Journal of Network Communications and Emerging Technologies (JNCET)
Volume 13, Issue 2, April (2025)

A Review of Blockchain Based Identity Management for Cloud, Fog, IoT and Enterprise Systems

Anant Wairagade
Independent Researcher, NIT Nagpur Alumni, Phoenix, Arizona, USA.
vanant@gmail.com

Nikhil Gupta
Independent Researcher, IIT Bombay Alumni, San Francisco, California, USA.
nikhil_gupta@berkeley.edu

Vijay Govindarajan
Independent Researcher, Colorado State University Alumni, Redmond, Washington, USA.
vijay.govindarajan15@alumni.colostate.edu

ABSTRACT

In the realm of technology, the need to validate and secure digital identities among different environments, including cloud, fog computing, Internet of Things (IoT), and enterprise systems, is more than ever. Traditional identity management systems, though aiming to provide the solution, suffer from data breaches because of dependence on centralized architecture and further encounter challenges. The incorporation of blockchain into identity management gives a decentralized, tamper-proof ledger along with robust cryptographic protocols that improve the security challenges of authentication, authorization, and privacy. This article reviews the existing blockchain based identity management methods in the field of cloud, fog computing, IoT, and enterprise systems. A critical analysis was performed which highlighted these methods strengths in providing security while pointing out limitations in the form of energy, latency, communication overhead, and scalability concerns. Furthermore, existing use cases of blockchain platforms that employ identity management solutions such as IoTeX, IOTA, Neblio, Kaleido, Sovrin, SelfKey, Civic, VerseOne are also explored, and a comparison is made between them. Moreover, an evaluation is performed under specific criteria to show which systems work efficiently under specific criteria. On the basis of evaluation of existing literature and use cases, several challenges came to light, such as lack of scalability, performance issues, and compliance with the regulatory framework. Future directions provide insights into a possible improvement, such as improving scalability and performance, and the use of quantum-resistant algorithms to improve security and enhancing interoperability standards to address existing challenges. Overall, this study gives a detailed roadmap for researchers and identity management practitioners which aim to develop efficient blockchain based identity management systems, balancing strong security and performance while keeping compliance in evolving landscape of IoT, cloud, fog computing and enterprise systems.

Index Terms – Blockchain, Identity Management, Blockchain Based Identity Management, Resource Limited Environment, Decentralized Identity Management.

1. INTRODUCTION

In this evolving technological environment, the need for cybersecurity is more than ever. Identity management is one of those emerging cybersecurity solutions that ensure that devices, entities, and individuals are authenticated and authorized accurately in a network [1]. The increasing trend and reliance on online platforms for sensitive transactions further increase the need for effective identity management (idM). According to the report by [2], 1 billion records globally were exposed because of data breaches in 2024. This indicates the dramatic increase in the number and nature of cyberattacks that targeted identity management systems. The use of weak identity verification methods in enterprises often poses vulnerability contributing to cyberattacks [3-4]. According to the 2024 Verizon Data Breach Investigations Report [5], weak identity verification has resulted in over 77% of data breaches caused by weak passwords compromised credentials, and managed permissions. The results of such breaches not only result in huge financial losses but often leads to reputational damage and strict regulatory penalties under laws such as GDPR.

The increasing reliance on distributed architectures like cloud, fog computing, and Internet of things (IoT) further increases these challenges. Cloud and fog environments incorporate identity management to ensure access is controlled towards the resources and unauthorized entities or devices cannot exploit the authorization to gain access to resources [6-8]. According to [9], by 2025 99% of the cloud security failures will be because of weak identity controls. Similarly, in the IoT, the huge amount and diverse nature of connected devices results in identity challenges.

A single IoT system might require millions of devices and each of them needs strong authentication and authorization methods to navigate cybersecurity attacks such as man in the middle (MiTM), spoofing, unauthorized access, and others [10-11]. According to McKinsey, cyber vulnerable IoT systems will result in huge economic losses exceeding 1 trillion dollars annually by 2025 [12]. Most of these losses will be related to attacks because of weak identity management systems [13]. This indicates that strong identity management is no longer a choice but is necessary part of securing digital infrastructures. Apart from mitigating unauthorized access they also provide security against evolving cyber threats along with scalability features which are necessary towards digital environment.

The traditional methods of identity management mostly rely on centralized architecture, which results in single-point failure along with their vulnerabilities towards data breaches and user privacy [14]. Furthermore, these central entities are targeted by cyber attackers to gain sensitive information, such as passwords, which makes them a suitable choice for cyber attackers [15]. Blockchain integration with identity management offers the solution to these problems by offering a decentralized and immutable ledger, thus removing the requirement for a centralized entity, and removing the single point failure while improving security [16]. Furthermore, the employment of blockchain in identity management ensures that when the data is recorded, it cannot be modified, thus resulting in a temper proof verification [17]. Furthermore, it also ensures that users can keep full command of their digital identities and provide the permissions securely and selectively without requiring a third party for validation [16]. The employment of smart contracts in blockchain also enhances identity management by improving automation processes such as role-based access control or multi-party verifications [18]. For example, enterprises using blockchain can incorporate dynamic access control to ensure that permissions are adapted in real-time to meet the requirements of compliance [19]. The integration of blockchain in identity management results in a shift from traditional identity management to an enhanced and efficient user centric mode that provides security with efficiency.

Over the years, blockchain based identity management has been deployed for overcoming security challenges within cloud computing, fog computing, IoT, and enterprises by employing decentralized and cryptographic secure architecture. In cloud, where the sharing of resources and dynamic scalability further enhances the risk of unauthorized access and insider threats, the employment of blockchain provides robust and immutable access controls and reduces the risk of credential theft in cloud [20]. Its employment for identity management in fog computing ensures that authentication is geographically distributed among the nodes. This results in safe communication between the edge devices and the fog layers while minimizing the cyberattacks such as node impersonation attacks and data tampering attacks [21]. Furthermore, its immutable nature provides data integrity even in environments like fog computing which provides a protocol for efficient operation [22]. In an IoT environment, blockchain based idM ensures critical challenges like unauthorized data access and device spoofing attacks using decentralized identities and lightweight cryptographic methods to provide tamper proof device to device communication [23]. Furthermore, enterprise security can be further improved through blockchain identity management which provides a means of securing integrations between modern frameworks and legacy systems [24]. Moreover, it enables strong privacy preserving mechanisms, and also helps effective access control through smart contracts, making sure that permission adapts dynamically to evolving security threats.

In this article, we aim to provide a review of blockchain-based identity management in cloud, fog computing, IoT, and enterprise systems, as these environments require strong identity management to ensure security along with compliance and scalability. This review also explores the current state of the art methods used for blockchain based identity management in these domains. Furthermore, this work also performs a comprehensive assessment of existing methods to point out the advantages, and limitations of these methods and their applicability in real world environments. Furthermore, this review highlights the real-world use cases of blockchain based identity management in the cloud, fog computing, IoT, and enterprise system to evaluate their effectiveness in mitigating cyberattacks and the impact on performance. Through this study, we aim to identify critical challenges in existing work and provide a future roadmap for researchers to provide the opportunity to perform innovation to improve blockchain identity management in the mentioned domains. To our knowledge, his is the first review of its kind that thoroughly explains blockchain based identity management across IoT, cloud, fog computing, and enterprises, while previous studies have only focused on single domains.

2. BACKGROUND

2.1. Identity Management (idM) System

Identity management is a detailed and structured framework designed to protect and verify the digital identities of individuals, services, and devices inside an organization [25]. Nowadays, organizations are increasingly relying on huge networks and interconnected systems, ensuring that parties involved in the network can interact, authenticate, and authorize the resources [26]. The crucial aspect of the IdM system is to make certain that the right entities are given access to appropriate resources at the right time and under appropriate circumstance for the correct reason [27]. This is achieved through the use of a variety of structured

policy tools and technologies which basically formulate the entire life cycle of digital identities, from their creation to management and then deactivation and deletion. This method involves various components from protection, to authenticating, and authorizing the identity credentials, and then monitoring access rights to ensure that information and system remain safe from unauthorized breaches [28-29].

2.1.1. Key Components of Identity Management System

The key components of any idM system involve a series of processes and methods that are produced to provide security and efficiency along with scalability in distributed environments. The core of any idM system relies on the digital identity and the processes associated with it. The digital identity forms the basis of a representation of an entity which can be any device or a user or any application inside a network [30]. It further comprises several key elements. Among them, the first is identifiers which have a unique attribute that make an entity different from another. The identifiers include usernames, email addresses, or device IDs. These identifiers are further tied to credentials such as passwords or biometric private keys, which are often used to authenticate entities [31]. Another important component of digital identity is the attribute, which contextual information such as the rules of permission or the level of security clearance. These components form the basis of digital identity and act as a bridge between an entity and a system to ease controlled and secure access to the organization resource [31].

An idM system is the management of digital identities, which is handled by the identity lifecycle management that ensures that identities are safe, remain relevant, and update through a period of usage [32-33]. This lifecycle as shown in Figure 1 starts with a phase called provisioning in which identities are generated and granted permission based on the roles. At this stage, authentication and password management are also implemented to ensure secure access. Once these identities are in working mode, they need constant synchronization to affirm consistency among different platforms and systems. This phase makes use of self-service tools to handle their credential effectively. Access updates are essential in this context to modify permission to match the organization needs [33]. In such a phase, authorization methods play an important role in providing efficient access policies. Furthermore, governance practices are also employed in this phase to ensure compliance with regulatory standards [32-33]. Lastly, de-provisioning deactivates the identities thus revoking access rights and preventing users' access to the resources any further policies [34].

The identity management processes include authentication, authorization auditing, and monitoring which are essential in safeguarding access to resources. The first method of defense in the idM system is authentication which verifies that entities are legitimate and authentic. Methods like multifactor authentications along with biometrics or authentication tokens are also used for improved authentication and robust security. Modern systems also incorporate federated authentication which ensures that users can gain access to multiple systems with a single legitimate identity among different domains, which while ensuring security also improves usability. Furthermore, cryptographic keys and biometrics, and password less authentication are also employed to ensure robust security [35-37].

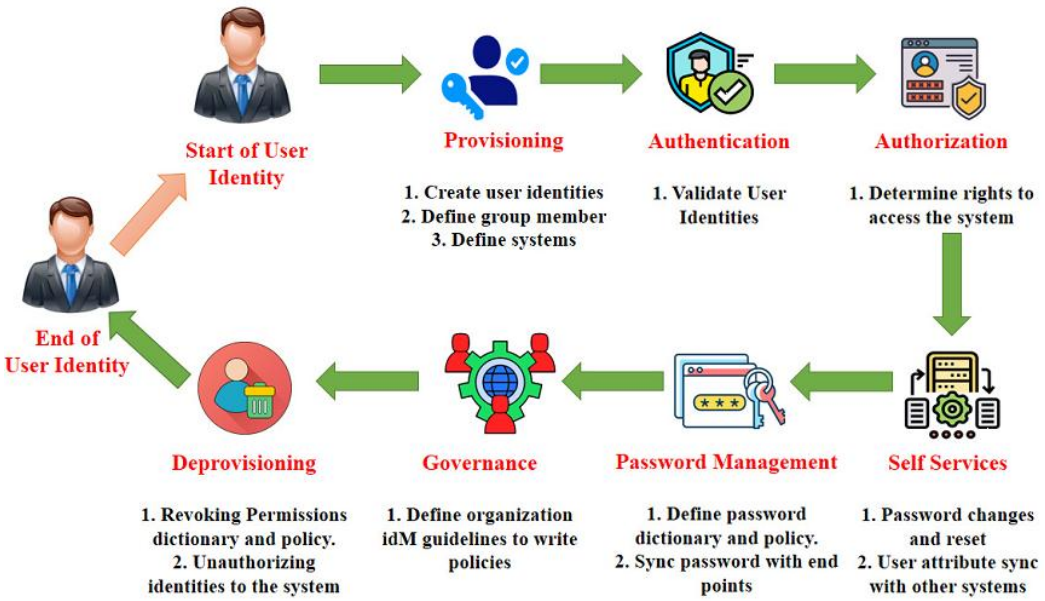

Figure 1 Life Cycle of Identity Management System

After authentication, authorization is another critical process in the idM system, which ensures what resources an authenticated entity can access and for how long it can access. For that purpose, different methods of authorization are employed, and most widely used are access control mechanisms. Different methods of access control such as role-based access control (RBAC), Attribute-based access control (ABAC) a policy-based access control (PBAC) are used based on the requirements of the access requirements of the organization, level of security, and contextual factors such as user roles, attributes, and others. The methods make certain that entitles only access those resources that are essential for their task, thus removing the danger of overprivileged accounts, and insider threats, and boosting the security of the organization. Furthermore, modern idM systems also incorporate token-based authorization methods which focus on time limited and specific scope access tokens to ensure secure access to the resources. Moreover, zero trust authorization methods are also adopted which continuously validate users and devices before authorizing access to the resource to enhance security [38-40].

