IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 18 August 2022, accepted 11 October 2022, date of publication 25 October 2022, date of current version 3 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3216643

SURVEY

Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey

MD. RAYHAN AHMED, A. K. M. MUZAHIDUL ISLAM, (Senior Member, IEEE), SWAKKHAR SHATABDA, AND SALEKUL ISLAM, (Senior Member, IEEE)
Department of Computer Science and Engineering, United International University, Dhaka 1212, Bangladesh

Corresponding author: Salekul Islam (salekul@cse.uiu.ac.bd)

This work was supported by the Institute for Advanced Research Publication Grant of United International University under Grant IAR/2022/Pub/019.

ABSTRACT Identity Management System (IDMS) refers to how users or individuals are identified and authorized to use organizational systems and services. Since traditional identity management and authentication systems rely heavily on a trusted central authority, they cannot mitigate the effects of single points of failure. As a decentralized and distributed public ledger in a peer-to-peer (P2P) network, Blockchain (BC) technology has garnered a considerable amount of attention in the field of IDMS in recent years. Through Self-Sovereign Identity (SSI), users can have full authority over their digital identity. Successful implementation of a BC-based IDMS can significantly increase the degree of privacy and security of a user's SSI. However, the integration of BC-based IMDS to provide a user with SSI is still an unorganized area of research in its early stages of development. This article presents an extensive literature review of state-of-the-art academic publications as well as commercial market offerings regarding the applicability of BC-based SSI solutions. It also provides a detailed preliminary regarding the building blocks of blockchain technology and a progressive roadmap of IDMS solutions. In order to develop an effective BC-based IDMS solution that focuses on securing a user's SSI, this article outline five essential components of a BC-based IDMS: authentication, integrity, privacy, trust, and simplicity. Furthermore, we perform a security analysis that outlines several types of adversarial threats that can cause potential damage to the BC-based IDMS. We identify and discuss associated issues and challenges by analyzing several notable BC-based IDMS solutions in academic literature. We also highlight potential research gaps and provide future research scope.

INDEX TERMS Blockchain, peer-to-peer network, identity management system, self-sovereign identity, security.

I. INTRODUCTION

The Identity Management System (IDMS) is a collection of policies and technologies that work together to ensure that the relevant users within an organization have access to technology resources such as applications, systems, specific services, data, and cloud platforms. It guards against illegal access to systems and resources and generates alerts when unauthorized personnel or programs try to access information from inside or outside the enterprise perimeter. IDMS incorporates all technologies, procedures, and protocols within an enterprise used to distinguish, validate, and allow someone to use resources or programs within that enterprise and perhaps other similar organizations. Our digital online identity, which we use in our private dealings, occupation, health care system, academic institutions, or different professional associated events, somehow adds to the growing dependence on the digital identity management system, which is equipped to administer and preserve the people's digital identities with convenient facilities. It has become a crucial component in

The associate editor coordinating the review of this manuscript and approving it for publication was Mehdi Sookhak.

the management and authentication of digital identities. The purpose of a sophisticated IDMS is to improve the security of data and system productivity while lowering costs, and repetitive tasks. However, there exist several problems with the traditional IDMS, such as theft, fraud, lack of control, and loss of data [1]. By allowing more excellent connectivity across departments and other organizations, digital identification minimizes the level of administrative protocol and accelerates the timeliness of processes within enterprises. However, enterprises experience design and security difficulties with IDMS processes, forcing them to investigate new solutions. The majority of IDMS nowadays are centralized, with a single administrator controlling the system.

Blockchain technology and distributed ledger (DL) are generating a lot of buzz and spurring many initiatives in various industrial sectors. Nonetheless, the financial sector is seen as the primary user of blockchain technology. Blockchain technologies' emergence enables self-governing identities to practice decentralization where each node that participates is separate from the others. Instead of adopting a centralized authority's guidelines, distributed entities use common standards to connect yet preserve their independence and maintain internal confidentiality. An identity authentication system is required to keep the environments secure because of this decentralization of the network. Though blockchain is a relatively new technology, it possesses properties of transparency, immutability, credibility, tamper resistance, traceability, and decentralization necessary for various applications [2]. Using blockchain for identity management can give individuals ownership of their identities by providing a global ID that can be used for diverse purposes. The verification of digital identity confirms that individuals on digital platforms are who they appear to be. Identity verification and the security of confidential information are core components of trust in identity management. Personal information used to authenticate someone's identity, such as a name or unique identity number, is recorded on the block's hash using the blockchain authentication scheme. Self-Sovereign Identity (SSI) is a form of digital identity management that empowers individuals with control over their digital identities [3]. The Decentralized Trusted Identity (DTI) system facilitates verification of identity by allowing trusted third parties to verify an individual's identity by checking public credentials such as a passport, birth certificate, national identity card, or driving license [4]. A distributed ledger (i.e., blockchain) in identity management empowers everyone in the network to have the same measure of truth regarding which credentials are legitimate and then who verified the authenticity of the data residing in the credential without disclosing the authentic data. Numerous IDMS solutions are accessible on the market now, both in terms of their implementation and provided facilities. Features such as multifactor authentication, one-time passwords (OTPs), and biometric logins using fingerprints, facial and retinal scans have all gained widespread popularity due to mobile devices such as smartphones. IDMS-based on the blockchain is still an evolving area that must be studied and critically analyzed as a future breakthrough for digital identity and information management, but not guaranteed.

From the standpoint of academic research, BC-based IDMSs are gaining much attention to propose innovative solutions for digital identities. Researchers are exploring the scope of BC-based IDMS in diverse areas, such as cloud environments [5], [6], [7], [8], [9], [10], Electronic Health Records (EHR) systems [11], [12], [13], [14], [15], Internet of Things (IoT) [16], [17], [18], [19], [20], property and land registration [21], [22], [23], [24], [25], [26] and much more. Several surveys and reviews are conducted in the existing literature on BC-based IDMS. Houtal et al. [27] present a survey that studies SSI solutions for patient identity management in healthcare systems. Similar work done by Shuaib et al. [28] reviews the applicability of the BC-based SSI system in the healthcare sector and presents a model use case for representing the SSI system. However, the authors do not provide comprehensive details of the academic BC-based IDMS literature. Gordon and Catalini [29] review patient-driven interoperability solutions using blockchain. Soltani et al. [30] present a comprehensive survey regarding the SSI ecosystem and efficiently explain the building blocks of SSI architecture. However, there is a clear lack of review and analysis of both academic and market offerings regarding BC-based IDMS solutions. Liu et al. [31] present a review of generic BC-based IDMS and only discuss trust, authentication, and privacy components. However, [31] does not discuss the sub-features associated with each of the mentioned components. Kuperberg [32] presents a survey that discusses BC-based IDMS from the perspective of enterprise and ecosystem where the author establishes a set of 75 evaluation criteria to evaluate a BC-based IDMS solution. The author discusses critical issues of implementing a BC-based IDMS, including usability, implementation, compliance and accountability, regulation, standards, and integration from the point of the enterprise ecosystem. However, [32] along with [29], [30], [33], [34], [35] do not discuss academic research specifically in the field of BC-based IDMS. Zhu and Badr [36] provide a survey of BC-based IDMS for the Internet of Things (IoT) infrastructure and cover only a minor number of academic research along with market offerings. Their study lacks an in-depth analysis of the SSI ecosystem's standards and privacy issues, including its building blocks and concepts. Most of the surveys mentioned before do not provide a clear roadmap of the IDMS solutions. Moreover, most of them do not include a comprehensive analysis of various major digital identity management components such as user privacy, data integrity, authentication mechanisms, trust protocols, and simplicity of the digital identity management architecture. These components are discussed in detail in section V. Security of the user's data is one of the fundamental issues in BC-based IDMS, but none of those surveys discuss the diverse attacks that are possible in the BC-based IDMS structure. In Table 1, we present a comparative summary of our survey with existing noteworthy

surveys in academic literature regarding BC-based IDMS solutions.

The focus of this survey is to provide an overview of required tools and technologies and an in-depth understanding of the core components to build an effective BC-based decentralized solution by reviewing recent state-of-the-art advancements. This article presents a comprehensive analysis of the SSI research landscape as well as an overarching analysis of the blockchain types, iterating through several IDMS architectures before arriving at the distributed ledger-based decentralized approaches. It also provides a comprehensive discussion and comparison of existing commercial market offerings regarding both BC-based and non-BC-based IDMS solutions as well as proposed academic literature work on this expanding topic. Several survey and review articles focused on the most popular commercial BC-based IDMS solutions but did not adequately analyze or discuss the proposed BC-based IDMS in the academic literature. There is an apparent lack of academic surveys encompassing both market offerings and academic BC-based IDMS solutions by discussing five essential components of a BC-based SSI ecosystem: privacy, integrity, authentication, trust, and simplicity components and their corresponding sub-components in detail. We believe to the best of our knowledge; this study is the first to perform this. This article also presents an in-depth security analysis of the BC-based IDMS solutions by discussing various attack mechanisms that can damage the BC-based IDMS architecture. More precisely, we review the state-of-the-art BC-based IDMS for the SSI ecosystem in the diverse domains of IoT, cloud computing, electronic medical healthcare (EMH), Wireless Sensor Networks (WSN), and Generic BC-based IDMS solutions and their security analysis in academic research. We also focus on the research challenges associated with implementing BC-based management of digital user identity.

We are particularly interested in relevant English-language articles: reputed journals and conferences published between October 2015 and January 2022 in academic databases (e.g., IEEE Explore, ScienceDirect, ACM Digital Library, Wiley, Springer Link, Taylor & Francis, and MDPI) and patents. We also searched for related articles in Google Scholar too. The initial search strings that we used are (''digital identity management system'' OR ''IDMS'') AND (''blockchain''), (''decentralized identity management system'' OR ''decentralized-IDMS'') AND (''blockchain''), (''blockchain'' AND (''SSI'' OR ''self-sovereign identity'' OR ''SSI solution''), (''access-management'' OR ''access-control'') AND (''identity management system'' OR ''cloud'' OR ''Wireless Sensor Networks'' OR ''WSN'' OR ''Internet of Things'' OR ''IoT'' OR ''Healthcare'' AND ''blockchain''), (''decentralized identity'' OR ''integrity verification'' OR ''Authentication'' OR ''User Authentication'' OR ''Authorization'' OR ''SSI'' OR ''privacy-preservation'' OR ''privacy-protection'') AND (''blockchain''), (''digital identity trust models'' OR ''Trust framework'') AND (''blockchain''), (''IMDS'' OR ''SSI'' OR ''Trust models'') AND (''blockchain''), (''identity management security'' OR ''IDMS Security'' OR ''Threats'' OR ''Vulnerabilities'' AND ''blockchain''). Out of the one hundred and fifty-three articles studied, we discuss sixty-three notable articles in this paper. This study focuses on primary research. Reviews, surveys, and analyses are therefore omitted. We also omit those papers published as a summary or poster presentation. Papers that focus on user-centric and federated IDMS are also excluded. The final search strings that were used are (''digital identity management'' AND ''blockchain''), (''identity authentication'' AND ''blockchain''), (''blockchain'') AND (''self-sovereign identity'' OR ''SSI'' OR ''decentralized identity'' OR ''internet of things'' OR ''wireless sensor networks'' OR ''cloud computing'' OR ''healthcare''), (''blockchain'' AND ''self-sovereign identity'' AND ''privacy-preservation''), (''decentralized identity'' AND ''blockchain''), (''identity trust models'' OR ''identity trust framework'') AND (''blockchain''). (''access management'' OR ''access control'' OR ''authorization'') AND (''blockchain''), (''public integrity verification'' AND ''blockchain''), and (''identity management security'' AND ''blockchain''). The following summarizes the paper's major contributions:

- We present an in-depth review of the BC-based IDMS proposed in academic research in the domains of IoT, cloud computing, WSN, and EMH. We also review generic BC-based IDMS, which are not specific to any domain.
- Clear and concise preliminaries are provided regarding blockchain technology, and IDMS roadmaps leading to Distributed Ledger-based decentralized approaches.
- We also review notable commercial market offerings in the field of BC-based IDMS solutions and present a comparative summary among them by highlighting their application regarding Christopher Allen's SSI principles, utilized blockchain, network type, transaction cost, and nature of implemented codebase.
- We outline five essential components of digital BC-based IDMS along with their sub-components that highlight a user's authentication, and privacy, systems simplicity, data integrity, and trust amongst anonymous users.
- A security analysis is also provided that discusses various attack categories that might serve as a potential threat to the BC-based IDMS architecture.
- Discussion regarding research challenges, issues, and future research directions are also provided.

