypt what's stored in the cloud. This in the long run way the profile is covered by way of a trifling password, regardless of all of the underlying cryptography.

Issue 2: many cases require a central authority

the second difficulty is the complexity of attesting attributes – in lots of real-international use-instances you need a centralized authority to certify the attributes. Be it a government, a bank or similar institution. So for realistic motives, we nonetheless rely upon centralized consider, even though the era itself is shipped. It does deliver flexibility to the consumer, of route, and has help for multiple attesting our bodies for unique contexts, but in which it subjects (e.g. banks doing KYC), you usually turn out to be with verifying the identification report issued by way of a central authority authority.

Issue 3: flexibility for the enterprise

The 0.33 issue is the flexibility in phrases of the employer. going for walks the blockchain infrastructure in a centralized fashion loses the decentralized advantages, at the same time as maintaining the complexity of it. alternatively, relying on the decentralized community means the employer has plenty much less manipulate on the governance, and they should truely have their personal layer ontop of that that can handle authorization. In that sense, a standard IAM is tons extra applicable for the business enterprise.

out of doors the scope of the agency, but, self-sovereign identity remains an thrilling frontier which, despite the fact that not universally applicable, may be utilized in certain cases in preference to the broken username/password pairs.

Conclusion

In conclusion, this research paper highlights the promising potential of integrating blockchain technology into identity and access management (IAM) systems in operating systems. The study demonstrates that traditional IAM systems encounter significant challenges related to centralization, privacy, and security vulnerabilities. By leveraging the decentralized and immutable nature of blockchain, IAM systems can be enhanced to overcome these limitations.

Throughout the paper, a thorough literature review and analysis of case studies and implementations were conducted to evaluate the benefits and limitations of blockchain-based IAM. The research emphasises the positive impact of blockchain on identity verification, authentication, and access control, while also addressing the challenges such as scalability, privacy, and regulatory concerns.By examining real-world case studies and successful implementations, valuable insights and lessons are provided, showcasing the practicality and effectiveness of blockchain-based IAM solutions. The paper concludes that the integration of blockchain technology holds the potential to revolutionize IAM in operating systems, leading to more secure and decentralized identity management solutions.

In summary, this research not only contributes to the understanding of blockchain's significance in IAM but also offers directions and research opportunities for further advancing blockchain-based IAM systems. The findings presented in this paper serve as a significant stepping stone toward the future development of secure and efficient identity and access management within operating systems.

References

1) https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology#:~:text=Blockchain is a method of,computers participating in the blockchain.

2) https://medium.com/fluree/blockchain-for-identity-access-and-credentials-management-e622cc285af3

3) https://www.financemagnates.com/cryptocurrency/education-centre/blockchain-based-digital-identitybenefits-risks-and-implementation-challenges/#

4) https://www.imperva.com/learn/data-security/iam-identity-and-access-management/

5) https://www.financemagnates.com/cryptocurrency/education-centre/blockchain-based-digital-identitybenefits-risks-and-implementation-challenges/

6) https://logsentinel.com/blockchain-use-cases-for-iam/