Auditing and Monitoring in identity management is also a critical component, which focuses on monitoring access activities and maintaining a thorough log of those activities. This method ensures anomaly detection and unauthorized activities along with breaches and improves compliance with regulatory frameworks such as GDPR. Organizations make use of this to analyze access patterns and identify vulnerabilities in their access policies to improve their policy to ensure robust security. Furthermore, these logs work as a critical source for forensic investigation in case of breaches, allowing other organizations to trace and handle the root cause of cyber incidents more efficiently [41-42].

2.1.2. Working of Identity Management System

An identity management system involves the integration of components such as users, service providers, and identity providers, which make use of cryptographic methods and secure communication on protocols and centralized identity validation to ensure safe and scalable operations [43]. Figure 2 shows a typical identity management system working which is as follows:

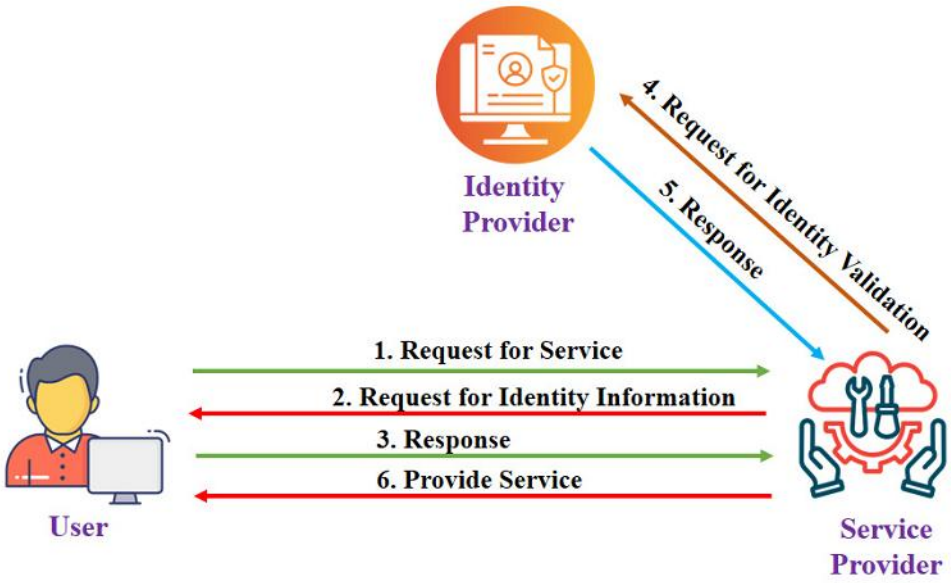

Figure 2 Working of an Identity Management System

1. Firstly, the user requests services from a service provider (SP) to access the resource it manages. This could involve accessing the resource from cloud storage or initiating the transaction in an enterprise application
2. In response, the SP first needs to verify the identity and for that purpose, it asks for identity credentials from the user which can be a username, passwords or token. The purpose is to ensure that only valid users can go forward.
3. In response, the user presents the requested credentials. The SP then provides these credentials to a third party requests the Identity provider for credentials validation. This method ensures stable security policies among different services scalabilities.

4. The identity provider makes use of advanced cryptographic methods and existing data of registered identities to ensure the authenticity of the user.
5. Upon validating the credentials, it transmits the information back to the service provider regarding the validity of the credentials.
6. If the credentials are valid, the SP gives the user access to the intended services or resources. However, if the credentials are invalid, then the access is denied.

Overall, all of this process ensures the mechanism for identity management is robust while thwarting unauthorized access.

2.1.3. Identity Management System Architectures

There are different architectures through which identity management systems are implemented and each one of them is designed according to the specific needs of the organizations, their security needs, and operational environments. These architectures include centralized, federated, and distributed.

The centralized architecture known as Identity provider makes use of a centralized authority system which handles all the identity data and authentication processes. This architecture is widely employed in enterprises, where a single entity manages and handles access to resources inside an organization [44]. This type of architecture results in efficient administration and reduces redundancy and simplifies identity management. However, despite its advantages, it suffers from major drawbacks of single point failure, which makes the whole system vulnerable [45].

Federated identity management allows users to link their identity to various separate identity systems. The user is authenticated once and then access to resources is allowed across multiple systems using a trusted relationship between the SP and the identity provider [46]. This attribute is achieved with protocols like Security Assertion Markup Language and OpenID Connect, which facilitate the assertions of secure identity between different parties [47]. This type of architecture enables single sign-on (SS) abilities among distributed environments and reduces the requirement for duplicate identity databases but needs strong trust methods and agreement on security standards between entities in the network. However, the reliance on communication protocol results in vulnerabilities in the system, because of any weakness in the communication protocol [48].

The decentralized identity management architecture makes use of technologies such as blockchain and decentralized identifiers (DIDs) to allocate identity data among different nodes while removing the dependence on a centralized party. This architecture allows the user to directly manage their digital identity while improving privacy and reducing the risks associated with centralized system breaches. These types of systems are vastly used in domains such as IoT and personal management due to the need for tamper-proof records and user centric controls. However, despite their unique features, this decentralized idM system faces challenges in the form of scalability and interoperability [49-50].

2.2. Blockchain

The idea of blockchain was first introduced by Satoshi Nakamoto [51], who designed a ledger technology that is distributed in nature, and which ensures secure, tamper resistance, and transparent data management in a decentralized approach. The blockchain, unlike the rest of the traditional centralized mechanisms, works through the use of peer-to-peer networks, in which each node can keep a copy of the ledger [52]. This method bypasses the requirement for third parties, thus resulting in less operational cost and improving the trust between the network participants. The core functionalities of blockchain involve decentralization, the ability to provide strong cryptographic security, and immutability which makes it a suitable option for applications like identity management and more [53].

At the core of the blockchain is its decentralized architecture which makes certain that a single entity doesn't control the system, thus improving the fault tolerance and robustness to cyberattacks. In the decentralized structure, the distribution of data is made among different nodes, and each of them keeps a similar copy of the ledger [54]. When any modification to the ledger data is needed, a consensus from most nodes is essential in that required. This distributed nature also provides robustness and data availability in case of partial system failure [55]. An essential element of the blockchain is the Merkle tree which allows the verification of larger datasets. This tree organizes the transaction information in the form of a hierarchical structure, where each leaf node indicates a transaction structure, and each non leaf node indicates the hash of its child nodes. The root or base of the tree is known as the Merkle root, which provides one specific cryptographic representation of all transactions in the block. The Merkle structure helps the nodes verify the addition of a transaction in the blockchain without the need to download the entire dataset, which improves efficiency and scalability. Furthermore, this structure of Merkle as shown in Figure 3 also provides feature of immutability because to its capability to ensure that any changes to a single transaction would need recalculating the whole tree structure, which is computationally not feasible due to the need of huge computational resources [56-57].

Smart contracts are a critical element of blockchain which is self-executable code. They are stored on the blockchain to impose agreements when already defined requirements are satisfied. The employment of smart contracts means that there is no need for a third party to enforce the agreements, thus enhancing efficiency while improving the operational overhead. These smarts are immutable which ensures that once the conditions are agreed upon and deployed, they cannot be changed. Furthermore, their code is often transparent and visible in the blockchain. In identity management systems and dynamic permission management systems, smart contracts are often deployed to ensure a strong method for process automation while keeping the same level of trust and security [58-59].

The backbone of the blockchain network is the consensus algorithm whose purpose is to ensure agreement between the nodes on the authenticity of the transaction and the ledger state. Without depending on any third party, these algorithms ensure the consistency and integrity of the blockchain network [60]. The earliest use of consensus in blockchain is Proof of Work (PoW), which works through computing complex mathematical puzzles to validate the transactions and generate new blocks. It provides effective security; however, it results in huge energy and computational requirements [61]. On the other Proof of Stake (PoS) provides an alternative solution that is more energy efficient. In this method, the validators are selected based on their stake in the networks which reduces the need for huge computations [62]. An advanced form of PoS is Delegated Proof of State (DPoS) in which participants are required to select the delegates to validate the transactions, which maintains the decentralization while enhancing the scalability [63]. Furthermore, in permissioned blockchain, Practical Byzantine Fault Tolerance is used which ensures an iterative method of voting to gain consensus which makes it effective for private networks [64]. All of the consensus methods have their own benefits, and their applicability are usually dependent on the requirements of the blockchain methods. Table 1 shows the comparison of identity management system architectures.

Table 1 Comparison of Identity Management System Architectures

Aspect	Centralized	Federated	Decentralized
Control Authority	Managed by a single entity	Distributed among trusted entities	No single authority; distributed across nodes
Scalability	Restricted to the ability of the central system	Moderately scalable across organizations	Highly scalable, depending on the network
Security Risks	Single point of failure; higher risk of centralized breaches	Shared responsibility: trust relationships mitigate risks	Tamper-resistant; eliminates single points of failure
User Privacy	Limited; the central authority controls user data	Moderate; relies on trusted third-party providers	High; users retain full control over identity data
Implementation Complexity	Relatively simple; relies on a single repository	Moderate; requires protocol agreements (such as SAML, OpenID)	High; requires advanced technologies (such as blockchain)
Interoperability	Low; tightly controlled within one organization	High; enables cross-domain access	Moderate; standards like DIDs improve compatibility
Use Case	Active Directory, LDAP	Google SSO, SAML-based systems	Blockchain-based identity solutions, Self-sovereign Identity (such as SSI)

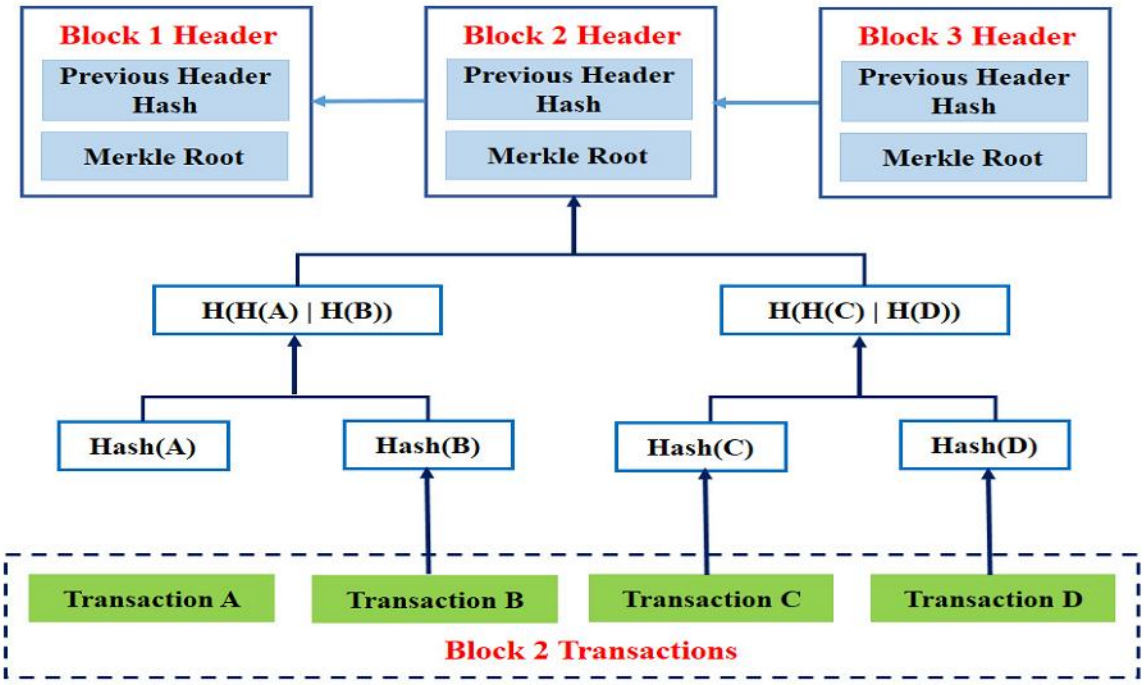

Figure 3 Blockchain Merkle Tree Architecture [65]

3. EXISTING METHODS OF BLOCKCHAIN BASED IDENTITY MANAGEMENT

In this section, we perform a detailed literature review of existing work done by researchers over the years on blockchain based idM systems.