Paper Organization: The organization of this survey is visually illustrated in Figure 1. The rest of the paper is organized as follows. Section II provides the required preliminaries, an overview of blockchain technology, and a clear roadmap of the IDMS leading to decentralized solutions. Section III reviews some notable commercial market offerings of both BC and non-BC-based IDMS. Academic research regarding BC-based IDMS in the field of cloud computing, the IoT, WSN, EMH, and Generic IDMS proposed

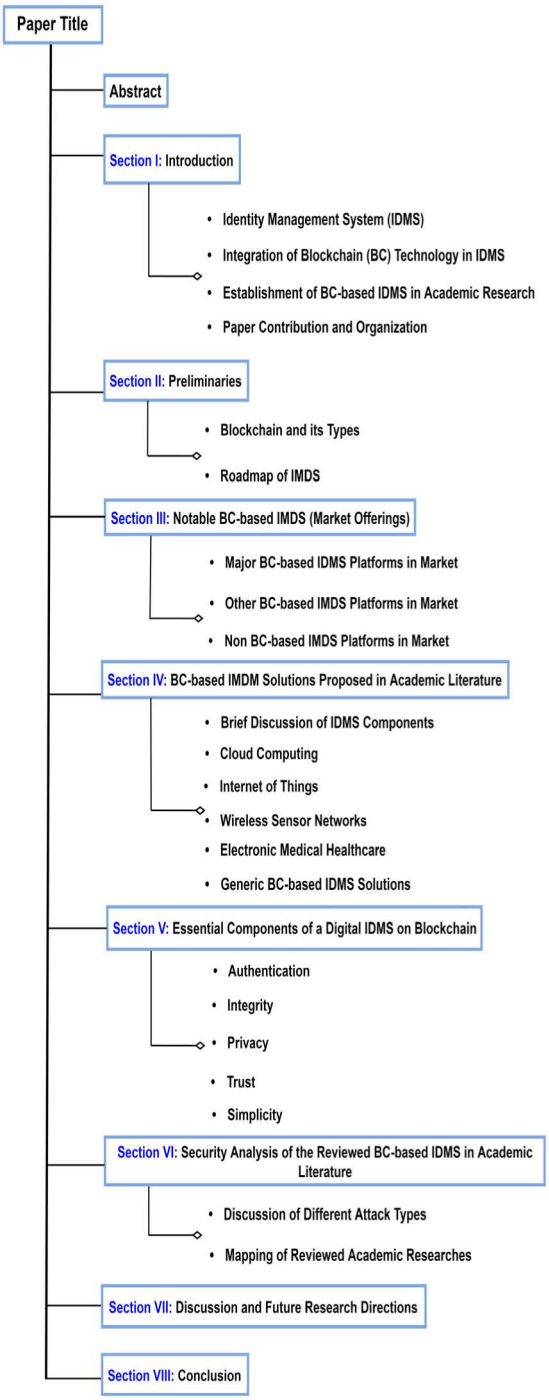

FIGURE 1. Pictorial illustration of the organization of this survey.

by researchers are reviewed in section IV. In section V, we outline the essential components of BC- based IDMS with their corresponding sub-components. Section VI provides a security analysis of the reviewed BC-based IDMS solutions. Section VII discusses the challenges, and issues associated with developing an effective BC-based IDMS and provides future research directions. We conclude the survey in section VIII.

II. PRELIMINARIES

Numerous sectors benefit from blockchain's transparency, security, and various other aspects, which add value to their organizations. Thus, it is poised to alter the management of digital identity in a highly secure and efficient manner. In the next section, we provide the required preliminaries of blockchain technology and provide an overview of the roadmap of the IMDS architectures.

A. BLOCKCHAIN

As the central infrastructure for Bitcoin [37] and other cryptocurrencies, blockchain is a DL architecture where all data is kept in equal-status nodes rather than a central server. Each node process data independently, ensuring the integrity of the blockchain system and relieving the pressure of increasing the volume of data on system resources [38]. By design, blockchain is decentralized because a decision is not based on a single point, but rather the decision is the outcome of the consensus of participating nodes in the chain. Consensus protocols of several forms exist, such as proof of work (PoW), proof of authority (PoA), proof of capacity (PoC), and proof of stake (PoS) amongst many more. Still, their purpose remains the same: to determine how participating nodes approve confirmed blocks and are added to the blockchain. It transfers trust from centralized entities to users in the network, allowing the dissemination of data and authority. It can be considered as a public, digitized, and shared ledger developed on a P2P setup [40]. In a blockchain, P2P transactions occur without the interference of a central authority and are validated with the same degree of assurance as a central authority. When a peer requests to join the network for the first time, several domain name system (DNS) servers, also referred to as DNS seeds, are communicated. These DNS seeds are used to locate active peers. Similar to a traditional public ledger, a blockchain consists of a chain of continuous data blocks where a block contains every committed transaction. A graphical illustration of a blockchain is demonstrated in Figure 2. Each block consists of a timestamp, a parent block/previous block hash value, and a nonce which is a hash verification arbitrary number. The initial block of a blockchain is known as the genesis block, and it has no parent block. The genesis block assures the integrity and consensus of the entire chain of blocks. Using a hash value reference of the parent block, each block points to the immediately previous block. It is then expanded by each extra block and thus represents a ledger's entire transaction history [41]. We discuss the internals and types of blockchain networks below:

1) BLOCK

Blockchain is a collection of increasing sets of records, referred to as blocks that are linked and safeguarded by encryption. As depicted in Figure 3, a block consists of the block header (block metadata) and the body. The header contains the following: a block version that indicates the set

TABLE 1. Comparison of this work with existing surveys and reviews. (: addressed, x: not addressed, -: not applicable).

Ref.	Preliminaries of Blockchain Technology	IDMS Roadmap	BC-IDMS Solutions (Academic Research)	Number of Reviewed Academic Research	BC-IDMS Solutions (Market Offerings)	Security Analysis	Discussion Regarding Essential Components of a BC-based IDMS Architecture in Academic Research and Market Offerings				
							Privacy	Integrity	Authentication	Trust	Simplicity
[27]	✓	x	✓	17	x	x	x	x	x	x	x
[28]	x	x	✓	6	x	x	x	x	x	x	x
[29]	x	x	✓	-	x	x	x	x	x	x	x
[30]	✓	✓	x	-	✓	x	x	x	x	x	x
[31]	✓	✓	✓	30	✓	x	✓	x	✓	✓	x
[32]	x	x	x	-	✓	x	x	x	x	x	x
[33]	✓	✓	x	-	✓	x	✓	x	✓	x	x
[34]	✓	x	x	-	✓	x	x	x	✓	x	x
[35]	✓	✓	x	-	✓	x	x	x	✓	✓	✓
[36]	x	x	✓	5	✓	x	✓	x	x	✓	✓
[39]	✓	✓	✓	30	✓	x	✓	✓	x	✓	✓
Ours	✓	✓	✓	**63**	✓	✓	✓	✓	✓	✓	✓

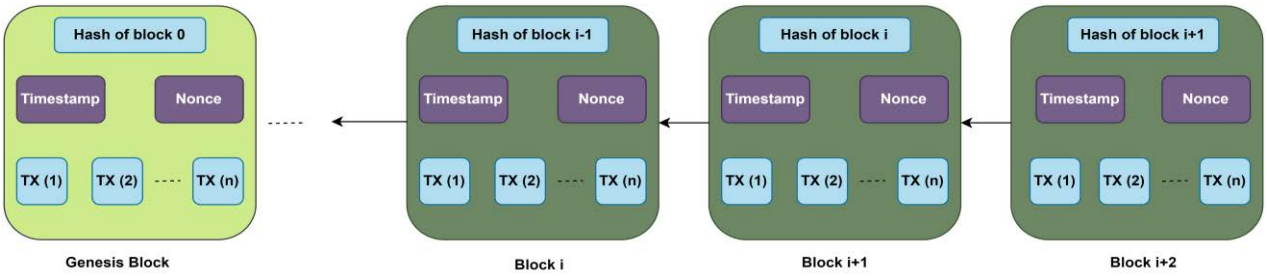

FIGURE 2. Example of a blockchain (Wang et al. [41]).

of validation rules to follow, a Merkle tree root that contains the hash of all the transactions, a 256-bit hash as a reference to the previous block, a timestamp that refers to the creation of that block, Difficulty (nBits) refereeing to the target threshold regarding the validity of the block hash, and a nonce value acting as the key ingredient of PoW consensus mechanism of the miners. A transaction counter and a list of transactions make up the block body. The highest number of transactions that can be stored in a block is determined by the block size and the transaction size. To validate transaction authentication, blockchain employs an asymmetric cryptography technique. Typically, an asymmetric cryptography-based digital signature is applied in an unreliable environment.

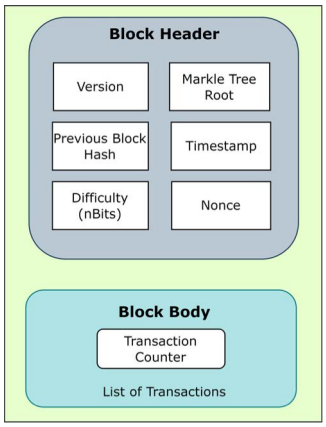

FIGURE 3. Structure of a block in a blockchain.

2) MINING

Blockchain mining is the process of using computing power to solve a cryptographic puzzle and miners are the individuals who mine the block. Mining is a time-consuming operation that demands significant investment and processing capacity [39]. If the miners find success in locating a new block, they receive the block's reward as compensation for contributing their processing power. Due to the difficulty of locating a block as an independent miner, miners typically join one or more mining pools and provide their computational power to the pools. Pool mining is a strategy in which miners collaborate to approve a transaction. Occasionally, the intricacy of the encrypted data in the blocks makes it challenging for an individual user to decrypt it. As a result, a group of miners collaborates to find a solution. Following

validation of the outcome, the incentive is distributed evenly among all users. Given the challenge of obtaining a valid block, the pool operator typically sets a lower difficulty for its miners than that of the blockchain network and requests that the pool's miners submit solutions that satisfy that difficulty [42]. For miners in a mining pool, the pool's reward method significantly impacts the miners' rewards.

3) DIGITAL SIGNATURE

A digital signature (DS) is a feature of an electronic document that allows the sender of data to be identified. Every user has a private and public key pair. Every transaction on the blockchain is signed by the sender's electronic signature, which is protected by their private key. The digitally signed transactions are disseminated over the whole network. True holders alone, as evidenced by the DS carried out all transactions. Some of the common DS algorithms employed in blockchain are the elliptic curve DS algorithm [43], and Edwards-curve DS Algorithm [44]. A typical digital signature process is illustrated in Figure 4. When sender A, tries to sign a transaction, A creates a hash value based on the transaction. A then encrypts this hash value using A's private key and transmits the encrypted hash together with the original data to the recipient B. B then validates the received transaction by comparing the hash value generated from the received data using the same hash function as sender A's and the decrypted hash (using A's public key). The DS provides the recipient B with the following information:

i. The message was created by a known sender A (authentication)
ii. Sender A cannot deny having sent messages (non-repudiation)
iii. The message was not altered during transmission (integrity)

B. TYPES OF BLOCKCHAIN

Blockchain solutions can be deployed using a variety of permission and access control techniques. There are four types of blockchain schemes: public, private, hybrid, and consortium. The scope of different blockchain types is depicted in Figure 5.

1) PUBLIC BLOCKCHAIN

A public blockchain, also known as a permissionless system, is a blockchain network that is entirely open to the public, and anybody can join and participate in it. As its underlying blockchain technology, most blockchain-based identification and authentication systems employ public blockchains such as Ethereum, Bitcoin, and Litecoin. The public blockchains are unchangeable, and decentralized, and are primarily used for exchanging and mining cryptocurrency. However, The data recorded on public DLs are available to everyone to track and evaluate [27]. Public blockchains do not scale well either. As additional nodes access and join the network, the network decelerates. To attain consensus, all nodes in a network must be in synchronization. Each node must solve a sophisticated, resource-intensive cryptographic challenge known as PoW. cryptocurrencies and document validation usually employ public blockchains [45].

2) PRIVATE BLOCKCHAIN

A private blockchain, also known as a permission-based system, is a blockchain network that operates in a restricted context, such as a closed network, and is controlled by a particular organization. It is only accessible by invitation, and anybody wishing to use it must first obtain authorization from the blockchain's governing body. The write permission of every node is carefully regulated by the governing organization, while read permission may be intermittently opened to the outside based on demand. Private blockchains are generally run on a small network within a corporation or organization where the identity and trustworthiness of participating nodes are known, thus making the identity verification and consensus mechanism simpler. Due to the lesser number of nodes compared to public blockchains, a private blockchain can execute transactions significantly quicker and at a lower cost. Hyperledger fabric [46] and Ripple are two of the most renowned private blockchains. These types of blockchains are typically utilized in the field of supply chain management and asset ownership [47], [48].

3) HYBRID BLOCKCHAIN

Both private and public blockchains have limitations; for example, public blockchains have lengthier validation processes for new data compared to private blockchains, while private blockchains are more subject to forgery and malicious actors. To solve these shortcomings, consortium and hybrid blockchains are constructed. The hybrid blockchain concept is made up of two components: private blockchain and public blockchain. This hybrid variant of blockchain networks allows companies to build up a private system alongside a public system. It enables them to regulate the access mechanism of particular data recorded in the blockchain through smart contracts and what data will be made public [19]. Even if a private entity owns the hybrid blockchain, it is unable to change transactions. Hybrid blockchains are managed by a single enterprise but are subject to scrutiny by the public blockchain to validate certain transactions. IBM Food Trust is a popular hybrid blockchain. When users join this hybrid blockchain network, they gain complete network access. Unless they engage in a transaction, their identity is protected from other users. It has several advantages, including the quickness of the private blockchain paired with the security provided by the public blockchain. The private blockchain produces a hash of transactions, and later it is authenticated and verified by the public blockchain. Hybrid blockchains are used in areas such as electronic medical records and real estate [23], [27].

4) CONSORTIUM BLOCKCHAIN

A consortium blockchain is also known as a federated blockchain. Similar to the hybrid blockchain, it covers

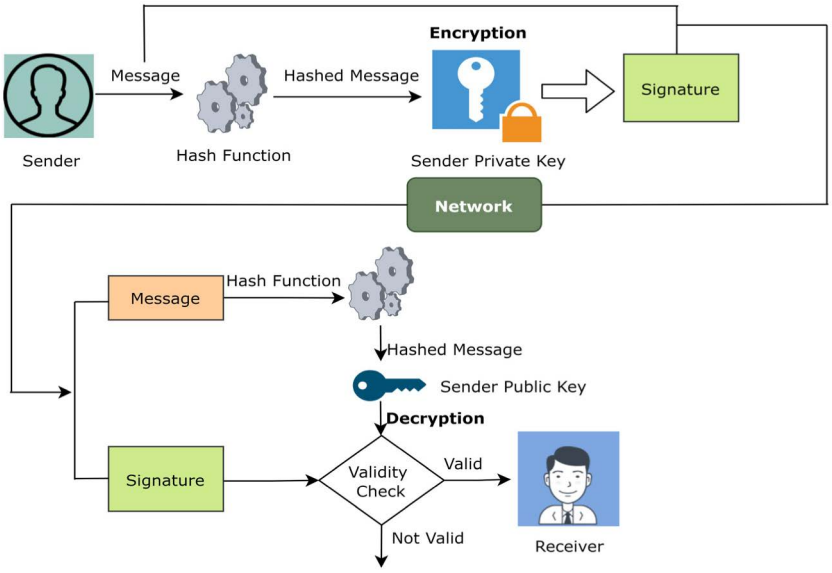

FIGURE 4. Workflow of a Digital Signature utilized in the blockchain.

features from both public and private blockchains. Nevertheless, it's different in that several organizational members collaborate to control the consensus procedure on a decentralized network. Here, more than one central authority is in charge. It is a permissioned blockchain that is managed by a collection of organizations instead of a single entity, as private blockchains are. This variety of blockchain has a greater degree of decentralization than private blockchains, which results in increased security. As opposed to a public blockchain, a consortium blockchain is an enterprise-level blockchain that does not have to deal with the challenges of developing a resource-saving global consensus mechanism [49]. It provides better customizability and offers better access controls but less transparency than a public blockchain. Banking, research, and payment systems are some of the use cases for this type of network. A comparative summary of the discussed blockchain types is presented in Table 2.