3.1. Blockchain Based Authentication Methods for Identity Management

Authentication is a critical component of identity management and its integration with blockchain provides more robust, scalable and tamper proof authentication mechanisms. Researchers over the years have deployed various blockchain based authentication solutions to enhance identity management in the IoT systems. The authors of [66] introduced an identity management system that uses blockchain based authentication to provide user and device authentication. Their approach uses the tamper-proof ledger of blockchain along with the consensus method for identity verification. In their approach, the IoT devices create identities using the attributes that are saved in the Merkle tree of the blockchain. The smart contracts then validate the identities and further detect any anomalies in the authentication phase to safeguard against attacks such as replay attacks and phishing attacks. [67] also worked on a blockchain based authentication scheme for the Internet of Vehicles (IoV). Their work aimed at limiting the involvement of cloud servers by shifting the re-authentication to the edge nodes. This results in decreased communication overhead and latency. Furthermore, the approach makes use of mutual authentication between vehicles and edge node and cloud along with a session key management to safeguard the critical data. In [68], the researchers worked on handling the vulnerabilities in smart cities by proposing a multifactor blockchain based authentication method that relies on smart contracts and zero knowledge to provide security along with privacy preserving authentication. The approach also ensures the protection of passwords and further obscures them from intruders. Furthermore, it ensures security against Denial of service (DoS), MiTM and phishing attacks.

The blockchain based authentication methods have been a major avenue of work for ensuring identity management in cloud computing. The author of [69] worked on overcoming the challenges in the cloud such as insider and outsider threats and proposed a blockchain based authentication method that makes use of a tamper-proof distributed ledger to trace insider activities while stopping unauthorized access. The method provides authentication by making use of signatures and unique IDs. The security of the method is also formally validated through Scyther and the result indicates that it overcomes impersonation, replay, and DoS attacks. In [70], they worked on providing authentication and authorization for mobile cloud environments while employing blockchain. They aim to handle the issues associated with traditional centralized systems. Their method ensures authentication and dynamic access privileges through smart contracts thus improving the scalability. Moreover, the use of zero knowledge ensures single registration without the requirement for a third entity, thus improving the fault tolerance. The method in [71] introduced a

blockchain authentication method that ensures privacy preservation in mobile cloud environments. Their method works in such a way that mobile users perform single registration on a public blockchain, which allows them seamless access to multiple cloud service providers. Their method provides cost effective authentication through the incorporation of ECC.

In [72], authors worked on an authentication mechanism that is decentralized and makes use of Neo blockchain for effective security in IoT and fog computing. Their method makes use of smart contracts for authentication and data integrity. The users are required to register their credentials which are stored on the blockchain, thus providing robust authentication without single-point failure. The approach is also cost effective and adaptable for resource limited environments like fog computing while providing better scalability with security. [73] introduced an authentication method through the use of an Ethereum smart contract to enhance the security and scalability of fog computing. Their methods incorporate biometric data along with email and password for robust registration and user verification. The approach also showcases better scalability and security while improving the transaction and execution cost. [74] proposed a method that incorporated permissioned blockchain for effective authentication and management in a fog computing environment. They used smart contracts to register and validate the devices. Furthermore, the elliptic curve is utilized for key generation and trust-based identity management which improves the computational overhead on the edge devices. The method is implemented on a private Ethereum 2.0 network which shows better registration and authentication time while safeguarding against cyberattacks. The authors of [75] proposed an authentication method for fog computing that makes employs smart contracts to provide authentication and enforce access policies. The method offers effective decentralized authentication and removes the requirement for third parties. Furthermore, it provides resistance against replay, eavesdropping, and attacks. Moreover, it provides attributes of transparency through the use of encryption on user attributes for the secure enforcement of the policy.

Table 2 Comparison of Blockchain Based Authentication Methods

Work	Domain	Strengths	Limitations	Performance Metrics	Blockchain Type	Blockchain Network	Development Type
[66]	IoT	Robust authentication	malicious nodes authenticating each other without validator node verification	Latency, throughput	Public	-	Simulation
[67]	Internet of Vehicle	Reduced communication overhead	Susceptible to collusion attack	Communication overhead, latency	Consortium	-	Simulation
[68]	IoT based Smart Cities	Privacy-preserving authentication,	Requires complex cryptographic operations.	Response time, authentication time	Public	Ethereum	Proof of Concept
[69]	Cloud	Mitigates insider threats	Limited fault tolerance	-	Permissioned	Hyperledger Fabric	Simulation
[70]	Mobile Cloud	Scalable authentication, fault tolerance	Storage overhead due to increase of devices	Computational cost, storage overhead	Consortium	***Hyperledger Fabric***	Simulation
[71]	Mobile Cloud	Privacy preservation, reduced	High Computational cost	Registration time, execution cost.	Public	-	Scheme
[72]	IoT & Fog	Robust authentication without single-point failure	Limited real-world deployment validation	Registration gas, authentication gas	Public	Neo	Simulation

[73]	Fog	Improved transaction cost	Doesn't measure authentication time, which is necessary where speed is essential	Transaction cost, execution time.	Public	Ethereum	Simulation
[74]	Fog	Enhanced Authentication with better registration time	In real world cases, network delays or packet losses could impact performance	Response time, throughput	Permissioned	Ethereum	Simulation.
[75]	Enterprises	Protection against key replay and impersonation attacks	May not scale well in complex supply chain scenarios	Computational cost, communication cost, storage cost	Permissioned	Ethereum	Scheme, Security tested through Scyther
[77]	Enterprises	Authentication ability to perform on the fly authentication	High initial setup, hard to implement in resource conservative environment	-	Private	-	Scheme
[78]	Enterprises	Ensures scalability, integrity,	Higher response times will impact real-time deployment	latency, throughput	Permissioned	Hyper-ledger Fabric	Simulation

Table 2 shows the comparison of blockchain based authentication methods Enterprises are another domain in which blockchain based authentication is used for identity management. In work [76], researchers proposed a mechanism that provides mutual authentication by radio frequency identification protocol integrated with blockchain in supply chain enterprises. The method further provides different access levels to supply chain nodes. Furthermore, their work offers protection against key replay attacks, MiTM, and impersonation attacks. [77] introduced the employment of decentralized authentication to design a point-to-point authentication for identity management in enterprise systems while making use of blockchain technology. The approach creates unique authentication credentials dynamically for each communication. Furthermore, the employment of quantum resistant cryptography and provisioning based on proximity improves the resistance against cyber threats. Furthermore, the method removes the requirement for contact connectivity between IoT devices and ensures on the fly authentication while improving the computational needs, which makes it one of the viable options for enterprises. Work by [78] suggested a distributed authentication scheme for smart manufacturing. It employed distributed blockchain and hyper ledger fabric to provide safe communication among the devices of various domains through utilizing smart contracts for security. The approach ensures mutual authentication and integrity along with scalability.

3.2. Blockchain Based Authorization Methods for Identity Management

Blockchain based authorization methods provide effective means of identity management by utilizing the immutability and transparency of blockchain to provide more advanced access control methods to overcome unauthorized access. The work by [79] proposed a method that utilizes blockchain to design an access control to handle the security concerns in IoT. They make use of attribute-based access control in which policies are defined by attributes like user roles and time. Furthermore, the use of smart contracts and the ethereum blockchain provides encrypted data storage. The method removes the requirement for the devices to have an access control list and thus avoids data tampering. To ensure secure data retrieval, attribute-based encryption is used which makes certain that only authorized users can decrypt the data over a certain time. The author in [80] introduced an ABAC through

the employment of blockchain technology for IoT. The method provides trust management and reduces the computational overhead associated with decentralized access management. The blockchain records are used to authorize the transaction to ensure data integrity and avoid tampering. In their approach, IoT devices do not take part in the consensus thus reducing the computational and communication costs. [81] proposed a method that relies on role-based access control integration with private Ethereum blockchain to handle access to IoT application data. The method ensures data sharing between the stakeholders and also makes certain that access is restricted based on the roles and responsibilities of the entities. The use of blockchain eliminates the requirement of central authority and its immutable ledger first secures the data transactions. [82] worked on a capability-based access control for the IoT. The method is decentralized and through the incorporation of blockchain and smart contracts it also handles access to the devices and the services. The access control makes use of a capability token to define and verify the access rights. Furthermore, the method provides revocation ability which improves the scalability and the security.

In [83], the researchers worked on a blockchain based ABAC to provide secure access management in the cloud. The methods use smart contracts for fine grained access control and provide the ability to the data owner to define the access period and the traceability of the interactions through the use of blockchain records. The method is viable for cloud domain deployment due to its efficiency and low operational cost. [84] introduced an access control that integrates blockchain to ensure secure access control in a cloud environment. They make use of attribute-based access control to improve flexibility and privacy for handling the access of critical information. Furthermore, the incorporation of a decentralized ledger provide suitable logging of access requests and access policy updates. Moreover, the use of smart contracts provides a dynamic access policy without the need for your key to update the policy. The critical data is encrypted through leveraging ciphertext policy attribute-based encryption. Overall, their work provides efficient identity management through the incorporation of robust access management. [85] worked on an access control that is decentralized and employs smart contracts for tasks like authorization. The approach makes use of policy-based access control and uses the access control list to describe and access rights which are carried out through blockchain smart contracts. The method provides confidentiality and integrity along with resistance against various cyberattacks. In [86], the authors produced a method that uses policy-based access control to improve identity management through authorization in a cloud environment. They integrate blockchain for storing the access permission through tamperproof method, thus providing confidentiality and integrity. Moreover, the method provides security against unauthorized access from internal and external threats. The authors of [87] produced a method that provides context aware access control by making use of blockchain for effective access management in cloud storage. They incorporate dynamic contextual attributes such as the time and location in the access policies and incorporate accountable token generation. The method is employed through Ethereum, and the results indicate encouraging results in terms of performance and cost effectiveness. Table 3 shows the comparison of blockchain based authorization methods.