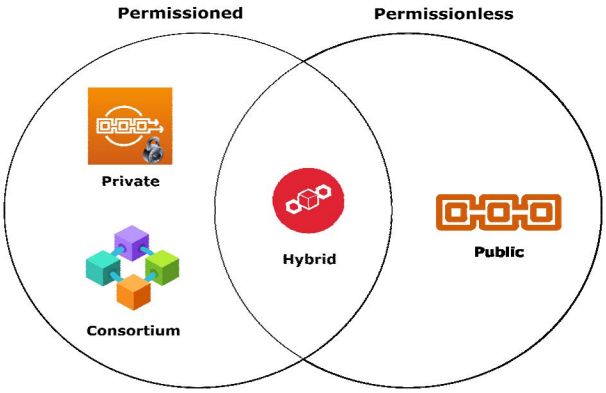

FIGURE 5. Scope of different types of blockchain.

C. ROADMAP OF IDMS

Identity is an important component of our everyday lives, both in the real world and online. Everybody utilizes their identity documents frequently on multiple platforms, and these documents are shared with third parties without their proper consent. Existing systems of identity management are hardly secure, with wrong authorization being a significant vulnerability. Users are requested to identify themselves via various government-authorized IDs such as national ID, vaccination cards, passports, and birth certificates. Sharing of multiple IDs brings the threat of identity theft, and lots of combinations of usernames and passwords for different services in the online platform, which brings the issue of the data breach. An IDMS must allow individuals to authenticate themselves first to get access rights to varying levels of infrastructure. As described by Stefanova et al. [50], a typical IDMS framework consists of the following stakeholders.

Identity Holder – Identity holders are the primary stakeholders of a typical IDMS framework, who benefit from the different services provided by the service and identity provider. Not every user has the same level of privilege [31].

Identity Provider (IdP)– IdPs are distributed trusted entities (i.e., companies, banks, organizations, etc.) that provide the users with their identity and related services such as authentication and registration. The issue of digital identification is automated, which saves time and eliminates the need for manual involvement.

Service Provider (SP) – SP is an entity that obtains users' credentials and provides required services by verifying with IdPs. Customer enrollment and validation of data are now much easier and less expensive. A workflow of a typical IDMS is presented in Figure 6.

TABLE 2. A comparative summary of blockchain types.

	Public (Permissionless)	Private (Permission-based)	Hybrid	Consortium
Benefits	Independence Transparency Trust	Access control Performance	Access control Performance Scalability	Access control Scalability Security
Drawbacks	Performance Scalability Security	Trust Auditability	Transparency Upgrading	Transparency
Use cases	Cryptocurrency Document validation	Supply chain Asset ownership	Medical records Real state	Research Banking Supply chain
Transaction Throughput	LOW (<= 100 Transactions per second)	High (> 100 Transactions per second)	High (> 100 Transactions per second)	High (> 100 Transactions per second)
Consensus Participation + Mechanism	All the miners PoW/PoS	Particular organization + Practical Byzantine Fault Tolerance (PBFT) / Ripple	Voting based mechanism + PBFT/ PoA/Tendermint	A selected set of nodes + Voting based mechanism
Infrastructure	Highly Decentralized	Distributed	Distributed	Decentralized
Example	Bitcoin, Ethereum, Litecoin.	Hyperledger Fabric, Quorum, SoluLab.	IBM Food Trust	Energy Web Foundation, R3.

Types of IDMS: This section will briefly discuss the evolution of different types of IDMS, beginning with the traditional centralized model and progressing through several phases as more models have been introduced.

1) TRADITIONAL CENTRALIZED IDMS

Traditional IDMS requires each individual to separately register and authenticate to the system for the service they desire. Businesses utilize this sort of IDMS service to store credentials (e.g., username, password) for each user with whom they do business. As illustrated in Figure 7, this enables a user to authenticate directly with the business they need to interact with, and each SP keeps each user's credentials. Here, both SP and IdP share the same space, which allows the user to directly register with the associated SP [3]. These multiple authentication credentials are a burden for many, as people use different authentication credentials for various online. Nevertheless, the user is encumbered by the requirement to authenticate separately, for each service using different credentials. Here different IdP controls the users' identity records for different services accessed by the user, which can also be canceled or exploited [35]. Major SPs, notably Google, Microsoft, Yahoo, eBay, and Amazon, amongst many, comply with this model; nevertheless, the trend is shifting toward other standards. However, there exist some problems with this method. Typical centralized IDMS suffer from the risk of single points of failure, a lack of interoperability, data breach, and privacy issues [51].

a: INACCESSIBILITY

A large number of people around the world have no proof of their identity in the internet world. This lack of identity is difficult to access identity-related data, mostly relying on paperwork processing. Still, most of the systems hugely rely on paper-based identities [51]. Therefore, it is presumed that if the hurdles of accessing physical resources are eradicated, it is possible to accumulate more persons to keep under the digital IDMS. A BC-based mobile identity system can be more efficient in solving these identity problems.

b: DATA INSECURITY

Most states maintain a centralized database to store the identity-related information of their citizens. A centralized system generally operates with legacy software that suffers significantly from single-point failure [52]. Adversaries from both inside and outside of the state are the main threats to such a system. It is not possible to be content with a cyber-attack unless the system itself follows a centralized mechanism.

c: IDENTITY THEFT

Identity theft is another crucial factor that has to be dealt with by every IDMS. Nowadays, a single user may have multiple identity profiles (i.e., usernames) for different online social platforms. The lack of standards for profile creation is the main reason behind the multiple identities of a single user [13]. As a result, social platforms are facing difficulties in identifying counterfeit users.

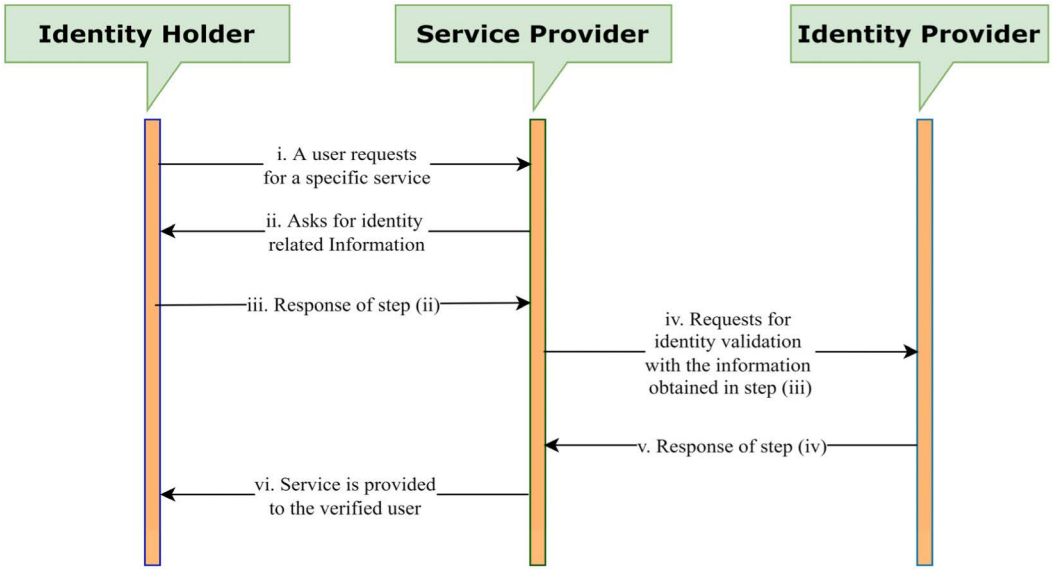

FIGURE 6. Workflow diagram of a typical IDMS solution.

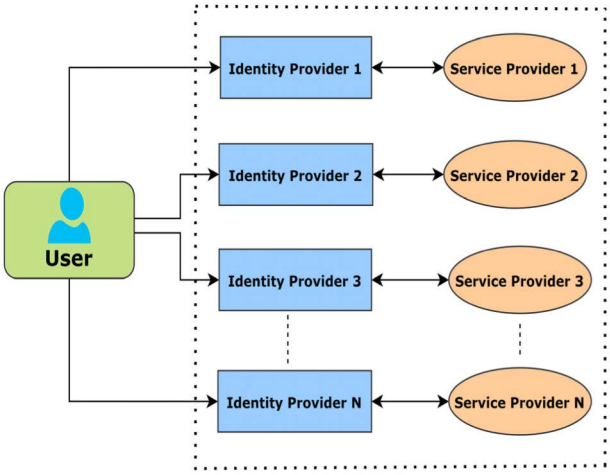

FIGURE 7. A pictorial representation of a traditional centralized IDMS.

2) FEDERATED IDMS

In the federated IDMS approach [53], a trustworthy federation is formed by a collection of SPs and IdPs [30]. In this type of IDMS, a user's credentials from one platform can be used to authenticate them on another different platform. In a federated IDMS, agreements between SPs are made to ensure that identities from various SPs are accepted across all business domains. These agreements cover a range of issues, from policy to technology standards. When a user is recognized and authenticated with a single SP using one of their agreed identifiers, they are deemed to have been recognized and verified with all of the other SPs as well [54]. This enables the user to access any participating SPs by authenticating through one of the federated IdPs. As shown in Figure 8, this method allows users to use a single set of authentication credentials provided by the IdP in order to gain privileges to smoothly access a large number of services. Here, each identity domain consists of a single IdP and one or more SPs [3]. An IdP acts as an intermediary which creates, manipulates, and handles user credentials, allowing users to register and log in to many SPs [55]. For instance, upon logging into a platform, the users are provided with the option to use their Facebook ID, Google ID, or other social media IDs; they engage with federated identity. An IdP is responsible for evaluating and validating user credentials, not the applications themselves. The SP relies on the IdP to authenticate the user and deliver the SP with user attributes and their values [3]. Although federated IDMS may provide users with convenience, the IdP still retains the control of the user's credentials [56]. This is accomplished by the IdP giving the SP an authentication token. This is referred to as single sign-on (SSO) [57]. This permits the use of social logins (e.g., Facebook, Google, etc.). Users can shift their identity from one provider to another by using the SSO of an IdP. Thus, it relieves the user of the burden of maintaining numerous credentials. However, it raises questions about interoperability, privacy, and security, given the credential SPs privileged position between the user and relying businesses [51]. Federated IDMS is beneficial in many access management applications, such as governmental services, information technology businesses, and educational institutions.

3) USER-CENTRIC IDMS

A user-centric version of identity management is followed by most BC-based IDMS. Instead of depending on a trusted intermediary, the user controls their identification credentials and communicates directly with various SPs [58]. In the user-centric model, when a user wishes to access a service provided by one of the designated SPs, that user is then

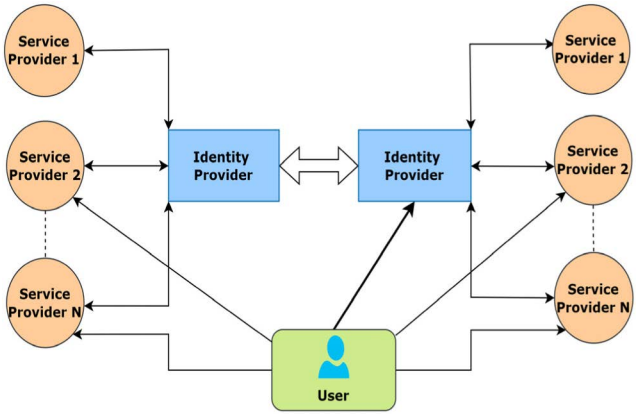

FIGURE 8. A pictorial representation of a federated IDMS.

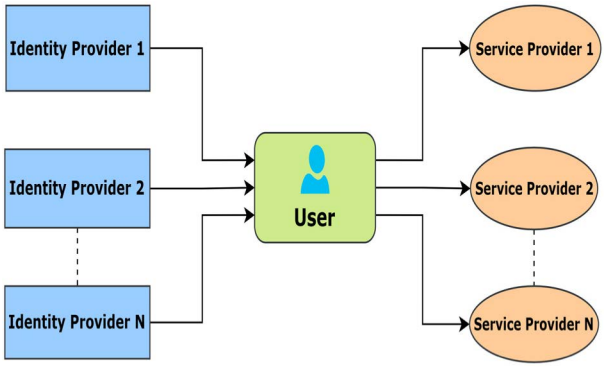

FIGURE 9. A pictorial representation of a user-centric IDMS.

forwarded to the requested IdP. The user authenticates himself to that IdP. After successful authentication, the IdP transfers the user attributes to the SP, where a decision is taken to accept or reject the service request generated by the user [3], [59]. The user must expressly consent to the use of his identity. As shown in Figure 9, the user can have multiple identifiers and the related credentials issued by one or more IdPs. Users have exclusive full control of their authorization or can choose third parties to do so in support of them [51], [60]. This enables users to share reliable information on a requirement basis. It seeks to give the total user control over their identity and provides a security and transparency level by enabling the identity holder to disclose only the required details to every SP for different services. Although, the SPs and IdPs may not always have an established trust relationship in this approach. Although, just like federated IDMS, the user-centric IDMS is designed to provide users more authority and control, IdPs retain ownership and control over user identities [56]. Some of the systems that leverage this user-centric model include OpenID [61], OAuth [62], Picos [63], and CardSpace [64]. The next step in this road map is the decentralized identity management system. Figure 10 illustrates the key roles within the VCs and the use of DIDs within the SSI framework.

4) DISTRIBUTED LEDGER-BASED DECENTRALIZED APPROACHES

Blockchain data structure-based distributed ledger (DL) technology has emerged as a new paradigm for digital IDMS, which aims to provide decentralization, transparency, privacy, and control to the users. DL-based IDMS mainly falls into the following two categories, self-sovereign identity (SSI) and decentralized trusted identity (DTI) [1], [4], [65]. Although SSI and DTI are similar in many ways, SSI is mostly used in the BC-based IMDS concept. This DL-based decentralized approach is the topic of discussion in this article.

a: SELF-SOVEREIGN IDENTITY (SSI)

Self-sovereignty demands that both individuals and organizations have control over their credentials and communicate as partners or peers. SSI allows you freedom of using your digital wallet and uses the credentials you were given to verify your own identity without giving up the control of personal information to loads of databases whenever you wish to access new products [66]. Ferdous et al. [3] provided a fundamental taxonomic outline of an SSI ecosystem by mathematically formalizing various properties of an SSI. Soltani et al. [30] investigate essential research initiatives, platforms, frameworks, and underlying key elements such as verifiable credential (VC), decentralized identifiers (DID), DL, and diverse privacy engineering protocols regarding SSI management. At the core of the SSI ecosystem, there exist two essential functions, namely, VC and DID [30], [67], [68].

i) VERIFIABLE CREDENTIALS

Verifiable credentials (VCs) [69] is a specification standardized by the World Wide Web Consortium (W3C) working group. It is a cryptographically secure, machine-readable, and tamper-resistant digitized alternative to physical, real-world credentials such as a passport, national ID card, or driving license. It is a decentralized process and involves the interaction of a trust structure between three distinct actors, namely, the identity holder, provider, and verifier [69]. Additionally, there is a publicly readable and verifiable data registry (VDR), which can be a blockchain, a DL, or other secure decentralized storage. The identity provider (IdP) issues the VCs mainly concerning an individual or occasionally an organization. The specific verifier itself determines if a provider is reliable or not. It can be a trusted party such as a university, certified company, bank, medical, or government agency that has been presented with a certain level of trust to deliver information. As shown in Figure 10, in step (1) and (2), IdP can issue personal credentials for a user and writes a public DID to a VDR. The VC comprises a series of claims about the holder's attributes, such as name, date of birth, ID, or any other related information the provider wishes to provide to the recipient. The holder entity receives the VCs upon request from the issuer and has full control over its controlling and verification. The holder entity manages its credentials in a digital wallet that the holder owns.

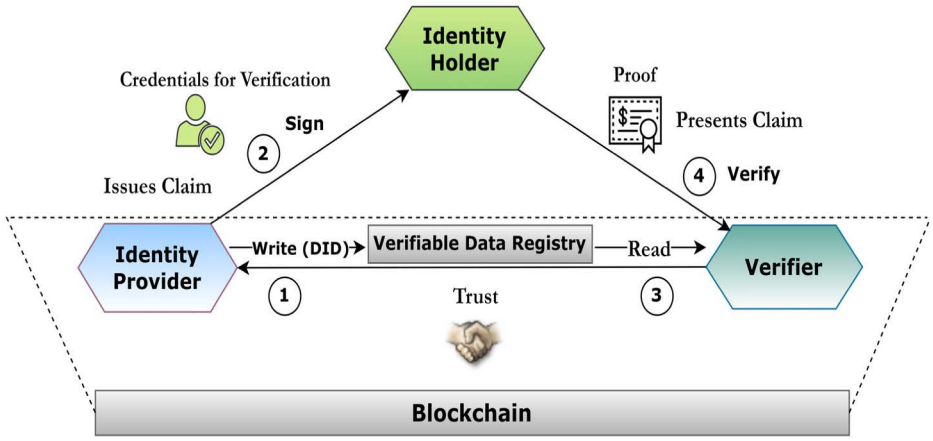

FIGURE 10. Self-sovereign identity framework among the verifiable credential actors i.e., identity holder, identity provider, and verifier actors.

In step (3) and (4), the verifier verifies the integrity, legitimacy of those user credentials when a user presents a claim. The verifier requests the respective holder about their identity information or attributes. It collects evidence that an authorized organization issued the VCs [30] by reading the records from the VDR. A website that requests credentials from its clients is an example of a verifier. The VDR can modulate the generation and verification of identities, cryptographic public keys, schemas for VCs, revocation registries, and other pertinent data that may require utilizing VCs [69]. The assistance of selective disclosure by VCs enables holders to authenticate their identity without disclosing more information than they need for performing a particular action [70]. Selective disclosure uses the zero-knowledge proof (ZKP) method to determine the extent of data to be disclosed.

ii) DECENTRALIZED IDENTIFIERS

For making the process of VCs work, the IdP, holder, and verifier are required to use Decentralized Identifiers (DIDs) [71]. It is a cryptographic counterpart to VCs and works with VCs to make the SSI framework function properly. It is a globally distinct, permanent, and secure cryptographic identifier of a DID subject [72]. When an organization issues VCs, they include their Public DID. The very same Public DID is recorded on the blockchain too, see steps (1) and (2) of Figure 10. When a holder shares a VC with a verifier, the verifier can check the DID on the blockchain to see who provided the credential, see steps (3) and (4) of Figure 10. The verifier can do so without contacting the providing party. The blockchain serves as a VDR in this case.

One of the most significant works on this SSI topic is an online article by C. Allen [73], in which he discussed the importance of SSI by representing the evolution of online identity. In the article "The Path to Self-Sovereign Identity," C. Allen has created a detailed list of SSI properties. Allen has pinpointed ten SSI properties that laid out the requirements for a system employing the SSI concept. Those points are mentioned below for the reader's expediency:

1. Existence–Users with SSI should have an identity in the real world. Every online identity is associated with a non-digital identity that represents and controls the online identity.

2. Control–Users ought to have whole control over their identities/credentials and should have the authority to be independent in their choices and actions.

3. Access–Users must be able to access their data and reclaim it anytime. No intermediary can influence or dispense the data that does not have access to it.

4. Transparency–Procedures of the system should be open to participate and open in the governance, while the algorithms should be open source and independent.

5. Persistence–Characters should be long-lived and the identifiers should be accessible as long as the owner of the identity wishes it to be.

6. Portability–SSI data such as service and information must be transportable without the need for a third party.

7. Interoperability–Identities should be broad, not restricted to any instance, but should be functional on as many instances or services as possible.

8. Consent–Users must have clear consent about accessing the data. The user should always define which data is to be shared and with whom by giving consent about it.

9. Minimization–Data claim disclosure must be minimized. Thus, only the slightest amount necessary to accomplish the required task must be revealed.

10. Protection–User's rights must be protected and respected in any case of conflict.

b: DECENTRALIZED TRUSTED IDENTITY (DTI)

DTI has been developed based on the core idea of SSI, which provides individuals with complete ownership over their personal data. DTI solution is similar to traditional digital identity management solutions in that it uses authorization

from a trusted service. DTI facilitates identity proofing by letting trustworthy third parties (TTP) verify public credentials like a passport, driver's license, or national ID card [1], [4]. It provides a service that authenticates the user and preserves his or her digital identity on the blockchain [74]. First, an identity holder registers with a TTP (e.g., IdP) through an identity proofing process. The TTP then approves the holder's registration and provides the holder with a VC. It records cryptographic proof of the VC in a blockchain. The holder generates a verifiable presentation from the VC and offers it to the SP in order to access the desired service. The SP verifies the presentation by matching it to the blockchain-stored cryptographic proof. After comparing the presentation, the SP provides the holder access to its service [75].

c: THE CONCEPTUAL DIFFERENCE BETWEEN SSI AND DTI

Though the two schemes have no significant difference, they are distinguished by their underlying concepts. From the existing literature and implementations, several possible conceptual differences can be observed between SSI and DTI. Both slightly differ in the method of identification-related data verification. DTI can be administered by a centralized service that verifies the identity of users using government-issued identification documents such as national ID cards, passports, social security numbers, and driver's licenses, among others. After verification, the validated identity attestations are maintained on a DL for further verification by third-parties [1], [74], [76]. On the contrary, SSI allows users to completely own and manage their respective identities without having to rely on any existing third-party attestations. Identity-related information can be gathered later by receiving credentials from different IdPs. With DTI, a user is not associated with any IdP or central registry [65]. So, a user is not bound to showcase his data to anyone for data validity. On the other hand, users store their data on their own devices in SSI, therefore can showcase their data to any other individual when someone needs to validate them without relying on a centralized authority. The DTI does not necessarily meet the requirements or conditions of SSI, such as controllability, portability, interoperability, and security [65]. Both SSI and DTI-based IDMS solutions can be developed on either permissionless or permissioned blockchains. The kind of blockchain utilized to construct the solution directly impacts the properties of IMDS solutions [74].

To summarize the IDMS approaches discussed above, in traditional centralized IDMS and federated IDMS, the administrative control is with the single authority and several federated authorities, respectively. The user-centric IDMS provides this administrative control to multiple authorities with the exclusion of the federation of IdPs. Decentralized BC-based approaches try to provide individual control across any number of authorities. In addition, the user-centric IDMS does not empower its users to manage their personally identifiable information entirely. On the contrary, decentralized BC-based approaches accomplish it using blockchain technology [40]. Compared to other approaches, the decentralized approaches can minimize data disclosure through selective disclosure and ZKP methods [77]. User identity information is stored at the IdPs of both federated and user-centric approaches, which raises the risk of availability, security, data breach, identity theft, and privacy issues raised with the traditional centralized IMDS. Decentralized BC-based SSI and DTI approaches try to address those challenges and shortcomings and give users complete control of their identity data. In the next section, we review some of the notable BC-based SSI and DTI solutions in the commercial market that we have named as *market offerings*.

III. NOTABLE BC-BASED IDMS (MARKET OFFERINGS)

Blockchain creates an SSI or DTI across distributed systems by ensuring trust, and privacy. Several companies and information technology organizations are concentrating their efforts on creating BC-based digital IDMS. Below, we discuss some major BC-based IDMS offered in the market.

A. MAJOR BC-BASED IDMS IN THE COMMERCIAL MARKET

This section will review the most common and globally studied BC-based IDMS schemes in academic research: uPort, Sovrin, and ShoCard. We consider these three schemes as major ones mainly because of their innovative SSI and DTI management approaches and the degree of disclosed information regarding the technical design, functionalities and documentation, white papers, and reports [1]. Dunphy and Peticolas [1] provide a comprehensive analysis and a summary of three of the mentioned schemes using Cameron's seven laws of identity [78]. The authors use Facebook connect for the comparative assessment. In another article, Haddouti et al. [79] also analyze the architectures of the mentioned IDMS applications and evaluated them based on Cameron's seven laws of identity. Ferdous et al. [3] analyzed different white papers and technical reports to check if the mentioned IDMS applications satisfy the foundational, flexibility, controllability, security, and sustainability properties of SSI.

1) UPORT

uPort [80] is an open-source decentralized identity framework that seeks to give everyone a decentralized identity [1]. It uses a public permissionless Ethereum blockchain and multiple smart contracts to maintain SSI. It consists of a mobile application, multiple Ethereum smart contracts, and a public registry for uPort identities [56]. Using this framework, users can safely disclose their identity, including the transfer of credentials for accessing different services, signing transactions, and managing keys and data securely. However, the original uPort project has been divided into two new projects, Veramo [81] and Serto [82], both aiming to give users control over their identity data. Veramo is a JavaScript-based framework that facilitates the usage of cryptographically verified data in applications utilized by anyone. Serto offers organizations to get started with DIDs and VCs. It is

built on W3C open standards [82]. In addition, uPort mobile applications, libraries, and services are deprecated now.

2) SOVRIN

Sovrin [66] is a public blockchain that anyone can use without obtaining prior authorization. It is based on a permissioned blockchain Hyperledger Indy, which means that only verified nodes can participate in the consensus procedure. Sovrin employs a voting ledger to grant permissions to nodes. The nodes are divided into two types, validators and observers. Validator nodes are permitted to commit new blocks in the blockchain, which contains transactions. Observer nodes, in contrast, only read the blockchain data [83]. Nodes, particularly validators, need unique privileges to join the network. A quorum of the board of trustees determines which privileges are granted [84]. According to the rules, this board's trustees can elect new members and choose stewards. Stewards are entities (trusted organizations within the ecosystem) responsible for performing consensus and managing validator nodes. Sovrin employs ZKP for all valid identity claims to keep data disclosure to a minimum [79].

3) SHOCARD

ShoCard [85] provides business users with a service for authentication and permission for information. It is a public Bitcoin blockchain-based digital identity and authentication platform. It enables individuals and companies to identify each other in a safe and verifiable manner to enable any transaction to be performed swiftly, effortlessly, and with peace of mind. ShoCard identities are kept in the bitcoin blockchain [86]. Users have their private keys on their phones or PCs, and they also have a public key that services can use to authenticate their identity with ShoCard. Though is built on top of a public blockchain, its architecture is engineered to be very scalable. However, Shocard does not provide minimization of data [33], [87], though Bokkem et al. [88] differ on that point.

B. OTHER BC-BASED IDMS PLATFORMS IN MARKET

In this section, we also review some other market offerings such as EverID [89], LifeID [90], SelfKey [91], Jolocom [92], Sora [93], IDchainz [94], Civic [95], BlockStack [96], MyData [97], and UniquID [98]. which are also emerging as secure decentralized architectures in the field of BC-based IDMS. However, these solutions are not as globally accepted or popular as uPort, Sovrin, and ShoCard platforms.