Table 3 Comparison of Blockchain based Authorization Methods

Work	Domain	Strengths	Limitations	Access Control Type	Performance Metrics	Type of Blockchain	Blockchain Network	Developmet Type
[79]	IoT	Enhanced security and transparency	Complexity in real world deployment due of management two block chains	ABAC	Execution cost, transaction cost	Hybrid	Ethereum	Simulation
[81]	IoT	Ensures secure, tamper-proof authorization and data transmission	As the number of devices increase, will encounter scalability concerns	RBAC	-	Private	Ethereum	Simulation
[82]	IoT	Fine grained access control with reduced bottleneck	Higher Computational	CBAC	Computational Overhead, Network Latency	Private	Ethereum	Simulation

[84]	Cloud	Dynamic access control for encrypted data without requiring changes to user keys	Complexity of the encryption and decryption processes may affect transaction speed	ABAC	-	Private	Ethereum	Scheme
[85]	Cloud	Provides immutable logging of access control actions and auditing	May deal with scalability concerns due to blockchain-related overheads	PBAC	-	Permissioned	Ethereum	Scheme
[87]	Cloud	Fine grained access with location-aware contextual information	High computational cost due to encryption and decryption layers	CAAC	Transaction cost, latency	Private	Ethereum	Scheme
[88]	Fog	Fine grained access with fault tolerance	High computational overhead	CAAC	Latency, energy consumption	Private	-	Simulation
[89]	Fog	Efficient privacy preserving access	Can introduce bottlenecks in large scale deployments	ABAC	Execution time	Private	Ethereum	scheme
[90]	Fog	High scalability and low latency	Overhead by storing and managing key pairs	PBAC	Communication cost, latency	Permissioned	Ethereum 2.0	Simulation
[92]	Enterprise	Supports time based transactions	Higher latency in transaction processing	PBAC	-	Permissioned	-	Scheme
[93]	Enterprise	Enforced policies by smart contracts	Cannot hide the identity of the requester	PBAC	-	Hybrid	Hyperledger Fabric	Scheme
[94]	Enterprise	Flexible access with fault tolerance	Complexity in real world deployment	PBAC	-	Permissioned	Hyperledger Fabric	Simulation

In [88], the authors produced a mechanism which employs blockchain integrated context awareness access control for fog computing environments. The method provides heterogeneity along with robust access management. Furthermore, it offers resource customization and effective data processing capability while utilizing context aware strategies. [89] also proposed blockchain-based access control in fog computing. The method makes use of ABAC to ensure fine grained access management. Furthermore, the employment of blockchain ensures transparency and reliability along with the mitigation of single point failure. To handle the limited processing abilities of IoT devices, most computational tasks are performed by fog nodes. This method ensures effective performance while maintaining robust access management. [90] worked on blockchain assisted ABAC for the

fog computing environment. The method utilizes the blockchain for the storage of metadata for transaction verification and access control. Furthermore, the system incorporates re-encryption and cryptographic mechanisms to provide security in data sharing and access. In [91], researchers also worked on access content for identity management through the integration of blockchain based fog computing. The method utilizes policy-based access control and enforces the policies without requiring a third party. Furthermore, it makes use of elliptic curve cryptography to perform key generation with cost effectiveness. The formal validation through ProVerif showcases the method robustness. Furthermore, the method ensures scalability and low latency which makes it more suitable for deployment in fog computing.

The authors of [92] worked on policy-based access control through incorporation of blockchain to limit unauthorized access in enterprise networks. The method also counters the unauthorized signature generation, providing scalability with the support of a dynamic validator. The method effectively negates single point failures and provides robust identity management along with improved security. In [93], they proposed an access control system based on policy-based access in enterprise applications. The method also integrates blockchain and makes use of hyper ledger fabric to provide effective privacy preservation, access revocation, and data updates along with additional attributes of scalability and transparency. [94] put forward an access control method which is decentralized and makes use of policy-based access control to improve identity management in enterprise applications. The method also makes use of cryptographic methods of secret sharing and ring sharing to prove robust and private data access. The method ensures customizable access rules while providing the ability to detect malicious nodes and safeguard user privacy. The implementation method is performed using Hyperledger Fabric and it provides additional attributes of scalability.

4. BLOCKCHAIN BASED IDM USECASES

In this section, we explore different use cases of blockchain which provide identity management and are feasible for deployment in IoT, cloud, fog computing, and enterprise environments.

4.1. IoTeX

IoTex is an existing use case of a blockchain based system that provides identity management. Its method relies on a decentralized identity based (DID) framework which makes certain that the user and the device can handle their own identities autonomously without the need for a centralized third entity. They rely on the principles of self-sovereign identity (SSI) in which the devices and the individuals can keep control of their credentials and data. Furthermore, it integrates blockchain with trust execution environments (TEE) and lightweight cryptographic protocols to ensure strong identity management [95]. Its architecture uses the root blockchain for global governance and various chains for specific applications and devices. This design ensures scalability and separates the identity operations to improve the bottleneck and improve transaction throughput. Furthermore, the integration of its architecture provides the ability to perform secret operations of the device by generating an environment that is isolated and is specifically for sensitive operations such as identity verification. Furthermore, through incorporation of smart contracts, IoTeX ensures access control which limits the device functions or data handling based on predefined parameters [96].

IoTeX is well suited for deployment in IoT, and its architecture has been optimized for IoT. Its architecture handles the challenges faced by IoT systems in the shape of scalability and latency. The incorporation of hierarchical blockchain in blockchain architecture ensures improved latency. Furthermore, the use of Roll Delegated Proof of Stake (DPoS) which is an enhanced form of PoS is used to provide fast transaction processing. Furthermore, IoTeX utilizes lightweight protocols that ensure robust idM without burdening the system, which overall improves the scalability. Moreover, IoTeX ensures data confidentiality which is a necessary need in critical IoT application like healthcare [97].

4.2. IOTA

IOTA is a method that relies on a distributed ledger and provides an effective idM system. Instead of employing traditional blockchain for idM, it uses Directed Acyclic Graph (DAG), a next generation distributed ledger. The IOTA architecture works in such a way that each node should be able to agree to two previous transactions before submitting its transactions. Furthermore, it makes use of SSI, which is a method in which participants and devices control identities without the requirement for a centralized party. This feature is applicable due to the employment of DIDs which are generated independently and are handled by the Tangle [98-99].

In IoT, where a large amount of devices are required to be authenticated and handled at the same time, the employment of Tangle in IOTA ensures lightweight transactions in an environment with a huge number of of devices, which is why it is most feasible for IoT. Furthermore, it focuses on improving the trust and security between the devices, while making certain that identities are verifiable while maintaining high scalability and low latency [100-101].

4.3. Neblio

To provide idM in the enterprise, the Neblio platform integrates blockchain simply through the employment of RESTful APIs, which are supported by various programming such as Python, Node.js, .NET, and JAVA. These API reduces the complexities associated with blockchain integration in enterprises and provide the ability to deploy the application that easily integrate blockchain functionalities without great knowledge related to distributed ledger working. Moreover, its architecture integrates identity management and ensures a secure and decentralized method to handle and authenticate the identities. The incorporation of an immutable ledger also keeps the cryptographic identifiers sorted, which makes certain that identity data is not changed or modified. Furthermore, it employs smart contracts in enterprises for automating the identity verification process and granting and removing access based on already defined conditions [102-103].

The critical aspect of Neblio is its consensus mechanism, which is POS, which provides a more secure and decentralized network while preserving the energy cost that is critical in enterprise applications. Furthermore, it also lessens the computational overhead which often results from POW, which makes it more suitable for large scalable business deployments for identity management. The feature that enables its use in enterprises is its scalability because its globally distributed node provides efficient real time data access and processing without latency issues in high scale transaction environments [104]. Furthermore, its ability to provide immutable data storage and a secure communication channel makes this method more suitable for enterprise applications like supply chains. Furthermore, while providing idM in enterprise applications, it makes certain that the user record of authentication and access are tamper resistant and auditable which is necessary for compliance with the regulations like GDPR. Moreover, it is flexible and provides the ability to integrate identity management into already existing business infrastructures, which makes it easy for a business to make use of blockchain solutions without burdening its IT infrastructure [105].

4.4. Kaleido

Kaleido is a platform that is based on blockchain as a service and provides idM. It makes use of identity attributes in the blockchain network and provides the capacity for individuals to generate their own identity. It provides the luxury to enterprises to effectively handle and manage identity while minimizing the administrative operations burden. Apart from using decentralized identities for identity management, Kaleido also provides specific identity wallets which provide the user with the ability to store share, and manage verifiable credentials (VCs) safely. These wallets incorporate cryptographic proof for identity verification, which improves trust in an enterprise system. Furthermore, it makes use of private and permissioned blockchain, which keeps the identity records, while ensuring that the identity data remains and is accessible to an authorized entity [106-107]

For cloud environments, Kaleido is the most preferable option because of its ability to integrate with the cloud while providing features of scalability, privacy, security, and efficient idM. It incorporates Ethereum based consortium blockchain which optimizes identity management in cloud applications. Furthermore, a critical need in the cloud is scalability, and Kaleido has this attribute to serving large number of identities and transactions, which makes it suitable for the environments that are constantly growing [108].

4.5. Sovrin

Sovrin is a platform that utilizes a permission blockchain called Hyperledger Indy to ensure identity management. Hyperledger Indy is purposely designed for a centralized identity solution, and Sovrin made use of that to provide the ability to entities and users to take control of their identities. Furthermore, Sovrin ensures the generation of SSI through the incorporation of DIDs, and the information related to identity is distributed across the blockchain network. Furthermore, it provides re-authentication and integrity of identity claims and stores the VCs and cryptographic proof of identities. It makes certain that users only share selected information for authentication, which removes the threat of identity theft [109-110].

It is among the favorable options for enterprise, its decentralized nature makes it easy to initiate trust between the entities in the network, and the employment of VCs and privacy by design features allow it to maintain data privacy while verifying the identity. Furthermore, its ability to provide permissioned access control allows the ability to enterprises to implement strong access policies to make certain that only authorized entity can gain access to the resources [111]. Unlike the rest of the solution, it solely focuses on enterprise centric features, which makes it a suitable option for enterprises that need robust identity management solutions.

4.6. SelfKey

SelfKey is a platform that provides idM by incorporating Ethereum blockchain and allows the user to be the possessor of their digital identity. It incorporates SSI, which is stored on the blockchain. Overall, this blockchain based system works as a distributed ledger that stores information related to identity. Currently, Ethereum 2.0 makes use of PoS consensus mechanisms, which improve the energy overhead and provide sustainability. This results in a system that is more reliable and more robust to cyber threats and

data thefts. Furthermore, the employment of cryptographic methods such as private allows the ether to authenticate through various platforms without the need to again authenticate [112-113].

In fog computing environments the data is always processed at the network edge and involves resource constraint devices, the SelfKey identify management is highly suitable in that regard due to its energy-efficient nature because of PoS. Furthermore, in fog computing, SelfKey ensures peer-to-peer identity verification between the edge device and makes certain that only the devices and users with the proper access can communicate and access the resources. This improves the security and privacy in fog computing.

4.7. Civic

This platform uses the Ethereum blockchain to secure identity verification in a decentralized way. It incorporates the SSI model to provide users the control over their data. Furthermore, it employs smart contracts to automate the process of idM such as access management and verification of the credentials. The use of features such as know you customer verification further improves its identity management. The employment of biometric authentication is another feature that further improves security by binding the digital identity to immutable and unique physical characteristics such as fingerprints, etc to make certain that only the legitimate user can access the data. Furthermore, Civic also provides its users the ability to reveal data to trustworthy entities such as financial institutions or service providers which keeps the other critical details private [114-115].

In enterprises, civic is the most feasible solution to provide identity management, especially in sectors such as finance, and healthcare. The ability of Civic to streamline identity verification and compliance with KYC and data protection laws make it unique from others. In financial institutions, Civic helps increase customer onboarding and improve transaction security while lessening identity fraud by making certain that only authorized individuals can access critical information. Table 4 shows the overview of blockchain based idM solutions.