1) EVERID

EverID is a device-free, user-centric universal BC platform. It is mainly used for identification and value exchange that enables everyone to authenticate their identity, documents, and biometrics by multiple third parties. It also allows transferring funds between members of the network through a decentralized system. It is driven by a private Ethereum instance deployed on hardware that EverID manages. It differs from other SSI solutions because it does not require a device. After all, the digital identity (a mix of biometrics, government-provided ID, and third-party verification) can be kept in the cloud [88].

2) LIFEID

LifeID is a tokenized, open-source BC platform for the SSI ecosystem. It makes use of ZKPs to limit the disclosure of sensitive data [30]. A user's device stores the data, and only the necessary information is disclosed when the user's identification needs to be established. It does not use passwords; instead, it relies on biometric authentication, thus requiring biometric-capable smartphones and apps [88]. Only the users can approve a third party's request for information while maintaining their consent. If a user loses the private key, he or she can create a new pair of keys by updating the global public registry.

3) SELFKEY

SelfKey is a decentralized, BC platform for the SSI environment. It is an Ethereum-based platform that allows individuals to exchange their identification traits with certifiers and service providers such as notaries and banks. Individual users' data is stored on the user's device, which is within the user's control. Other entities can only access specific data if they have been granted permission [74].

4) JOLOCOM

Jolocom is another open-source lightweight SSI solution that, by default, leverages the Ethereum blockchain. It uses decentralized identifiers along with hierarchical deterministic keys to generate numerous identities from a seed master identity in order to give a decentralized identity solution [35]. It comprises multiple Ethereum smart contracts, one of which is a registry smart contract [3]. Users engage, generate, maintain, and share their identities via a mobile App similar to uPort.

5) SORA

Takemiya and Vanieiev [93] propose another SSI protocol, named Sora. It relies on Hyperledger Iroha and decentralized identifiers. It stores the encrypted copies of users' cryptographic keys and confidential data on a centralized server. It enables the user to store the salted hash format of users' private data on the blockchain and the related digital signatures created by identity issuers [30]. Through this feature, it achieves identity authentication and non-repudiation properties.

6) IDCHAINZ

IDchainZ is an extended proof of concept-based DTI for a smart ledger named ChainZy. It utilizes two independent mutual DLs - one for storing the individually encrypted documents and another transaction ledger for storing the documents' keys on a series of connected and unconnected document rings. Rings are hierarchical. While master rings are aware of all their sub-rings, the subrings are unaware of their parent – assuming they even have one. Every document ring is a self-executing program stored on the transaction ledger. Parent rings have the ability to control access to

sub-rings. Sub-rings can be designed to have a maximum number of uses or a predefined self-destruction date. It allows multiple dependent parties to add, certify and share know-your-customer (KYC), as well as anti-money laundering documents [99]. Later, these exchanges are extended to all forms of documents.

7) CIVIC

Civic resembles and functions similarly to a digital wallet, except instead of storing money, it safeguards personal information while enabling users to share it selectively. Here, identification information is maintained on the user's device so it is constantly available [89]. The Civic application provides several identity-aware features, ranging from password-free online logins to secure storage of sensitive data such as healthcare information, and bank statements. It authenticates users with the use of a smartphone fingerprint scanner. The data may then be shared directly with businesses and people, who can verify it using Bitcoin's blockchain [99]. After a user submits identity data, Civic checks it against the phone, credit card, social media, and other public records using several identity validation service providers. In order to establish a secure digital identity, civic users rely on authentication authorities, resulting in a lack of portability [100]. Civic achieves a high pass rate for genuine users. It limits the dangers of fraudulent conduct by integrating various reliable sources with fraud detection algorithms, and manual auditing. It distributes verified identification data to the user's Civic App and blockchain attestations.

8) BLOCKSTACK

BlockStack is a decentralized computing network and ecosystem of applications that empower users to manage their identity and data [96]. Rather than relying on application-controlled servers, users can contribute their computing and storage resources (i.e., the user's local machine) [35]. While using BlockStack, users are not required to submit data to an external website, for example, Facebook, or an application like WhatsApp. They can, however, continue to exchange their data and media with friends and other people. This is accomplished through the use of decentralized applications built on blockchain technology. These applications operate locally within the user's browser, and the user retains ownership of their data (text, videos, images, files, etc.). It employs encryption to safeguard user data and gives users more control over their data by utilizing public key cryptography [74].

9) MYDATA

MyData platform promotes the idea that users should have a clearer understanding of where their data is stored, who is using it, and how they can control this. MyData is a Nordic model for human-centric personal data processing. Its current form was devised when the Finnish Ministry of Transportation and Communication funded a whitepaper on human-centric data processing in the year 2014 [101]. It can be used to protect data transmission between sectors such as government, healthcare, and finance. MyData authentication is built on three components: user-managed access, OpenID single sign-on, and Oauth 2.0, which all regulate access to Web APIs [35]. It enables consent-based data management and control without requiring users to put all their data in centralized repositories in order to regulate data flow.

10) UNIQUID

UniquID is a system built on a certificate-based architecture that leverages blockchain technology to address the challenges associated with reconciling IoT credentials and cross-domain identity and access management. The system is based on an infrastructure that enables devices to authenticate directly with one another. It does not need the trusted third-party identity and access management platform, as envisioned by the PGP Web of Trust [102]. Some of the major enterprise frameworks for implementing the BC-based solution are Ethereum, Hyperledger, Bitcoin, Corda, enterprise operation system (EOS), Internet of Things applications (IOTA), Ripple, Waves, Quorum, and New economy movement (NEM) [103].

Since blockchain technology already possesses several of C. Allen's SSI properties [73], hence, blockchain platforms have been used to construct SSI and DTI applications. While each of the briefly discussed BC-based commercial solutions meets the majority of the SSI properties of C. Allen, each has some flaws. The uPort and Sovrin IDMS platforms provide limited portability, interoperability, and scalability [104]. Smart contracts in uPort are compact and limited in capacity. It utilizes a proof-of-work consensus process that is not particularly effective. Sovrin has complex design issues. Sovrin does not appear to provide or need verifiable guarantees for the proper operation of network agents. As a result, lacks transparency and provability properties [88]. Other systems, such as IDchainz and EverID do not meet the minimization requirement because the user will fully divulge any data required to authenticate a claim. EverID, in particular, is not open source and thus lacks transparency and provability. Civic is not an authentication authority, and its users rely on the authentication authority; therefore, it cannot invalidate or revoke identity assertions or identity-related data [32], [100]. As for BlockStack, it requires much documentation such as identification, tax forms, and licenses from a user to get up and running.

C. NON-BC-BASED IDMS PLATFORMS IN COMMERCIAL MARKET

It is worth noting that there are IDMSs that do not utilize blockchains but nonetheless implement SSI. Blockchain is considered an ideal foundation for implementing SSI. However, it is not the only method.

1) IRMA

Unlike other SSI platforms, IRMA [105] does not utilize a blockchain. Nevertheless, it bears many resemblances to other SSI platforms. It stands for ''I Reveal My Attributes'' and carries out the Idemix [106] attribute-based credential system developed by IBM Zurich. It stores all the user

attributes in the application. Only the schema is stored online. It presently only allows users to revoke their credentials, e.g., in case of theft or loss of their wallets. Presently, it does not let providers cancel granted credentials. Revocation is accomplished using a key-share server. A key-share server brings the issue of a single point of failure for credential use, prohibiting all users from accessing their credentials [107]. IRMA ensures minimization by utilizing the ZKP method. This ZKP approach offers issuers of digital signatures control over what can be seen and changed since issuance. Users who obtain digitally signed attributes from trusted issuers such as the government can prove that the claims are provable [88]. However, since blockchain ensures the persistent property, IRMA cannot provide persistence. In IRMA's case, this turns into either the user's accountability or the accountability of a centralized party. Non-BC SSI systems, like IRMA, require fewer deployment requirements than blockchain variants, making them a viable option for fast prototyping and attribute-based use case scenarios [108].

2) RECLAIMID

Apart from IRMA, other non-BC variants of SSI exist, named reclaimID, proposed by Schanzenbach et al. [109]. It employs attribute-based encryption, which permits the user to selectively authorize and restrict access of requesting parties of his required attributes, which are used to access different online services [110]. A GNU name system (GNS) stores and shares user attributes within user-owned namespaces. The namespaces are comparable to digital identities. A pair of a public and a private key can cryptographically define a namespace, where resource records resemble the self-issued attributes of a user.

Bokkem et al. [88] present a comprehensive assessment of eleven SSI-related BC and non-BC-based market offerings regarding the SSI principles of C. Allen [73]. In Table 3, we extend that comparative analysis by adding Jolocom, Blockstack, Civic, UniquID, and MyData platforms. We also provide additional comparisons based on cost, open-source codebase, decentralization type, network, and utilized blockchain. Comparisons on market offerings are also present in [1], [3], and [79], mainly focusing on uPort, Shocard, Sovrin, and Jolocom platforms. The next chapter reviews the notable BC-based IDMS solutions proposed in academic research.

IV. BC-BASED IDMS SOLUTIONS PROPOSED IN ACADEMIC LITERATURE

The architecture of the BC-based IDMS varies depending on the applications to which the IDMS scheme is applied. Any BC-based IDMS's main objective is to ensure the proper functioning of the following five components: authentication, privacy, integrity, trust, and simplicity. A complete BC-based IDMS performs not only the identity creation, management, deletion, and revocation of users but also the user's authentication and access management. Identity authentication ensures that the communicating parties are genuine. Authenticating a user's identity in a computer or network protects information security. An ideal authentication procedure should be efficient, and trustworthy, and protects user privacy while verifying user credentials [35]. Privacy deals with protecting data and information, which are being exchanged in a communication. Privacy preservation of a user's attributes is one of the key elements of any BC-based IDMS. Trust is more intricate than privacy and authentication. It ensures that any communicating party can customize schemes to build trust with other parties. A trust domain can be defined as an enclosed space with uniquely identifiable mutually trusted network elements, and a trust model can be described as a collection of identifiable network entities belonging to the same or diverse trust domains, together with their respective pairwise trust relationships [111]. Blockchains are inherently resistant to the tampering of data by design. The reliability and trustworthiness of data are referred to as data integrity. It entails the upkeep and assurance of data accuracy and consistency over its full life cycle. Simplicity relates to interoperability, scalability, cost, data portability, lesser energy consumption, and ease of control. Simplicity is desired in the comprehensive functioning of any BC-based IDMS. In Section V, we discuss these five major components in detail. Different authors proposed various schemes focusing on the aforementioned components regarding IDMS in the blockchain. Apart from the mentioned five components, we also review those articles which focus on access management of the users. Access management is one of the most critical security methods for securing sensitive data kept by businesses, the healthcare sector, and individuals in the cloud [112]. Access control mechanism is closely associated with the authentication property. Combining authentication and access control mechanisms with blockchain technology can considerably enhance the system's trustworthiness, availability, security, resource utilization, scalability, and transparency.

BC-based IDMS provides security for the cloud and electronic medical healthcare (EMH) users. It tries to ensure the authenticity of the user trying to access the cloud resources or electronic healthcare records. With the IoT and the increasing proliferation of connected devices, the inadequacy of an effective IDMS is a critical issue. It exposes devices vulnerable to security issues such as identity theft and unauthorized individuals seizing control of intelligent devices such as medical equipment. Clustered WSNs are frequently deployed in unprotected or even hostile environments, leaving them susceptible to numerous cyber-attacks and security threats that can adversely impact their overall performance. Next, we review some of the notable academic BC-based IDMS proposals in the field of cloud computing, IoT, WSNs, and EMH, and those IDMSs which are not specific to any domain are labeled as generic.

A. CLOUD COMPUTING

Cloud computing has been one of the most modern research topics due to the indefinite expansion of resource sharing

TABLE 3. The reviewed commercially implemented IDMS solutions annotated with which criteria are supported (✓), which are not Supported (x), and answer not found (-) using christopher allen's SSI principles [88], cost, and type of identity, type of network and blockchain. (Here, existence - e, control – C1, access – A, transparency – T1, persistence – P1, portability – P2, interoperability – I, consent -C2, minimization – M, protection – P3, cost – C3, open-source codebase – os, distributed ledger technology – dlt, network – n, blockchain – B).

System	E	C1	A	T1	P1	P2	I	C2	M	P3	C3	OS	DLT	N	B
uPort	✓	✓	✓	✓	✓	x	✓	✓	x	✓	Paid	✓	SSI	Public / Private	Ethereum
Sovrin	✓	✓	✓	✓	✓	x	✓	✓	x	✓	-	✓	SSI	Public / Private	Hyper Ledger Indy
ShoCard	✓	✓	✓	✓	✓	✓	✓	✓	x	✓	Paid	✓	DTI	Public / Private	Blockchain Agnostic
EverID	✓	✓	✓	x	✓	✓	✓	✓	x	✓	Paid	✓	SSI	Private	Ethereum
LifeID	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Paid	✓	SSI	Public	Blockchain Agnostic
SelfKey	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Paid	✓	SSI	Public / Private	Ethereum
IDchainz	✓	✓	✓	✓	✓	✓	✓	✓	x	✓	Free	x	DTI	Not Mentioned	ChainZy Smart Ledger
Jolocom	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Free	✓	DTI	Public	Ethereum
Sora	✓	✓	✓	✓	x	✓	✓	✓	✓	✓	Free only for school.	✓	SSI	Private	Hyperledger Iroha
BlockStack	✓	✓	✓	✓	x	x	✓	✓	✓	✓	-	✓	DTI	Private	Bitcoin
Civic	✓	✓	✓	x	x	x	✓	✓	✓	✓	Paid	✓	SSI	Private	Ethereum
UniquID	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Free for non-commercial use.	✓	DTI	Private	Blockchain Agnostic
MyData	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	x	SSI	Private	Hyper Ledger Indy
IRMA	✓	✓	✓	✓	x	✓	✓	✓	✓	✓	Free for users but providers are charged.	x	SSI	Not Applicable	Not Applicable
reclaimID	✓	✓	✓	✓	x	✓	✓	✓	x	✓	Free	✓	SSI	Not Applicable	Not Applicable

and improved user experience. Its enormous commercial potential is rapidly developing [113]. Cloud storage services provide substantial benefits in terms of data management for consumers. Additionally, it maintains the integrity of cloud data saved in the cloud and the processing of stored data across several data centers. At the moment, the primary issue with cloud user identity management systems is their excessive reliance on third-party services. Moreover, when users upload their data, code, and operating processes to remote cloud servers, they relinquish control over them. At the moment, user identity management and authentication are critical components in cloud systems. Identity authentication verifies that cloud market players are valid nodes, such as service providers and clients. Next, we review some notable BC-based IDMS proposed in academic literature in the field of cloud computing.