Table 4 Overview of Blockchain based idM Solutions

Feature	IoTeX	IOTA	Neblio	Kaleido	Sovrin	SelfKey	Civic	VerseOne
/ Feasibility for Domain	IoT	IoT	Enterprises	Cloud	Enterprises	Fog Computing	Enterprises	IoT
Blockchain Type	IoTeX Blockchain	Tangle	Neblio Blockchain	Ethereum-based consortium	Hyperledger Indy	Ethereum (ERC-20)	Ethereum (ERC-20)	Ethereum
Smart Contract Usage	Conditional IoT access	Lightweight automation	Enterprise app automation	Advanced access controls	Identity claim verification	ID wallets and permissions	KYC and identity verifications	Device-centric access policies
Consensus Algorithm Used	Delegated Proof of Stake (DPoS)	Coordinator-less Tangle (DAG)	Proof of Stake (PoS)	Proof of Authority (PoA) & PoS (Ethereum-based)	Practical Byzantine Fault Tolerance (PBFT)	Proof of Stake (Ethereum)	Proof of Stake (Ethereum)	Leaderless Consensu
Identity Model	DID	DID	DID	DID	User-centric, privacy-first	DID , KYC	DID , KYC	DID , KYC
Privacy Features	Encryption, pseudonymity	No miners, quantum-resistant	Data encryption	GDPR-compliant, private network	Encryption, minimal data use	Pseudonymity, encryption	Encryption, reuse of credentials	Encrypted, GDPR-compliant

Integration Support	IoT devices, services	IoT devices, services	Legacy systems, dApps	Cloud services (AWS, Azure)	Limited	Multiple apps via API	Payment platforms	Limited
Authentication Type	PKI, DID-based auth	PKI, DID-based auth	PKI-based	PKI-based and OAuth-like models	User credentials, OAuth	PKI, biometrics	PKI, biometrics	PKI, biometrics
Notable Features	Integration with IoT devices	Quantum-proof; feeless transactions	Focus on app development; open APIs	Built-in compliance and dev tools	Privacy-first email; simple tools	Self-sovereign ID; ID wallet	Reusable ID; ID verification	KYC-focused ID; GDPR-aligned
Customization Ability	IoT-focused, flexible	Moderate, Focused on IoT devices	App development focused	Highly Tailored to cloud enterprises	Privacy-centric with limited customization	ID wallet customization	Reusable ID with customizable features	KYC and ID verification focus
Adoption Stage	Emerging in IoT	Mature in IoT	Mature in enterprise apps	Emerging for cloud	Emerging in Enterprise	Emerging in idM	Widely recognized for idM	Early stage
Open Source	Yes	Yes	Yes	Partially	Partially	Yes	Yes	Yes

4.8. VerseOne

This is a platform specially created for identity and credential management based on a blockchain that is purpose-built. It is a custom-made decentralized ledger that is optimized for identity management. What makes it different from the rest is that it doesn't keep sensitive information directly on the chain, but it stores specific points to off-chain data which keeps a balance between user privacy and transparency. Furthermore, the incorporation of privacy preserving verification makes this method more sophisticated by allowing individuals to prove their identity without exposing sensitive information. VerseOne offers interoperability among various platforms by providing effective compliance with the widely used standards which makes it a viable option for decentralized identity systems [116].

The working principles and design of VerseOne make it applicable to domains that require decentralized identity solutions such as IoT. The decentralized feature and privacy preserving nature make it highly effective in IoT, where different distributed devices communicate and authenticate each other without depending on the centralized server. Its ability to provide trust without centralized authority while providing privacy along with security among distributed environments for identity management make it more suitable for large scale environments such as IoT.

5. EVALUATION

In this section, we perform evaluation of blockchian based identity management real world solutions on the basis of important criteria such as performance, security, compliance, cost, scalability, and interoperability, ease of integration, user experience and decentralization.

5.1. Computational Overhead

The number of additional resources taken by the system to perform operations is referred to as computational overhead and these overall impacts the scalability and efficiency of a system. Neblio results in mediocre performance overhead due to its structure of blockchain. Despite that, it is still effective for small size enterprises. IoTeX and IOTA both ensure minimum performance overhead due to their efficient consensus algorithm, which makes them suitable for IoT environment. Kaleido which uses Ethereum blockchain does induce heavy performance overhead particularly in cases of network congestion. SelfKey , Civic, Sovrin and VerseOne also offer minimum performance overhead, however they fail to handle large scale operations like IoTeX and IOTA.

5.2. Security

Each of the existing platforms has its specific way of providing security. For instance, IoTeX emphasizes its end-to-end encryption, while IOTA uses a tangle network which removes the need for miners. On the other hand, Selfkey and Civic focus on advanced encryption with zero-knowledge proofs along with an additional focus on user-centric privacy for effective identity management. Neblio makes use of secure APIs, which makes it a feasible solution for enterprises. Kaleido makes use of PKI and signature mechanisms for secure transaction and entity verification. Sovrin employs zero-knowledge proofs and VCs for secure identity verification. VerseOne incorporates zero-knowledge proofs and elliptic curve cryptography for privacy and identity management cost-effectively. Sovrin stands out from the rest in terms of security due to its cryptographic and governance-driven security which effectively ensures privacy, and security.

5.3. Compliance

The blockchain-based identity management platforms need to comply with data privacy regulations to ensure the safe and ethical handling of personal data. IoTeX complies well with the GDPR and other privacy-related regulations and provides tools that ensure compliance with regulatory standards. IOTA, also designed for IoT just like IoTeX, faces difficulties in adhering to compliance. Its architecture doesn't support compliance mechanisms, which makes it difficult to meet regulatory standards. Neblio also offers compliance with GDPR, which makes it a suitable option for businesses. Self-key and Civic both focus on personal privacy and meet the GDPR but face difficulty in providing support related to larger-scale compliance. Sovrin and VerseOne comply with with GDPR while offering a privacy-centric solution but fail to meet the compliance capabilities needed for large-scale environments. Among these, Kaleido offers strong compliance with GDPR, HIPAA, and other regulatory frameworks. This makes it highly effective for cloud environments that require strict regulations and compliance to ensure trust among users.

5.4. Cost Effectiveness

The suitability of these platforms relies heavily on cost-effectiveness, which is critical for smaller-scale organizations. IOTA and IoTeX are both extremely cost-efficient, which is critical in IoT considering the scale of the network. Neblio does provide enterprise-level features with minimum cost; however, for large-scale applications, its cost to increase with the utilization of more resources. On the other hand, Kaleido offers affordable costs, but its dependence on Ethereum leads to high cost, and in the cloud, it further yields more operational cost associated with cloud scalability and maintenance. Civic, self-key does provide affordable solutions, but Selfkey does incur more cost due to the deployment of fog nodes. Sovrin and VerseOne provide affordable cost solutions, but for large environments they are not feasible. Overall, in terms of operational cost, IoTeX and IOTA excel from the rest of the solutions.

5.5. Decentralization

While providing the attribute of decentralization, The IOTA and IoTeX strongly excel in that aspect and remove the need for centralized authorities. SelfKey and Civic also ensure a decentralized method while relying on user-controlled identity. Neblio aimed at keeping a balance between decentralization and centralization but swayed towards centralized control. On the other hand, Sovrin and VerseOne provide minimal decentralization and prioritize simplicity over a fully decentralized system. Kaleido, though, supports decentralization; it can merge centralization and de-centralization and provide a hybrid method on the basis of user specifications.

5.6. User Experience

A friendly and smooth user experience is crucial to make certain that the platform is easy to use with privacy controls, usability, and accessibility. The IoTeX provides an interface that is flexible and suits the developers. Its ability is a customizable identity solution for IoT devices, however due to the requirement of technical knowledge, it may be complex for the general end user. Other the other hand, IOTA offers a user-friendly experience, however, it can be hard for traditional blockchain developers and is complex for general users.

Other the other hand, IOTA offers a user-friendly experience, however, it can be hard for traditional blockchain developers and is complex for general users. Neblio offers an interface that is developers specific and offers several multi-language APIs improving the experience of users with technical expertise. Again, for the normal user, this platform may not be feasible. Kaleido offers an interface that is highly user-friendly and provides inbuilt drag-and-drop tools and templates that ease integration of blockchain-based identity management user experience for ordinary users, which seeks to manage their identities securely and privately.

5.7. Interoperability

IOTA makes use of the tangle framework which offers compatibility with IoT devices but lacks integration with traditional blockchain methods. Neblio which was designed with a focus on the developers as key users provides APIs in different languages for different platform integrations. Sovrin and VerseOne provide limited interoperability which makes them not flexible for complex integration. Selfkey and Civic thought support decentralized identity standards but fall behind regarding platform adaptability. However, IoTeX and Kaleido provide perfect interoperability by giving tools and APIs for integrations with diverse platforms.

5.8. Scalability

Scalability is a critical attribute that blockchain based idM solutions must provide to handle the increasing number of users and transactions. IoTeX and IOTA provide high scalability in comparison with the rest of the solutions. Neblio provides a moderate level of scalability due to its focus on ease of integration rather than focusing on high throughput. Kaleido and VerseOne also achieve high scalability due to their Ethereum models which support dynamic workloads Furthermore, Civic, Sovrin, and SelfKey provide a moderate level of scalability which is because of privacy-preserving methods such as zero-knowledge proof and VCs which create computational overhead. Moreover, their dependence on semi-decentralized and permissioned models hinders their ability to manage large transactions.

5.9. Transaction Speed

In blockchain-based systems, the transaction speed is the rate at which it can validate and process the transactions and is usually measured as the time taken to complete the transaction. IoTeX provides high transaction speed with efficient processing of operation in IoT where speed is important for device transmission. IOTA also provides fast and seamless transactions. Similarly, Kaleido also ensures high transaction speed to manage the dynamic load in enterprises effectively. Sovrin offers medium transaction speed and balances security and functionality. On the encounters with occasional delays because of its focus on secure identity verification. SelfKey, Civic, And VerseOne also provide high transaction speed due to leveraging the PoS mechanism which enhances the identity verification operations throughput. Table 5 shows the overview of blockchain based idM solutions.

Table 5 Overview of Blockchain based idM Solutions

Criterion	IoTeX	IOTA	Neblio	Kaleido	Sovrin	SelfKey	Civic	VerseOne
Computational Overhead	High	High	Medium	Medium	Medium	Medium	Medium	Medium
Security	Strong	Strong	Medium	Strong	Strong	Strong	Strong	Strong
Compliance	High	Medium	High	Very High	Medium	Medium	Medium	High
Cost	Low	Low	Medium	High	Medium	Low	Medium	Low
Scalability	High	High	Medium	High	Medium	Medium	Medium	High
Decentralization	Strong	Strong	Medium	Medium	Medium	Medium	Medium	Strong
User Experience	Flexible	User-Friendly	Developer-Focused	User-Friendly	Business-Friendly	User-Centric	User-Centric	Business-Friendly
Interoperability	High	Medium	High	High	Medium	Limited	Limited	High
Transaction Speed	High	High	Medium	High	Medium	High	High	High
Energy	High	High	Medium	Medium	Medium	High	High	High
Communication Overhead	Low	Low	Medium	Medium	Medium	Low	Low	Medium

5.10. Latency

The responsiveness of a blockchain-based system is usually measured through its latency which is between the start and the completion of a transaction. The high latency impacts the overall efficiency, which makes the system not suitable for real-world operations. IOTA offers very low latency, making sure that the response is immediate, which is effective in an IoT environment. IoTeX also offers low latency which makes it also suitable for IoT. Kaleido, Civic, and SelfKey also provide low-latency which makes them suitable for applications where fast transactions and confirmations are necessary. On the other hand. Neblio,Sovrin and VerseOne provide medium latency along with some delay. These systems put more focus on security and reliability than speed and may be feasible for situations in which the priority is security however, for latency-sensitive scenarios they may not be feasible.

5.11. Energy Efficiency

Sustainability is considered critical for modern modern applications and today's applications should be energy efficient. Energy efficiency means that while decreasing energy usage, how effectively the blockchain based identity management system utilizes its resources. . IoTeX and IOTA are most efficient in terms of energy because of the employment of lightweight protocols which are produced while looking at the needs of IoT devices, thus reducing energy requirements. SelfKey, VerseOne, and Civic also efficiency which is because its focus is more on secure APIs for enterprise applications rather than energy Efficiency. Furthermore, Kaleido and Sovrin provide medium energy efficiency and are less optimized for resource constraint environment. Civics showcase high energy efficiency which is due to the PoS mechanism which decreases consumer consumption while improving security. Neblio on the other hand, makes a mechanism but offers medium energy which is because its focus is more on secure APIs for enterprise applications rather than manage complex communication and increase the sustainability demands.

5.12. Communication Overhead

The number of additional resources consumed by the system for transmission and processing data is referred to as communication overhead and in blockchain-based identity management systems, a high communication overhead impacts the scalability and network performance. IoTeX and IOTA result in low communication overhead, which is critical in IoT which is a resource-limited environment and in which efficient data exchange is necessary. Furthermore, SelfKey and Civic also provide low communication overhead, thus ensuring strong identity management without impacting the network resources. On the other hand, Neblio, VerseOne, Sovrin, and Kaleido offer medium communication overhead because these systems provide security through computationally heavy operations which makes them less suitable for deployments necessitating sustainability.

6. CHALLENGES

The detailed exploration of the existing work and the analysis of blockchain based idM use cases provided us with insights regarding the challenges they encounter.