Wang and Jiang [2] utilize two-adic ring theory [114] and related arithmetic algorithms to authenticate identities in a consortium blockchain for a fog computing environment. The two-adic ring is a finite ring that can be used to represent any bit string contained within a finite field. Designed on this theoretical foundation, it inherits the effectiveness of binary sequence ciphers in computer communication and resolves many key distribution and node verification constraints. Password security is based in part on the two-adic ring theory. In the proposed scheme, the master node trusts one another; the master node is designed to provide the essential responsibilities of a key generation center and be responsible for block generation and accounting.

Bendiab et al. [6] integrate blockchain in cloud identity management by proposing a decentralized trust model. The scheme is comprised of the following phases: The user wishes to get access to secured resources and services of a cloud service provider (CSP) using trust management platforms with which he is not enlisted; these CSPs are referred to as foreign CSPs. The foreign CSP then refers the user to the home CSP for authentication. In the second and third phases, the home CSP evaluates the authentication request and generates an access token containing claims about the user's identity and rights. In phase four, the token is placed on the blockchain to establish that it is a legitimate token held by the user and issued by a trusted CSP in the Trust Management Platform (TMP). It considerably boosts the exchange's security and level of service. Lastly, after validating and storing the token on the blockchain, the CSP proceeds with the transaction and grants the user access to protected resources depending on the given access privileges; otherwise, the CSP halts the transaction and refuses access to protected resources. The proposed model enables service vendors to successfully manage their trust behaviors and connections with consumers or other providers in a dispersed, decentralized, and dynamic way.

Utilizing the consolidated IDMS protocol [115], Wang et al. [116] develop an Ethereum-based protocol for managing cloud user identity. They have ensured party authentication by using smart contracts with Jason Web Token (JWT). JWT consists of three components as presented in Figure 11. The first is the header, which contains information about the

type of token, i.e., the content being signed or encrypted, as well as the cryptographic techniques used to secure it. The payload is the second part of the token, and it contains verifiable security statements or a set of registered, public and private claims, such as the user's identity and the access they have. In the last part of the token, the signature verifies that the token is legitimate, and integrity is maintained. The goal of utilizing JWT is to confirm the data's authenticity, not to hide it. The protocol allows CSPs and users to manage the system together using the reputation values. Robust cryptographic measures are also evaluated for public-private key pair generation.

Sabir and Fetais [117], deploy a partially decentralized consortium blockchain system to provide a uniform patient-centric data portability model for healthcare. The system has four entities: hospitals, patients, storage providers, and the blockchain network. The patient has complete control over their data. Entities communicate with the network via their decentralized apps. To anchor vast quantities of data to the blockchain, the proposed method employs cryptographic hashing algorithms.

Nayak et al. [118] devise a system called Saranyu. It has been implemented on top of the Quorum blockchain system, in a cloud computing data center. By using smart contracts, it manages tenants, service accounts, and the usage of resources. The key aspects of the system are to create custom smart contract classes of users' payment credentials, as well as delegate permission for the usage of service characteristics to tenants, sub-tenants, and many other services.

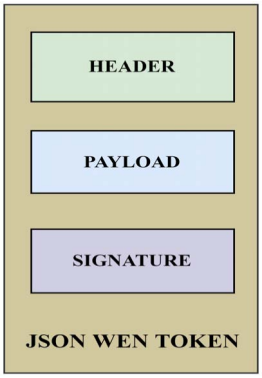

FIGURE 11. Components of a Jason Web Token (JWT).

Yang et al. [112] propose a framework that uses the account address of a blockchain node as the identity, instead of username and password which are stored by the cloud authentication database. The proposed system excludes a trusted center and does not force users to consider the cloud as a trusted center. The node address is used to authenticate the user. Authorization-related data is kept directly on the blockchain. Additionally, access records are recorded on the blockchain. The framework can also withstand a variety of attack types, both internal and external. The model is implemented on the EOS platform.

In a campus-wide printing service-related use case study, Ahmad et al. [119] integrate facial recognition along with blockchain to minimize the necessity for the immense transfer of data to a distant cloud system. The system is intended to be implemented through the use of cloudlet. Cloudlet enables low latency and high bandwidth connectivity for large-scale IoT device connectivity. Blockchain technology confirms the face identification produced by the facial recognition process. Access to printing services is granted when the user's identification is validated.

Li et al. [120] formulate a BC-based IDMS for cloud-native environments. In this context, blockchain serves as a trusted endorsement for service identification and public key distribution of records. The authors also propose a communication disconnect method to disconnect both TCP and UDP communication between services in case of any security issues.

Table 4 -8 presents a comparative summary of BC-based IMDS solutions integrated into cloud computing, IoT, WSN, EMH, and Generic domains. In each of these tables, we highlight the type of blockchain, contribution, decentralized approach, network, and scope of the paper. We also highlight the major strengths and limitations of each of the reviewed academic BC-based IDMS solutions in the abovementioned domains. It is worth noting that most of the papers discussed in this article only mentioned the term decentralized approach, not being specific about SSI or DTI.

B. INTERNET OF THINGS (IOT)

With the expansion of the Internet of Things (IoT) at an incredible rate, ranging from individuals, organizations, and companies to things in the physical and virtual world, every entity is facing challenges in managing the identity and access of its user. Overall security, resource-constrained devices, compatibility, and especially scalability cannot be managed using conventional methods. However, blockchain technology can serve as a catalyst for overcoming such obstacles. Several BC-based IDMS solutions have been proposed in the literature to provide a secure IDMS solution for the IoT domain incorporating healthcare and cloud systems. We review some of them below.

Abou-Nassar et al. [9] devise a distributed, interoperable trust architecture for healthcare and IoT that incorporates blockchains. The proposed IoT healthcare system is a robust ecosystem that enables semantic labeling for IoT healthcare's health edge layers. The authors have utilized cryptographic techniques to authenticate, verify and secure various phases of data collection and transmission.

A two-end secure and transparent e-voting system via IoT devices utilizing blockchain technology that comprises the national election commission and voters is presented by Rathee et al. [16]. The trust of the IoT devices is calculated using a social rank optimizer, which finds trust levels by monitoring communication behaviors. The social rank optimizer is used to determine if a node's behavior is legitimate or malicious by evaluating its trust value m. Furthermore, the suggested m is validated against different security criteria such as message modification, DoS, and DDoS attacks.

TABLE 4. A comparative summary of the BC-based IDMS solutions of academic literature, incorporated into the cloud computing domain (decentralized: DT, not mentioned: -).

Ref.	Contribution	Type of Network	Approach	Scope	Blockchain	Strengths	Limitations
[2]	Scheme	Consortium	-	Identity management	-	Ensures that signatures cannot be forged, the anonymity of nodes participating in the transaction, and forward security via a security proof and efficiency analysis.	Reliant on the master node. Every participating block needs to confirm the authenticity of creating the identity of the master node in each transaction, causing system overhead. Prioritizes the cloud service provider, ignoring the privacy of the users.
[6]	Framework	Public	DT	Trust model	Hyperledger Fabric	The trust parameter in the model can dynamically change according to the behavior of the associated entities. The proposed design performs a cross-domain validation.	Provides a framework only, and did not perform any implementation or testing. The scalability of the framework is not discussed.
[112]	Framework	-	DT	Access control	EOS	Provides availability, integrity, accountability, confidentiality, and authenticity to the users. Provides efficient access control with lower transaction costs.	Lack of determinism or algorithmic enforcement of the consensus mechanism. The network is vulnerable to attacks in which the network may be flooded with counterfeit transactions that are connected with previous valid transactions.
[116]	Protocol	Public	DT	Identity management	Ethereum	Reduced cost and time compared to the consolidated IDMS. Do not rely on the IDMS server or User.	Tested upon only one protocol, consolidated IDMS. Mining in Ethereum is a time-consuming operation, this slows down the process of user login setup.
[117]	Scheme	Consortium	DT	Identity management	Hyperledger Fabric	Simple architecture with only one channel and one Hyperledger fabric endorser.	Do not specify the exact security types and issues the architecture resolves.
[118]	Framework	Private	-	Identity management, Authenticati on	Quorum	Custom smart contracts are constructed for a specific type of user that provides privacy and trust.	Do not address the scalability component and procedure to defend against cyber-attacks.
[119]	Framework	-	DT	Identity management	-	Less computing complexity.	Does not provide any technical details and scalability remains a matter of concern.
[120]	Framework	-	-	Identity management	FISCO-BCOS	Lower delay in initialization and update stages.	Certificate revocation delay is higher than traditional public key infrastructure.

Bourus et al. [18] design a lightweight design and accompanying protocols for the management of identity using consortium blockchain and try to address concerns about privacy, reliability, and scalability in a centralized IoT system. The method solves privacy and security concerns associated with traditional centralized systems and emphasizes the notion of delegating identification system power to a set of organizations.

Hammi et al. [121] devise BC-based virtual zones, named bubbles of trust, where devices can communicate securely in a distributed environment. The proposed approach applies to a wide variety of IoT contexts, applications, and settings. It is built on top of a public blockchain and benefits from its security features.

Chen et al. [122] propose a user-centric IoT-based IDMS framework that is based on a global identity provider responsible for the maintenance of the global identity space. Various SPs create a local identity consistent with the global identity and maintain a consistent perspective of the global identity. As a result, each local identity may have its credential and means of authentication. For instance, a user may use fingerprint authentication to unlock his smartphone while using

facial recognition authentication to access his company's access control system.

Omar and Basir [123] provide a semi-decentralized IDMS solution for the IoT based on blockchain and smart contract technologies. This framework maintains a compromise between simplicity of implementation and decentralized architecture. The framework emphasizes three essential principles: user identity as a living asset, identity as a unique and global, and third-party authority minimization.

Yang et al. [124] propose a BC-based lightweight authentication mechanism for IoT by employing the modular square root cryptographic approach to ensure the security and efficiency of the authentication process. At the same time, blockchain technology is utilized to increase security and ensure the system's scalability. Security analysis regarding different attack resistance is also carried out. In a similar work, Shi et al. [125] employ a lightweight symmetric encryption algorithm to preserve privacy for distributed IoT setups.

Lansky et al. [126] formulate a lightweight authentication system based on Elliptic Curve Cryptography (ECC) named BCmECC. It depends on a public blockchain to confirm the users' public key and provides the needed security. They evaluate the suggested system's security level using the BAN logic and the Scyther tool [127]. Table 5 presents a comparative summary of the academic BC-based IMDS solutions integrated into the field of IoT.

C. WIRELESS SENSOR NETWORKS (WSN)

Due to the advancements in wireless communication technology, users are willing to receive more integrated and efficient wireless mobile network services. Identity management and access authentication are essential components of mobile network security because they prevent users from unlawfully accessing or attacking the network. However, there are several flaws in the current service-centric wireless mobile network design regarding user identification and the authentication process [40]. Numerous researchers have proposed secure BC-based IDMS solutions in literature in the WSN domain. We review some notable ones below.

Cui et al. [19] present a BC-based distributed multi-WSN scheme for authentication in IoT. Each IoT node is separated into base stations, ordinary stations, and cluster heads based on their capabilities and energy. To authenticate the cluster heads, they have adopted the global blockchain scheme, and for ordinary nodes, a local blockchain scheme was adopted. The base station initializes the security parameters like the hash of the ethernet address, generating IDs for station, cluster, and ordinary nodes, and generating private-public key pairs for all the nodes within a network. The nodes' identity credentials are registered and stored in a public/global blockchain using smart contracts. After that, the authentication requests from the nodes are validated using the suggested framework.

Xu et al. [40] propose an SSI management scheme for wireless mobile networks. They suggested a BC-based IDMS in which customers have sovereignty over their individuality. A specific user can generate his SSI and keys. For authentication, the SSI and private keys are utilized. Blockchain is used to keep the SSI and public keys. Furthermore, a hash function is utilized to identify false users, and any phony user identity that is already stored in the blockchain is erased. Because the data is kept in the blockchain network, any service provider may access it for authentication reasons. Their suggested system is divided into five phases: preliminary, consensus, verification, cancellation, and imbursement. The authors state that their method has decreased communication overhead.

Yang et al. [128] present an enhanced multi-domain authentication framework for the intelligent transportation system that incorporates all the authorities for necessary supervision and a comprehensive vehicular identity management process among the authorities at the management layer. The authors suggest an extension of the generation of a two-phase pseudonym and distribution process based on an enhanced key derivation technique that significantly increases the performance of privacy-preserving authentication. To accommodate the low-latency requirement of vehicular ad-hoc networks, the authors suggest a batch revocation technique based on the blockchain's cross-domain information and pseudonym distribution record.

Xu et al. [129] designed a blockchain-enabled radio access network (RAN) as a new decentralized RAN architecture that enables increased security and privacy in the identification and verification processes. It is a comprehensive strategy for adapting the traditional RAN to a decentralized focus facilitated by an innovative IDMS solution.