1. The major concern is energy consumption because systems like Neblio despite using PoS sacrifices energy efficiency and instead focus on integration ease which make these solutions not suitable for energy limited environment.
2. In cloud and fog environments, the high computational overhead in existing methods necessitates lightweight systems, because of the resource-conservative nature of edge devices.
3. The employment of authorization techniques in permissioned and private blockchain faces challenge of blockchain overhead. Furthermore, the employment of smart contracts and their execution along with data encryption further increases this overhead, which results in slower response time, which hinders the scalability. Moreover, the blockchain based authentication methods that employ zero-knowledge proof also results in high computational overhead.
4. Existing systems for blockchain based idM such as Sovrin, VerseOne, and Kaleido manage high frequency data communication and different layered interactions which usually result in medium to high communication overhead. This overhead can drain the system from its resources and affect its performance more, in resource-limited environments such as IoT and fog computing.
5. The environments where real-time data processing is critical require low latency for effective interactions. Existing methods suffer from latency problems that hinder their applicability in latency sensitive environments such as IoT.
6. The majority of blockchain based identity idM are designed for specific platforms and encounter problems related to interoperability. For example, the methods that incorporate hyper ledger fabric struggle to work with other blockchain

networks such as Neo or Ethereum without modifications. This limits the system's ability to integrate different features, specifically in environments that need cross-platform data transactions.

7. The operational cost associated with private blockchain in cloud, fog, and enterprises is high because these systems need constant maintenance and updates. Apart from that, huge storage requirements in the cloud and IoT also expand the operational cost.
8. Blockchain based idM method employing access control improves flexibility but requires more information to be saved and validated on the blockchain, which gives rise to privacy issues. Moreover, methods employing consortium blockchain, the problem of collusion among validators endangers the blockchain integrity and security.
9. Existing block chain based idM systems suffer from lower transaction speed with the increase in the number of transactions and devices. This limits these systems" applicability in scenarios where transaction speed is critical.
10. The majority of methods reviewed in the literature showcase good simulation results and proof of concept stages, however, face problems during deployment in real-world environments because of issues related to packet loss, network delays, and dynamic workloads.

7. FUTURE DIRECTIONS

In this section, we highlight different key future directions with which researchers should incorporate to deal with the challenges associated with blockchain based idM.

1. Future Work should make use of advanced consensus mechanisms such as sharding which distributes the blockchain into two parts to ensure parallel transaction processing. Furthermore, DPoS should be more employed which will help reduce the validation time in large-scale environments. This will improve the scalability of blockchain based idM system. Moreover, fog, and edge based decentralized processing should be incorporated more to ensure dynamic load balancing and less bottleneck and improve the system scalability.
2. Future systems should incorporate hybrid architecture which combines the public and private blockchain features to minimize the latency and decrease communication overhead in idM solutions. This type of system will transfer the resource consuming task to the permissioned layer and use decentralized layers for auditing purposes. This will lower communication delays and will allow important operations to be processed locally which will result in better acceptance in environments like IoT and fog computing.
3. Moving forward, more focus should be put on optimizing communication protocols which decrease the network congestion and reduce communication overhead in blockchain based identity management systems. Furthermore, by making use of off-chain processing and message passing methods, data transmission can be accelerated which will minimize latency.
4. In the future, there is a further need to improve the security of blockchain based idM solutions. These solutions should incorporate quantum-resistant algorithms such as lattice cryptography and hashed-based signatures to improve data security against quantum computing attacks. Moreover, Future methods should make use of adaptive privacy methods that adjust their privacy level dynamically based on user context and risk factors.
5. Future work should embrace universal identity standards such as VCs and DIDs to improve compatibility among different platforms. Researchers should also consider developing universal standards to ensure identity management is more reachable and uniform among different applications.
6. In the future, there is a need to design a framework based on cross-chain communication that ensures absolute interaction among different blockchain networks. With Palkadot and Cosmos, the data flow will become free and efficient between different blockchain networks. This will help the blockchain identity management system to access and verify the identities among different platforms.
7. In the coming years, more focus should be put on scalability testing in real-world scenarios to distinguish the performance bottleneck in blockchain based idM systems. Furthermore, the simulation of high-volume transactions and user interaction will also help in detecting the system's ability to handle large-scale dynamic deployments. Apart from that, researchers should prioritize incremental adoptions in future deployments using controlled pilot projects to test the blockchain based identity management solutions in specific industries. This will provide the ability to gradually integrate blockchain solutions, thus creating the risk and challenges before full scale adoption.

8. In future, more focus should be given to technologies that rely on green blockchain that reduce energy consumption while offering effective performance. By consensus mechanisms such as PoS and Proof of Authority (PoA), energy consumption can be reduced in contrast to PoW based methods. There is also a need to combine sustainable infrastructure and energy-efficient cryptographic algorithms to further reduce energy consumption and develop more environment friendly approaches.
9. There is a need to incorporate AI into blockchain based idM systems to improve security and performance. The incorporation of AI in such systems will help detect anomalies and improve the process of fraud detection in real-time. The employment of machine learning algorithms in the future will optimize the process of authentication by dynamically predicting potential dangers and adapting access controls.
10. Future systems should put their focus on improving the transaction speed using layer 2 solutions for instance, state channels and rollups to offload transaction processing from the main chain. Moreover, researchers should also find mechanisms to enhance the performance of smart contracts in identity verification to minimize the delays in transaction execution.
11. In the future, blockchain based identity management methods can use open-source developments to minimize costs through the use of community collaboration and contributions. Because open-source platforms give developers to ability to design and customize the solutions without requiring expensive infrastructure. With known open-source frameworks, organizations can minimize the cost of licensing and enhance the speed of system deployments. To minimize the operational cost, future methods should also optimize the smart contracts so they only execute necessary functions which will minimize the computational resources and the transaction fees.
12. The future methods should make use of dynamic compliance tools that adapt automatically to the changing regulatory requirements. These tools can monitor legal changes in running time and adjust the policies according thus improving compliance with standards. Moreover, the compliance process can be further improved by smart contracts, automated auditing systems along the integration of AI. This will help in distinguishing risks and will suggest the correct actions according to the regulations.

8. CONCLUSION

The integration of blockchain in identity management overcomes the limitations of traditional identity management systems and provides secure, enhanced privacy, and decentralized solutions. This work aims to showcase the ability of blockchain based identity management solutions in evolving environments such as cloud, fog computing, IoT, and enterprise systems. The review of existing literature highlights the strength of those methods in providing secure identity management. However, they face limitations in the shape of latency issues, scalability challenges, communication overhead, and lack of regulatory compliance. Furthermore, the review of existing blockchain platforms for identity management reveals that platforms like IoTeX and IOTA are lightweight and offer energy efficiency which makes them suitable for IoT. Furthermore, solutions like Sovrin, Civic and Neblio do cater for enterprise needs but offer limited scalability. SelfKey and Civic excel for fog and cloud computing by offers high scalability. Futhermore, these platforms face challenges in the form of limited latency, limited interoperability, limited scalability, high operational cost, and high communication overhead and computational cost, which hinder their applicability in large-scale applications. Handling these challenges is necessary and future work should use methods such as integration of AI, designing context-aware access control, and using hybrid architecture to improve performance. Furthermore, future work should also focus on improving the deployment in real world setting. Lastly, the use of green blockchain technology and enhancing the performance of the smart contract can remove resource constraints and improve the operational cost as well. By overcoming these challenges, blockchain based identity management will play a more robust and efficient role in providing cyber security in IoT, cloud, fog computing, and enterprise systems.

REFERENCES

[1] Alsmadi, I.: Identity management. In: The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics, pp. 313–329. Cham: Springer International Publishing (2023). https://doi.org/10.1007/978-3-031-21651-0_12
[2] Larue, S.: ITRC H1 2024 findings - Over 1B data breach victims. Bluefin (2024). https://www.bluefin.com/bluefin-news/itrc-h1-2024-findings-over-1b-data-breach-victims/ (accessed Dec. 10, 2024).
[3] Simpson, W. R., Foltz, K. E.: Secure identity for enterprises. IAENG Int. J. Comput. Sci. 45(1) (2018).
[4] Tirfe, D., Anand, V. K.: A survey on trends of two-factor authentication. In: Contemporary Issues in Communication, Cloud and Big Data Analytics: Proceedings of CCB 2020, pp. 285–296. Springer Singapore (2022). https://doi.org/10.1007/978-981-16-4244-9_23
[5] Verizon: 2024 Data Breach Investigations Report. Verizon Business, 2024 https://www.verizon.com/business/resources/T22a/reports/2024-dbir-data-breach-investigations-report.pdf (accessed Dec. 10, 2024).
[6] Mahalle, P., Babar, S., Prasad, N. R., Prasad, R.: Identity management framework towards internet of things (IoT): roadmap and key challenges. In: Recent Trends in Network Security and Applications: Proceedings 3, pp. 430–439 (2010). Springer Berlin Heidelberg . https://doi.org/ 10.1007/978-3-642-14478-3_43
[7] Dhamija, R., Dusseault, L.: The seven flaws of identity management: usability and security challenges. IEEE Secur. Priv. 6(2), 24–29 (2008).

https://doi.org/10.1109/MSP.2008.49
[8] Habiba, U., Masood, R., Shibli, M. A., Niazi, M. A.: Cloud identity management security issues & solutions: a taxonomy. Complex Adapt. Syst. Model. 2, 1–37 (2014). https://doi.org/ 10.1186/s40294-014-0005-9
[9] Sukianto, A.: Common cloud misconfigurations and how to avoid them. UpGuard, May 07, 2023. https://www.upguard.com/blog/cloud-misconfiguration
[10] Railkar, P. N., Mahalle, P. N.: Identity management for internet of things. 1st edn. (2022). https://doi.org/10.1201/9781003338505
[11] Zhu, X., Badr, Y.: Identity management systems for the internet of things: a survey towards blockchain solutions. Sensors 18(12), 4215 (2018). https://doi.org/10.3390/s18124215
[12] Caso, J., Cole, Z., Patel, M., Zhu, W.: Cybersecurity for the IoT: how trust can unlock value. McKinsey, 2023.
[13] Mendoza, M.: $11 trillion: potential economic impact of internet of things by 2025. Tech Times (2015).
[14] Dib, O., Toumi, K.: Decentralized identity systems: architecture, challenges, solutions and future directions. Ann. Emerg. Technol. Comput. 4(5), 19–40 (2020). https://doi.org/10.33166/aetic.2020.05.002
[15] Sabena, F., Dehghantanha, A., Seddon, A. P.: A review of vulnerabilities in identity management using biometrics. In: Second International Conference on Future Networks (2010). https://doi.org/10.1109/ICFN.2010.79.
[16] Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., Choo, K.-K. R.: Blockchain-based identity management systems: a review. J. Netw. Comput. Appl. 166, 102731 (2020). https://doi.org/10.1016/j.jnca.2020.102731
[17] Lim, Y., et al.: Blockchain technology the identity management and authentication service disruptor: a survey. Int. J. Adv. Sci. Eng. Inf. Technol. 8(4), 1735 (2018). https://doi.org/10.18517/ijaseit.8.4-2.6838
[18] Gilani, K., Bertin, E., Hatin, J., Crespi, N.: A survey on blockchain-based identity management and decentralized privacy for personal data. In: 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), (2020). https://doi.org/10.1109/brains49436.2020.9223312
[19] Nayak, A. K., Reimers, A., Feamster, N., Clark, R.: Resonance. In: Proceedings of the 1st ACM Workshop on Research on Enterprise Networking (2009). https://doi.org/10.1145/1592681.1592684
[20] Haouari, I., Mostapha, Z., Yassir, S.: Current state survey and future opportunities for trust and security in green cloud computing. In: Advances in Business Information Systems and Analytics, 83–113 (2017). https://doi.org/10.4018/978-1-5225-3038-1.ch004
[21] Sousa, P. R., Resende, J. S., Martins, R., Antunes, L.: The case for blockchain in IoT identity management. J. Enterp. Inf. Manag. (2020). https://doi.org/10.1108/jeim-07-2018-0148
[22] Alzoubi, Y. I., Alahmad, A., Kahtan, H.: Blockchain technology as a Fog computing security and privacy solution: an overview. Comput. Commun. 182, 129–152 (2022). https://doi.org/10.1016/j.comcom.2021.11.005
[23] Zhu, X., Badr, Y.: A survey on blockchain-based identity management systems for the Internet of Things. In: IEEE International Conference on Internet of Things (iThings) 2018. https://doi.org/10.1109/cybermatics_2018.2018.00263
[24] Kuperberg, M.: Blockchain-based identity management: a survey from the enterprise and ecosystem perspective. IEEE Trans. Eng. Manag. 67(4), 1–20 (2019). https://doi.org/10.1109/tem.2019.2926471
[25] Hansen, M., Schwartz, A., Cooper, A.: Privacy and identity management. IEEE Secur. Priv. Mag. 6(2), 38–45 (2008). https://doi.org/10.1109/msp.2008.41
[26] Goode, L.: The importance of identity security. Comput. Fraud Secur. 2012(1), 5–7 (2012). https://doi.org/10.1016/s1361-3723(12)70006-4
[27] Clauß, S., Köhntopp, M.: Identity management and its support of multilateral security. Comput. Netw. 37(2), 205–219 (2001). https://doi.org/10.1016/s1389-1286(01)00217-1
[28] Mohammed, I. A.: Systematic review of identity access management in information security. Int. J. Innov. Eng. Res. Technol. 4(7), (2017).
[29] Cao, Y., Yang, L.: A survey of identity management technology. In: International Conference on Information Theory and Information Security (2010). IEEE. https://doi.org/10.1109/icitis.2010.5689468
[30] Torres, J., Nogueira, M., Pujolle, G.: A survey on identity management for the future network. IEEE Commun. Surv. Tutor. 15(2), 787–802 (2013). https://doi.org/10.1109/SURV.2012.072412.00129
[31] Bertino, E., Takahashi, K.: Identity management: concepts, technologies, and systems. Artech House (2010).
[32] Jensen, J.: Identity management lifecycle - exemplifying the need for holistic identity assurance frameworks. In: Lecture Notes in Computer Science, pp. 343–352 (2013). https://doi.org/10.1007/978-3-642-36818-9_38
[33] Benantar, M.: Access control systems: security, identity management and trust models. Springer Science & Business Media (2005).
[34] Sharma, A., Sharma, S., Dave, M.: Identity and access management - a comprehensive study. In: 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), pp. 1481–1485 (2015). IEEE. https://doi.org/10.1109/ICGCIoT.2015.7380701
[35] Han, P., Sui, A., Wu, J.: Identity management and authentication of a UAV swarm based on a blockchain. Appl. Sci. 12(20), 10524 (2022). https://doi.org/10.3390/app122010524
[36] Fan, P., Liu, Y., Zhu, J., Fan, X., Wen, L.: Identity management security authentication based on blockchain technologies. Int. J. Netw. Secur. 21(6), 912–917 (2019).
[37] Blue, J., Condell, J., Lunney, T.: A review of identity, identification and authentication. Int. J. Inf. Secur. Res. (IJISR) 8(2), June 2018.
[38] Karatas, G., Akbulut, A.: Survey on access control mechanisms in cloud computing. J. Cyber Secur. Mobil. (2018). https://doi.org/10.13052/2245-1439.731
[39] Chapin, P.C., Skalka, C., Wang, X.S.: Authorization in trust management. ACM Comput. Surv. 40(3), 1–48 (2008). https://doi.org/10.1145/1380584.1380587
[40] Trnka, M., Cerny, T., Stickney, N.: Survey of authentication and authorization for the Internet of Things. Secur. Commun. Netw. 2018, 1–17 (2018). https://doi.org/10.1155/2018/4351603
[41] Yawalkar, P. M., Paithankar, D. N., Pabale, A. R., Kolhe, R. V., William, P.: Integrated identity and auditing management using blockchain mechanism. Measurement: Sensors 27, 100732 (2023). https://doi.org/10.1016/j.measen.2023.100732
[42] Podugu, S., Rayapureddi, V. K., Gupta, M.: Auditing Customer Identity and Access Management. Advances in IT Standards and Standardization Research Series, pp. 181–210 (2023). https://doi.org/10.4018/978-1-6684-8766-2.ch007
[43] Lesavre, L., Varin, P., Mell, P., Davidson, M., Shook, J.: A taxonomic approach to understanding emerging blockchain identity management systems. arXiv preprint arXiv:1908.00929 (2019).
[44] Chen, J., Liu, Y., & Chai, Y.: An identity management framework for Internet of Things. In: 2015 IEEE 12th International Conference on e-Business Engineering, pp. 360–364 (2015). https://doi.org/10.1109/ICEBE.2015.67.
[45] Habiba, U., Masood, R., Shibli, M. A., Niazi, M. A.: Cloud identity management security issues & solutions: a taxonomy. Complex Adaptive Systems Modeling, 2(1), 1–18 (2014). https://doi.org/10.1186/s40294-014-0005-9.
[46] Chadwick, D. W.: Federated identity management. In: International School on Foundations of Security Analysis and Design, pp. 96–120 (2007).

https://doi.org/10.1109/CIACS.2015.7395570.
[47] Jensen, J.: Federated identity management challenges. In: 2012 Seventh International Conference on Availability, Reliability and Security, pp. 230–235 (2012). https://doi.org/10.1109/ARES.2012.68.
[48] Chadwick, D. W.: Federated identity management. In: Foundations of Security Analysis and Design V, pp. 96–120 (2009). https://doi.org/10.1007/978-3-642-03829-7_3.
[49] Satybaldy, A., Hasselgren, A., Nowostawski, M.: Decentralized identity management for e-health applications: state-of-the-art and guidance for future work. Blockchain in Healthcare Today, 5, 195 (2022). https://doi.org/10.30953/bhty.v5.195.
[50] Goodell, G., Aste, T.: A decentralized digital identity architecture. Frontiers in Blockchain, 2, (2019). https://doi.org/10.3389/fbloc.2019.00017.
[51] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
[52] Bhutta, M. N. M., et al.: A survey on blockchain technology: evolution, architecture and security. IEEE Access, 9, (2021). https://doi.org/10.1109/access.2021.3072849.
[53] Gao, W., Hatcher, W. G., & Yu, W.: A survey of blockchain: techniques, applications, and challenges. In: 2018 27th International Conference on Computer Communication and Networks (ICCCN), pp. 1–11. IEEE (2018). https://doi.org/10.1109/ICCCN.2018.8487348.
[54] Pardeshi, K. R., Deepak, G., & Pareekh, P.: Review of Blockchain Architecture A Survey. A Journal of Composition Theory, 239–248 (2021).
[55] Zeng, S. Q., Huo, R., Huang, T., Liu, J., Wang, S., & Feng, W.: Survey of blockchain: principle, progress and application. Journal on Communications, 41(1), 134–151 (2020).
[56] Mohan, A. P., Asfak R., M., & Gladston, A.: Merkle Tree and Blockchain-Based Cloud Data Auditing. International Journal of Cloud Applications and Computing, 10(3), 54–66 (2020). https://doi.org/10.4018/ijcac.2020070103
[57] Kuznetsov, O., Kanonik, D., Rusnak, A., Yezhov, A., Domin, O., & Kuznetsova, K.: Adaptive Merkle trees for enhanced blockchain scalability. Internet of Things, 27, 101315–101315 (2024). https://doi.org/10.1016/j.iot.2024.101315
[58] Hewa, T. M., Hu, Y., Liyanage, M., Kanhare, S., & Ylianttila, M.: Survey on Blockchain based Smart Contracts: Technical Aspects and Future Research. IEEE Access, 9, (2021). https://doi.org/10.1109/access.2021.3068178
[59] Hewa, T., Ylianttila, M., & Liyanage, M.: Survey on blockchain based smart contracts: Applications, opportunities and challenges. Journal of Network and Computer Applications, 177, 102857 (2020). https://doi.org/10.1016/j.jnca.2020.102857
[60] Nguyen, G.-T., & Kim, K.: A Survey about Consensus Algorithms Used in Blockchain. Journal of Information Processing Systems, 14(1), 101–128 (2018).
[61] Platt, M., Sedlmeir, J., Platt, D., Xu, J., Tasca, P., Vadgama, N., & Ibañez, J. I.: The energy footprint of blockchain consensus mechanisms beyond proof-of-work. In: 2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 1135–1144 (2021). IEEE. https://doi.org/10.1109/QRS-C55045.2021.00168
[62] Sriman, B., Ganesh Kumar, S., & Shamili, P.: Blockchain technology: Consensus protocol proof of work and proof of stake. In: Intelligent Computing and Applications, pp. 395–406 (2020). Springer. https://doi.org/10.1007/978-981-15-5566-4_34
[63] Skh Saad, S. M., & Raja Mohd Radzi, R. Z.: Comparative review of the blockchain consensus algorithm between proof of stake (POS) and delegated proof of stake (DPOS). International Journal of Innovative Computing, 10(2), Nov. 2020. https://doi.org/10.11113/ijic.v10n2.272
[64] Li, Y., Qiao, L., & Lv, Z.: An optimized Byzantine fault tolerance algorithm for consortium blockchain. Peer-to-Peer Networking and Applications, 14(5), 2826–2839, Mar. 2021. https://doi.org/10.1007/s12083-021-01103-8.
[65] Chen, Y.-C., Chou, Y.-P., & Chou, Y.-C.: An image authentication scheme using Merkle tree mechanisms. Future Internet, 11(7), 149, Jul. 2019. https://doi.org/10.3390/fi11070149.
[66] Mukhandi, M., Damião, F., Granjal, J., & Vilela, J. P.: Blockchain-based device identity management with consensus authentication for IoT devices. In: 19th Annual Consumer Communications & Networking Conference, pp. 433–436 (2022). IEEE. https://doi.org/10.1109/CCNC49033.2022.9700534.
[67] Shen, M., Lu, H., Wang, F., Liu, H., & Zhu, L.: Secure and efficient blockchain-assisted authentication for edge-integrated Internet-of-Vehicles. IEEE Transactions on Vehicular Technology, 71(11), 12250–12263 (2022). https://doi.org/10.1109/TVT.2022.3194008.
[68] Md. O. Ahmad et al.: BAuth-ZKP—A Blockchain-Based Multi-Factor Authentication Mechanism for Securing Smart Cities. Sensors, 23(5), 2757, 2023. https://doi.org/10.3390/s23052757.
[69] G. Deep, R. Mohana, A. Nayyar, P. Sanjeevikumar, and E. Hossain: Authentication Protocol for Cloud Databases Using Blockchain Mechanism. Sensors, 19(20), 4444, 2019. https://doi.org/10.3390/s19204444.
[70] L. Yu, M. He, H. Liang, L. Xiong, and Y. Liu: A Blockchain-Based Authentication and Authorization Scheme for Distributed Mobile Cloud Computing Services. Sensors, 23(3), 1264, 2023. https://doi.org/10.3390/s23031264.
[71] M. Vivekanandan, S. V. N., and S. R. U.: Blockchain based Privacy Preserving User Authentication Protocol for Distributed Mobile Cloud Environment. Peer-to-Peer Networking and Applications, 2021. https://doi.org/10.1007/s12083-020-01065-3.
[72] O. Umoren, R. Singh, S. Awan, Z. Pervez, and K. Dahal: Blockchain-Based Secure Authentication with Improved Performance for Fog Computing. Sensors, 22(22), 8969, Nov. 2022. https://doi.org/10.3390/s22228969.
[73] O. Umoren, R. Singh, Z. Pervez, and K. Dahal: Securing Fog Computing with a Decentralised User Authentication Approach Based on Blockchain. Sensors, 22(10), 3956, May 2022. https://doi.org/10.3390/s22103956.
[74] Babu, E. S., Devi, A. A., Kavati, I., & Srinivasarao, B. K. N.: Blockchain-based Authentication Mechanism for Edge Devices in Fog-enabled IoT Networks. In TENCON Region 10 Conference, pp. 558-563 (2023). IEEE. https://doi.org/10.1109/TENCON58879.2023.10322432
[75] Mounnan, O., El Mouatasim, A., Manad, O., Hidar, T., Abou El Kalam, A., & Idboufker, N.: Privacy-aware and authentication based on blockchain with fault tolerance for IoT enabled fog computing. In Fifth International Conference on Fog and Mobile Edge Computing, pp. 347-352 (2020). https://doi.org/10.1109/FMEC49853.2020.9144845.
[76] Sidorov, M., Ong, M. T., Sridharan, R. V., Nakamura, J., Ohmura, R., & Khor, J. H.: Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains. IEEE Access, vol. 7, pp. 7273–7285, 2019. https://doi.org/10.1109/access.2018.2890389.
[77] Autry, C. P., & Roscoe, A. W.: Decentralised edge authentication in the industrial enterprise IoT space. International Journal of Computer and Information Engineering, 14(11), 413-416, 2020.
[78] Cao, Z., Wen, X., Ai, S., Shang, W., & Huan, S.: A decentralized authentication scheme for smart factory based on blockchain. Scientific Reports, 14(1), Oct. 2024. https://doi.org/10.1038/s41598-024-76065-x.
[79] Zaidi, S.Y.A., Shah, M.A., Khattak, H.A., Maple, C., Rauf, H.T., El-Sherbeeny, A.M., El-Meligy, M.A.: An attribute-based access control for IoT using blockchain and smart contracts. Sustainability 13, 10556 (2021). https://doi.org/10.3390/su131910556
[80] Ding, S., Cao, J., Li, C., Fan, K., & Li, H.: A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. IEEE Access, 7, 38431–38441 (2019). https://doi.org/10.1109/access.2019.2905846.
[81] Al Neyadi, D., Puthal, D., Dutta, J., & Damiani, E.: Role-Based Access Control in Private Blockchain for IoT Integrated Smart Contract. IFIP Advances in