Raju et al. [130] present a privacy-aware BC-based IDMS solution for cognitive cellular networks. In their system, cellular networks and cellular nodes act as the participating nodes. In this system, users' personally identifiable information, which is required for user claims, is protected from unauthorized access through the use of shared secrets. Data exposure is minimized using a partitioned blockchain data storage system, which contains only the pseudonymous identity of a subscriber that is required for access provisioning. In Table 6, we present a comparative summary of the academic BC-based IMDS solutions integrated into the field of WSN.

D. ELECTRONIC MEDICAL HEALTHCARE (EMH)

Apparently, paper-based medical records are inconvenient for information exchange and sharing. Electronic health records technology [131], [132] enables a unique method of collecting and managing health-related data. However, standard management of electronic medical healthcare (EMH) records have several flaws. To begin, medical data is often held separately in different hospitals or research organizations, each with its database. As a result, when a patient goes from one hospital to another, he or she must undergo medical examinations again, adding to the patient's inconvenience. Second, only authorities, such as hospitals, have access to electronic health record systems data. Thus, if a dispute arises between

TABLE 5. A comparative summary of the BC-based IDMS solutions of academic literature, incorporated into the IoT domain (decentralized: DT, not mentioned: -).

Ref.	Contribution	Type of Network	Approach	Scope	Blockchain	Strengths	Limitations
[9]	Scheme	Private, Public	DT	Trust model, Privacy-preserving	Ethereum, Ripple	The system uses IoT-based multi-cloud solutions to effectively safeguard the confidentiality and security of patients' data.	Claimed scalability in terms of growing IoT infrastructure without sufficient proof or discussion.
[16]	Framework	Public	-	Trust model	Ethereum	Privacy and security issues are effectively handled by computing each entity's trust and storing it in a blockchain.	The encryption and decryption of content at each node may lead to an increase in the computational and communicational overhead. Double verification process with key management and storage overhead further leads to complex computational issues.
[18]	Scheme	Consortium	-	Identity management	Hyperledger Fabric	By splitting functions into several ledgers query time was shortened compared to invocation time.	Not tested with a large number of sensors; thus, scalability remains a concern. The system has high transaction costs.
[121]	Scheme	Public	DT	Trust model, Authentication	Ethereum	Provides a virtually secure zone where devices can communicate. The system is tested against a good number of attacks.	There is no initialization phase in the system and the system is not adapted to real-time applications.
[122]	Framework	-	-	Identity management, Authentication	-	Provides a multi-channel authentication model that tries to prevent the trojan virus and man-in-the-middle attacks.	Does not address the technical details about how the service channel is separated from the authentication channel.
[123]	Framework	Public	DT	Identity management	Ethereum	Changes in ownership do affect the proposed system's device security updates.	No mention of scalability or the restrictions imposed by transaction processing delay.
[126]	Protocol	Public	-	Authentication	Ethereum	Computation and communication cost is reduced with a robust evaluation of the security of the model.	The system does not explain how a user achieves full anonymity.
[124]	Framework	Public	-	Authentication	Ethereum, Hyperledger Fabric	Secure and lightweight.	Higher communication cost.
[125]	Scheme	Private	DT	Access control, Privacy-preserving	Ethereum	Utilize the wallet address in the blockchain as a user's identity.	Higher computation overhead.

the hospital and the patient, the hospital will always prevail, as it has the ability to alter or even destroy the patient's medical data. It is unjust to patients [13]. Blockchain's decentralized architecture makes it a perfect candidate for user identity and access management of patients in the medical healthcare sector. Several researchers have proposed secure BC-based IDMS solutions in academic literature in the medical healthcare domain. Some of them are reviewed below.

In [12], identity registration is carried out by Azaria et al. via the registrar smart contract. It uses public-key cryptography for the translation of valid string-based identity information to a unique Ethereum address. It can use a DNS-like solution to facilitate the integration of existing forms of identification. Four software components are introduced: a backend library, an Ethereum client, a database gatekeeper, and an electronic medical health record manager. These can be run on servers in conjunction with one another to form a cohesive, distributed system.

Combining multiple authorities into different levels, Tang et al. [13] propose an efficient authentication scheme for electronic health records using blockchain. It is an identity-based signature system with several authorities and efficient signing and verification algorithms. The proposed system can withstand collision attacks by demonstrating its efficacy in the random oracle model using the computational Diffie-Hellman premise.

TABLE 6. A comparative summary of the BC-based IDMS solutions of academic literature, incorporated into the WSN domain (decentralized: DT, not mentioned: -).

Ref.	Contribution	Type of Network	Approach	Scope	Blockchain	Strengths	Limitations
[19]	Scheme	Public, Private	-	Authentication	Hybrid	The security of the scheme is tested against various attacks. Reduces computational complexity, energy intake, and storage allocation.	Consensus procedures and mining-based attacks are not considered.
[40]	Scheme	Public	SSI	Identity management, Authentication	Bitcoin	Dynamic revocation is possible for illegal users.	No specification about how the cryptocurrency is being used in the payment phase.
[128]	Scheme	Consortium	-	Authentication, Privacy preserving	Hyperledger Fabric	Presents a parallel BC-based authentication scheme for establishing trust across several administrative domains. Mitigates the disadvantages associated with a single administrative domain.	Suffers from computation, storage, communication, and cross-domain information synchronization overhead.
[129]	Scheme	Public, Private	DT	Identity management, Privacy preserving	Blockchain Agnostic	Architecture is tested in multiple use cases such as switching, routing, quality of service, and service billing.	Do not provide concrete proof of the immutability or unforgeability stated in the proposed system.
[130]	Scheme	Private	DT	Identity management	Ethereum	Reduces signaling traffic and increases access provision time by partitioning the blockchain.	The scheme does not address issues regarding deployment, scalability, and security threats.

Mikula et al. [14] propose a healthcare-related use case study and demonstrate the effectiveness of blockchain in secure identity and access management for physicians in Denmark. The prototype consists of a client-side application, an application server, a database, and a server for authentication and authorization. The Application interacts with the application server, which verifies users using information saved in the database. The prototype is based on a Hyperledger fabric framework and records minimum computation and storage costs.

Xiang et al. [15] suggest a biometric-based blockchain network to verify a patient's identification in an electronic health care system. Their idea's objective is to deliver low latency real-time service while patient verification is required. Confidential medical records are maintained on a legal blockchain network, which ensures data privacy. The system is divided into five phases: the starting phase, the enrollment phase, the login phase, the mutual authentication phase, and the password update phase. To demonstrate its resilience, the system is tested against typical security threats such as man-in-the-middle, and replay attacks.

An Ethereum consortium BC-based IDMS named Health-ID for remote healthcare is presented by Javed et al. [4]. This Health-ID architecture has four entities: user, healthcare regulator, blockchain, and cloud. By using web tokens for identity attributes, the owner can govern their own identity. After executing identity verification, healthcare regulators provide their attestation. The design utilizes two distinct smart contracts to tokenize the identification of the network's entities and the end-users so that a unique health ID identifies each entity.

Xia et al. [133] propose a secure and scalable access control mechanism for sensitive information sharing of health data. They utilize secure cryptographic techniques and digital signatures to enable effective access control to sensitive shared data via a permissioned blockchain and design a constantly monitored system. After their identities and cryptographic keys are authenticated, data owners can access electronic medical health records stored in a common repository. After authentication and service, the requests become part of a closed, and permissioned blockchain.

Zyskind et al. [134] propose a BC-based off-chain information management system that can be utilized as a trustworthy data storage and processing platform by integrating blockchain with off-chain storage. Data is stored off-chain in a centralized key-value database in this system; it is a hybrid of distributed hash tables proposed by Maymounkov and Mazieres [135], and LevelDB's [136] key-value storage. Data is accessed through the DL. DL-based transactions are classified into (1) access management for authentication purposes and (2) data storage/retrieval inquiries.

Hussein et al. [137] devise a scheme that utilizes a revised encryption method for implementing the cryptographic hash generator. It produces a novel key design from MD5 strings. This updated approach uses the Discrete Wavelet Transform (DWT) to improve the security level of the encryption

process. The system can be effectively used in various working contexts, such as clinics, hospitals, and healthcare facilities, to convey sensitive data. Sharma et al. [138] propose a layered smart contract-based scheme for managing access control in the healthcare system. They used ZKPs as an authentication method in the system, for rapid and secure distribution of access to electronic health records while maintaining privacy. To address the constraints of proxy re-encryption, which serves as an access control mechanism for medical data, a hybrid encryption model with both symmetric and asymmetric encryption is utilized. In Table 7, we present a comparative summary of the academic BC-based IMDS solutions integrated into the field of the electronic medical healthcare sector.

E. GENERIC BC-BASED IDMS SOLUTIONS

Apart from the discussed IDMS solutions in the aforementioned domains, many researchers have proposed several BC-based IDMSs. Some notable ones are reviewed in this section.

Ren et al. [139] suggest a BC-based IDMS that entails providing certificates to ensure authenticity. The system includes a space-efficient data structure to protect an identity's integrity. They also create a lightweight protocol that ensures public key exchange between two parties and requires fewer processing resources. The entire system is backed by self-sovereign identification, with valid users identified through smart contracts.

Mell et al. [140] develop a smart contract-based IDMS on the blockchain. The system operates without the assistance of a third-party credential service provider. Authentication is enforced by communication parties using agreed-upon methods. Key point is that no public key-generating service is required to support it, which saves money and allows for less overhead during processing. A hierarchical identification system is also designed to verify various aspects of the service provider and service user.

To offer security against a typical security threat, Kassem et al. [141] suggest DNS-IDM, a decentralized IDMS. They also addressed the constraints of the traditional decentralized management system and claimed to have solved some of those shortcomings in their new method. Although the system via which people can interact defines privacy standards. Any damaging efforts by outsider attackers will be sent through a specialized program known as DNS-IDS. Because this program checks the credentials, the attacker is unable to contact the user. All valid credentials are kept in a distributed database that is accessible via a BC network. As a result, only legitimate queries may travel through the DNS-IDS app and reach the intended people. Because the credential database is separated in a remote location, the DNS-IDS app is decentralized. Lin et al. [142] propose a BC-based authentication approach that provides digital identification to every system member. Their approach uses directed graph search. Each node in the graph produces a signature that may be used to identify the node uniquely. A hash function is used to validate the signature of each individual node in the authentication system. If two nodes are not connected, they cannot interact until the signature is confirmed. Scalability is improved by the ability to add or remove any number of nodes. Hamer et al. [143] propose a self-sovereign-based IDMS that uses fingerprints to verify user identity. The system additionally protects users' privacy by employing the World Wide Web Consortium (W3C) validator. W3C is an international blockchain community whose members are in charge of establishing a blockchain security standard. In this system, all users must register using a mobile application rather than any other kind of identity other than their fingerprint. Their technique is capable of handling many systems and allows for scaling without the assistance of any authority. The proposed method necessitates the employment of a trustworthy organization to supply the public key to consumers and SPs.

For user authentication, Lee et al. [144] suggest a BIDaaS, a BC-based identification service. The solution is intended for mobile users and is appropriate for businesses that have mobile communication infrastructure. It includes three entities: the BIDaaS provider, the partner, and the user. Users must register with a BIDaaS provider, but the service provider does not need to register. The service provider has access to the private blockchain, which is managed only by the BIDaaS provider. On the other hand, service providers cannot write anything in the private blockchain; however, they can request more resources in addition to the virtual ID. Asamoah et al. [145] design a BC-based IDMS for smart city operations. The goal behind their design is to offer the identification of every smart component of the city through a BC-based network. The system gathers the qualities of a city's people and distributes them to other method modules for authentication reasons. A well-secured id creation method will assign a user id to each resident.

ZKP is a feasible technique for achieving SSI. The system presented by Borse et al. [146] allows users to achieve selective anonymity for specific user identification elements. The membership ZKP is linked to the Pedersen commitment [147] in this system. ZKP is utilized to create a secure SSI system by keeping user characteristics hidden from the public ledger.

Keeping the user attributes private and secure is one of the core functionalities of blockchain. Keeping that in mind, Singh et al. [148] present a credential protocol for preserving user privacy. The provided scheme ensures user unlikability, untraceability, and unforgeability. The scheme is based on cryptographic techniques that use pairings, short signatures, commitment, and ZKP. The scheme also provides a real-world use case for the proposed scheme's deployment. Leveraging zero-knowledge succinct non-interactive argument of knowledge, Lee et al. [149] propose a self-sovereign IDMS that focuses on preserving user privacy. Here, a user requests that an authorized agent verify the user's identification and issue a certificate based on that identity. The commitment, together with its certificate, is stored in the blockchain. The blockchain commitment is used to establish whether the

TABLE 7. A comparative summary of the BC-based IDMS of academic literature, incorporated into the EMH domain (decentralized: DT, not mentioned: -).

Ref.	Contribution	Type of Network	Approach	Scope	Blockchain	Strengths	Limitations
[4]	Scheme	Consortium	DT	Identity management, Privacy-preserving	Ethereum	Provides higher throughput compared to the public blockchain.	The scheme does not address security threats.
[12]	Framework	Public	DT	Access control	Ethereum	Supports user anonymity, and security, and deals with single-point failure issues by relying on several participating entities at the same time.	The system is not implemented and the key distribution policy is not discussed in detail.
[13]	Scheme	Consortium	-	Authentication	-	Robust authentication scheme with multiple authorities resisting collusion attacks.	The effectiveness of the system is only compared with two other works. Technical details are less discussed.
[14]	Framework	Public	DT	Identity management, Access control	Hyperledger Fabric	Fast computation setup and lower storage cost.	Experiments were limited to only the computer's local memory resources arising the question of scalability.
[15]	Scheme	Private	-	Identity management, Authentication	Distributed ledger	The security of the scheme is tested against various attacks. Data is managed efficiently.	Assumes that initially no key update is required for the key generating server. In any type of failure, the server needs to be updated dynamically.
[133]	Framework	Private	DT	Access control	-	Lightweight and uses identity-based authentication in order to achieve users' trust and membership.	Do not perform any experimental study. Do not investigate the communication and verification protocols and algorithms between participating entities.
[134]	Scheme	Public	DT	Identity management, Access control	Bitcoin	Data are stored in off-chain storage. Storage consumption is reduced.	Uses symmetric cryptography; thus, there is always a chance of the risk of key theft of the users. Overly reliant on the security provided by the internal blockchain and do not deal with malicious services.
[137]	Scheme	Private	-	Access control	-	Medical record sharing and access control using a revised cryptographic hash generator that generates the necessary user security key.	Do not mention the blockchain type and storage capacity are not addressed along with the proper scalability of the architecture.
[138]	Scheme	Public	-	Access control	Ethereum	Satisfies the non-repudiation condition of a blockchain as the proxy server always saves a copy of the encrypted symmetric key every time a transaction is requested and logs every event.	Do not provide any proof of immutability or integrity of the proposed system.

user's private information meets a specific condition, resulting in proof.