Information and Communication Technology, 227–245 (2023). https://doi.org/10.1007/978-3-031-45882-8_16.
[82] Xu, R., Chen, Y., Blasch, E., & Chen, G.: Blendcac: A blockchain-enabled decentralized capability-based access control for IoTs. In: 2018 IEEE International Conference on Internet of Things (iThings), pp. 1027–1034 (2018). https://doi.org/10.1109/Cybermatics_2018.2018.00191.
[83] Wang, S., Wang, X., Zhang, Y.: A secure cloud storage framework with access control based on blockchain. IEEE Access 7, 112713–112725 (2019). https://doi.org/10.1109/access.2019.2929205.
[84] Sukhodolskiy, I., Zapechnikov, S.: A blockchain-based access control system for cloud storage. In: 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 1575–1578 (2018). IEEE.
[85] Sohrabi, N., Yi, X., Tari, Z., Khalil, I.: BACC: Blockchain-based access control for cloud data. In: Proceedings of the Australasian Computer Science Week Multiconference, pp. 1–10 (2020). https://doi.org/10.1145/3373017.3373027
[86] Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., Yu, K.: AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud. IEEE Access 8, 70604–70615 (2020). https://doi.org/10.1109/ACCESS.2020.2985762
[87] Panda, S., Sahoo, S., Halder, R., Mondal, S.: Contextual attribute-based access control scheme for cloud storage using blockchain technology. Software Pract. Exp. 54(10), 2042–2062 (2023). https://doi.org/10.1002/spe.3250
[88] Tuli, S., Mahmud, R., Tuli, S., Buyya, R.: FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing. J. Syst. Softw. 154, 22–36 (2019). https://doi.org/10.1016/j.jss.2019.04.050
[89] Li, J., Li, D., Zhang, X.: A secure blockchain-assisted access control scheme for smart healthcare system in fog computing. IEEE Internet Things J. 10(18), 15980–15989 (2023). https://doi.org/10.1109/JIOT.2023.3268278
[90] Gowda, N. C., Manvi, S. S., Malakreddy, B.: Blockchain-based access control model with privacy preservation in a fog computing environment. In: International Conference on Electronics, Computing and Communication Technologies (CONECCT), pp. 1–6 (2022). https://doi.org/10.1109/CONECCT55679.2022.9865845
[91] Chaurasia, A., Kumar, A., Rao, U. P.: BACP-IeFC: designing blockchain-based access control protocol in IoT-enabled fog computing environment. Cluster Computing 27(10), 13919–13944 (2024). https://doi.org/10.1007/s10586-024-04656-4
[92] Madaan, C., Agarwal, R., Saini, V., Kumar, U.: Decentralized Access Control Infrastructure for Enterprise Digital Asset Management. Cryptology ePrint Archive (2024).
[93] Markus, I., Xu, L., Subhod, I., Nayab, N.: DAcc: decentralized ledger based access control for enterprise applications. In: International Conference on Blockchain and Cryptocurrency, pp. 345–351 (2019). IEEE. https://doi.org/10.1109/BLOC.2019.8751479.
[94] Xu, L., Markus, I., I, S., Nayab, N.: Blockchain-based access control for enterprise blockchain applications. Int. J. Network Manag. (2019). https://doi.org/10.1002/nem.2089.
[95] Fan, X., Chai, Q., Li, Z., Pan, T.: Decentralized IoT data authorization with pebble tracker. In: 6th World Forum on Internet of Things (WF-IoT), pp. 1–2 (2020). IEEE. https://doi.org/10.1109/WF-IoT48130.2020.9221130.
[96] Rathee, P.: Introduction to Blockchain and IoT. In: Studies in Big Data, pp. 1–14. Springer, (2019). https://doi.org/10.1007/978-981-13-8775-3_1.
[97] Kareem, Y., Djenouri, D., Ghadafi, E.: A survey on emerging blockchain technology platforms for securing the Internet of Things. Future Internet 16, 285 (2024). https://doi.org/10.3390/fi16080285.
[98] Alshaikhli, M., Elfouly, T., Elharrouss, O., Mohamed, A., Ottakath, N.: Evolution of Internet of Things from blockchain to IOTA: A survey. IEEE Access 10, 844–866 (2021). https://doi.org/10.1109/ACCESS.2021.3138353.
[99] Khrais, L.T.: Comparison study of blockchain technology and IOTA technology. In: 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud, pp. 42–47 (2020). IEEE. https://doi.org/10.1109/I-SMAC49090.2020.9243366.
[100] Silvano, W.F., Marcelino, R.: Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. Future Generation Computer Systems 112, 307–319 (2020). https://doi.org/10.1016/j.future.2020.05.047.
[101] Conti, M., Kumar, G., Nerurkar, P., Saha, R., Vigneri, L.: A survey on security challenges and solutions in the IOTA. J. Netw. Comput. Appl. 203, 103383 (2022). https://doi.org/10.1016/j.jnca.2022.103383.
[102] Tavares, B., Correia, F.F., Restivo, A.: A survey on blockchain technologies and research. J. Inf. Assur. Secur. 14, 118–128 (2019).
[103] Sobral, J.M., Solari, M., Matalonga, S.: Preliminary results of a multi-vocal literature review of blockchain networks. In: 2020 39th International Conference of the Chilean Computer Science Society (SCCC), pp. 1–8 (2020). IEEE. https://doi.org/10.1109/SCCC51225.2020.9281265
[104] Anwar, F., Khan, B.U.I., Kiah, M.L.B.M., Abdullah, N.A., Goh, K.W.: A comprehensive insight into blockchain technology: Past development, present impact and future considerations. Int. J. Adv. Comput. Sci. Appl. 13(11), (2022).
[105] Averin, A., Averina, O.: Review of blockchain frameworks and platforms. In: International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), pp. 1–6 (2020). IEEE.
[106] Alshurafa, S.M., Eleyan, D., Eleyan, A.: A survey paper on blockchain as a service platforms. Int. J. High Perform. Comput. Netw. 17(1), 8 (2021). https://doi.org/10.1504/ijhpcn.2021.120739
[107] Lima, V.C., Bernardi, F.A., Alves, D., Kritski, A.L., Galliez, R.M., Rijo, R.P.C.L.: A permissioned blockchain network for security and sharing of de-identified tuberculosis research data in Brazil. Methods Inf. Med. 59(06), 205–218 (2020). https://doi.org/10.1055/s-0041-1727194
[108] Kumi, S., Lomotey, R.K., Deters, R.: A blockchain-based platform for data management and sharing. Procedia Comput. Sci. 203, 95–102 (2022). https://doi.org/10.1016/j.procs.2022.07.014
[109] Naik, N., Jenkins, P.: Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology. In: 2020 International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), pp. 90–95 (2020). IEEE https://doi.org/10.1109/MobileCloud48802.2020.00021.
[110] Khovratovich, D., Law, J.: Sovrin: digital identities in the blockchain era. GitHub Commit by jasonalaw, 17(38–99), 41 (2017).
[111] Naik, N., Jenkins, P.: Sovrin network for decentralized digital identity: Analysing a self-sovereign identity system based on distributed ledger technology. In: International Symposium on Systems Engineering (ISSE), pp. 1–7 (2021). IEEE.
[112] Bethel, O. E., Opuwari, P. U.: Enhancing digital identity security: A comprehensive analysis of blockchain-based authentication systems. Intent Research Scientific Journal 3, 13–35 (2024).
[113] Alissa, N. A., Alrodhan, W. A.: Self-sovereign identity management: A comparative study and technical enhancements. Int. J. Comput. Sci. Netw. Secur. 23, 27–80 (2023). https://doi.org/10.22937/IJCSNS.2023.23.12.3
[114] El Haddouti, S., El Kettani, M. D. E. C.: Analysis of identity management systems using blockchain technology. In: 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), pp. 1–7 (2019). IEEE .
[115] Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., Avital, M.: Blockchain-Enabled Decentralized Identity Management: The Case of Self-Sovereign Identity in Public Transportation. Blockchain: Research and Applications, 2(2), 100014 (2021). https://doi.org/10.1016/j.bcra.2021.100014.

[116] Oliveira, B. M. G.: Self-sovereign Identity Decentralized Identifiers, Claims and Credentials Using non Decentralized Ledger Technology. Master's thesis, Universidade do Minho, Portugal (2021).

Authors

Anant Wairagade is a Technical Lead with over 20 years of experience in Software Engineering enabling IT organizations with digital transformation and helping them become secure organizations. In his more than two decades long career, Anant has worked for financial services companies where he led the design and development of several successful products in the Security and Finance and CRM domain. At the beginning of his career, Anant worked as a Technology consultant for major Financial Services companies and Banks. Anant is a thought leader in Enterprise Integrations solutions. He is an expert in API based data connector development, Kafka and Messaging Middleware. Anant is also an active member of several Industry Open Standard communities. He is an IEEE Senior member and serves as Program Committee Member for several IEEE and other IT conferences. He holds a bachelor's degree in computer science and engineering from Visvesvaraya National Institute of Technology, Nagpur, India.

Nikhil Gupta is an AI Product Management leader and researcher specializing in AI-driven security, fintech, and enterprise platforms. With a decade of experience at Atlassian, Samsung, and other tech companies/ startups, he has led AI innovations from ideation to large-scale adoption, impacting millions of users globally. At Atlassian, he spearheads AI-powered security initiatives, leveraging machine learning for threat detection, observability, and risk mitigation. Previously, at Samsung, he played a key role in launching Samsung Knox Asset Intelligence and Samsung Pay, contributing to enterprise security advancements and co-authoring Samsung's security white paper for the Galaxy Book series. His work in ML-driven fraud prevention at Western Union significantly enhanced transaction security. He holds advanced degrees in Computer Science (AI/ML) from Georgia Tech, Operations Research & Data Science from UC Berkeley, and Engineering from IIT Bombay. He has peer-reviewed over 20 research papers for IEEE and other top-tier conferences and is a recipient of prestigious fellowships, including the UC Berkeley Fung Fellowship, Charpak France Fellowship and Indo-Canadian Research Award.

Vijay Govindarajan builds secure distributed cloud systems and privacy-preserving architectures at Expedia Group. He leads critical cloud infrastructure and platform security initiatives for Expedia's global pricing and distribution systems. Previously, he contributed to Microsoft's e-commerce platform security through Digi Signals. His early research focused on distributed systems architecture and modern approaches for supercomputing, leading to publications in Computer Networks & Communications. Currently, his research interests span cloud security, distributed systems, privacy-preserving AI frameworks, and secure edge computing. He holds an M.S. in Computer Information Systems from Colorado State University and a B.E. in Electronics and Communications Engineering from Anna University.