Yang and Li [150] propose smart contracts and a zero knowledge-based IDMS consisting of three entities: Identity and Service Provider, and User. Four procedures are adopted in their scheme: creation, transferring, responding, and revocation consisting of five steps: authorization, validation, response, challenge, and assertion, completing the challenge-response protocol's full cycle. They have also implemented behavior privacy and data minimization. Incorporating ZKP and face-to-face proofing validated in a bitcoin blockchain, Augot et al. [151] propose an architecture that brings flexibility to identity management in the blockchain. The system uses Merkle trees to group the commitments that minimize the transaction costs and save bandwidth. The system enables a verifier to efficiently update or cancel a user's identification.

As a possible solution to the loss of trust in conventional institutions and third parties, blockchain has risen

and allows itself to function as a trust-free economic unit. Gruner et al. [76] propose a computable trust model for BC-based IDMS. Trust is applied to digital ID in a decentralized manner. The computable trust scores enable granular decisions regarding the trust of service providers. They have modeled their scheme in a directed graph format, where vertices comprise digital ids, claims, and proofs. The edges represent the association between the attributes comprising vertices.

Biometric system is another way of authentication that has garnered interest. Leveraging biometric authentication and trustable authority, Gao et al. [152] present a smartphone device operable digital IDMS using blockchain supply chain management. The digital identity generator verifies the government Id and photos of that individual during the digital ID binding to the smartphone.

Odelu [153] presents a BC-based key management mechanism for authenticating the user using personal biometrics. The system consists of three majors namely, User, Registration Center, and Authentication Server. They analyze various security measures and test the method against security attacks like replay and man in the middle.

Sarier [77] proposes a novel BC-based non-transferable digital credential system for smart industrial applications. The system is designed by modifying the typical industrial IoT identity management lifecycle to work with blockchain. It efficiently enables non-transferability, controlled disclosure, cross-unlikability, and auditing. The non-transferability is provided by a newly computed hidden biometric property, which is produced after each authentication using a secure fuzzy extractor. The privacy of the user is protected by an effective authentication system. The new method allows for the suspension of credentials as well as their permanent revocation via the publication of a credential revocation list on the blockchain. Auditing on the blockchain is achieved by checking the credential revocation list, Merkle tree root commitments, or, additionally, proofs for the proper deletion of user credentials.

Relying on local processing, Hammudoglu et al. [154], propose a biometric authentication-based SSI system named Portable Trust. This architecture is meant to be fully local and autonomous and does not require any cloud service, server, or authorized access to the hardware of fingerprint readers. However, the size of the local storage confines the scalability of the system.

Fan et al. [155] present a BC-based identity security authentication system in a separate work. The approach aims to achieve fault tolerance while also increasing the hardness of compromising half of the network's nodes. The system's security was evaluated by suspending and resuming node work to simulate hacker attempts. As a result of issuing a valid certificate based on the public key, the blockchain may accurately authenticate the user identity information associated with the input public key and prevent the user with unauthenticated identity information from accessing the digital certificate.

Ao et al. [156] propose an identity authentication scheme by combining blockchain with identity-based cryptography (IBC). They have deployed smart contracts in the Ethereum blockchain to generate a decentralized private key generator. For the authentication, they have used the identity-based cryptography method along with a challenge-response protocol. The scheme deals with replay, and man-in-the-middle attack evades the complex certificate management with lesser complexity. Al-Bassam [157] provides an example of the claim identification model SCPKI using smart contracts to execute the concept of the Trust Web. Any entity might function as a registrar to sign or cancel other people's characteristics. The SCPKI makes it easy to detect fraudulent certificates when they are issued, but a globally transparent claim model will jeopardize identity privacy.

An SSI model named vault-point is proposed by Hong and Kim [158]. It complies with the OAuth 2.0 framework [159] that provides scalability and feasibility to the service providers following the OAuth 2.0 standard for authentication and authorization processes. The architecture of OAuth2.0 is demonstrated in Figure 12. OAuth 2.0 defines four roles: i. Resource Owner (end-user), which is an entity that has the ability to provide access to a restricted resource, ii. The resource server and the protected resources are hosted on this server. Before serving protected resources to the application, the resource server requires some form of authorization, iii. Client, on behalf of the resource owner, an application generally operating on a mobile device or a conventional web application requests access to a protected resource, and iv. the authorization server, which follows the OAuth 2.0 protocol, checks the user's identity before issuing access tokens to the application.

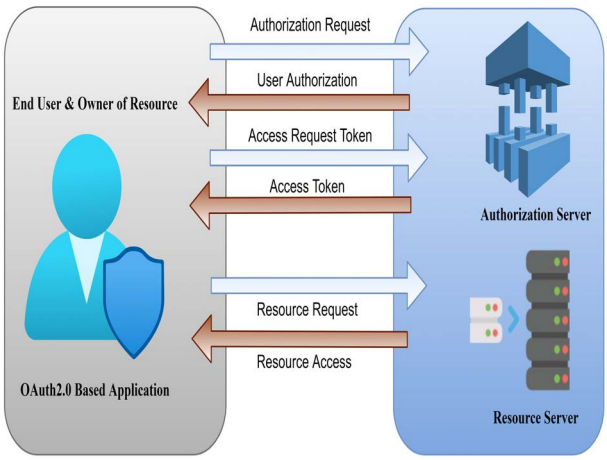

FIGURE 12. The architecture of OAuth 2.0 Protocol.

Faber et al. [160] propose a conceptual identity and authentication architecture using blockchain that focuses on transferring the control of user's data to the end-users providing trust, transparency, security, and control. Their human-centric approach incorporates the European Union's new General Data Protection Regulation in the design.

Friebe et al. [161] propose a framework named decent-ID. It incorporates smart contracts for decentralized user identity storage. The system combines the Ethereum blockchain with a distributed hash table that provides integrity and security. The privacy of user identification data is assured because no instance can access a user's data without explicit authorization.

Gao et al. [162] propose a three-phase (initialization, registration, authentication) BC-based privacy-preserving scheme. They analyze how a user independently creates identification information and performs the registration of identity certification through the blockchain.

Zhou and Zhao present EverSSDI [163], which uses Ethereum to execute complex smart contracts, and an interplanetary file system to store users' digital information. The system performs authentication, authorization, and quick recovery of SSI through smart contracts. The smart contract contains digital data only, while the actual information is encrypted and saved on the terminal in the file system, preserving the blockchain space and reducing the transaction cost.

Zhou et al. [164] propose a key distribution protocol named BIBE to integrate identity-based encryption with blockchain. Their total authentication technique involves two steps: BIBE key issuing and mutual identity verification. To begin, each party obtains its private key from the key generation center. Second, the key pairs perform mutual identity verification of the nodes and build a secure communication channel. As a result, data can be securely transmitted on both sides of the link.

A prototype designed by Stockburger et al. [56] investigates how a BC decentralized IDMS can use the SSI architecture to deliver high levels of security and transparency to all stakeholders participating in public transportation ecosystems. The suggested solution eliminates the need for numerous travel cards (one for each mode of transportation). It gives people more choice over their identities when using interoperable ticketing systems across Europe.

The KYC procedure verifies the identification of a user and assesses the possible implications of illicit intention to a business [88]. KYC processes are resource-intensive, slow, and intricate. To tackle this problem, Soltani et al. [165] propose a KYC2 framework. KYC2 offers an identity management framework in which the identification traits of banking clients are kept on their mobile devices. Once a client's identity has been satisfactorily validated, banks participating in the KYC2 ecosystem can issue verifiable credentials to them.

Zhong et al. [166] propose an authentication and authorization protocol for a smart power grid system using a consortium blockchain. The system addresses the common security threats to the BC authentication system for smart grid networks by analyzing various threat models. Kaaniche and Laurent [167] present a new BC-based infrastructure for auditing data usage that protects users' privacy while maintaining continuing data availability. The authors employ a hierarchical ID-based cryptography approach. A central master authority distributes the process of generating public/private keys to the many participating entities using legitimate ID-based public elements.

Abbasi et al. [168] propose a concept of BC-based IDMS named VeidBlock in the domain of software-defined networks. It is used for anonymous authentication and helps security protocols retain their security and privacy. They formed a small experimental setup and deployed all components using docker and observed that the component initially takes more time during the pre-execution process because it creates key pairs, sends certificate requests, processes certificate responses, and performs initial authentication. For runtime authentication, the component requires very little time. The requester process consumes less computing power since it simply sends the first message to the authenticator. The remainder of the computer power is used by the component requesting authentication.

In addition to academic research, Chari et al. [169] patent a design scheme to provide the essential BC-based IDMS. This design is based on the asset owners' collaborative support to provide security and ZKP features. In this system, one communicating party can ensure authenticity to another party by following a particular protocol where both parties do not need to share any extra information. The only fact is here that two parities know by whom they are communicating. Madisetti and Bahga [170] patent their design that focuses on the interoperability of the blockchain architecture regarding identity and access management. Hyun et al. [171] designed a BC-based secure identity authentication system. Ebrahimi [172] patents a BC-based design that demonstrates secure IDMS by certifying transactions among communicating devices. This approach allows devices to transfer relevant public-key and digital signatures. Through this, the device could obtain data from communicating devices. Table 8 presents a comparative summary of some notable generic academic BC-based IMDS solutions.

V. ESSENTIAL COMPONENTS OF A DIGITAL IDMS ON BLOCKCHAIN

To evaluate and protect the BC-based IDMS, we have identified five essential components: privacy, integrity, authentication, trust, and simplicity. Note that these five components are closely connected and sometimes it is difficult to distinguish them. However, dividing the BC-based IDMS into different essential components helps us to organize the contents we have provided here. Several academic studies have suggested many essential components of BC-based IDMS solutions. We have fine-grained those discussed components and outline five essential components of BC-based IDMS solutions to achieve self-sovereign identity, and categorize each of the reviewed articles based on their addressing of the outlined components and sub-components of this paper. As shown in Figure 13, the five essential components are authentication, integrity, privacy, trust, and simplicity. In this section, we discuss each of the mentioned components along with

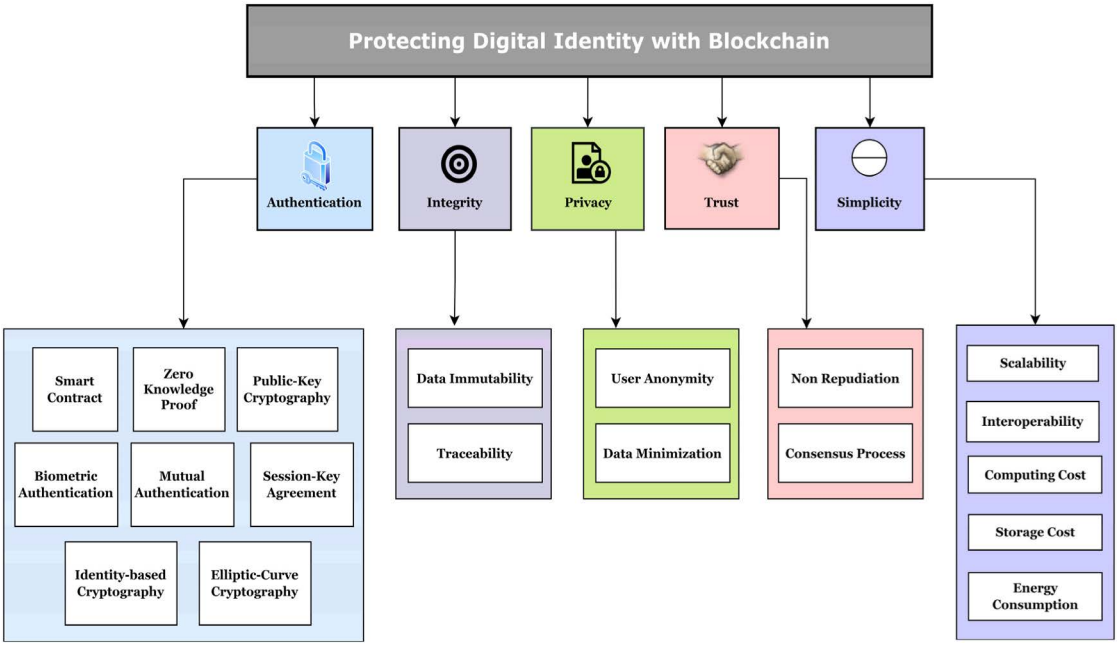

FIGURE 13. Five essential components and their corresponding sub-components of a BC-based digital IDMS.

their corresponding sub-components that can ensure a secure and robust BC-based IDMS solution.

A. AUTHENTICATION

Authentication is how a service provider verifies a user's identity before allowing access to the services. Based on the credentials supplied during registration, the provider allows the user to utilize the services. One of the major features of blockchain is that it can be used as a provider of authentication. Blockchain performs authentication through smart contracts that are designed and implemented on the blockchain. The smart contract generator can be configured via the smart contract authentication layer to initiate and then deploy on top of the blockchain framework every time verification is needed [13]. There are many reasons why blockchain will be pivotal in digital identity authentication. Mainly because it has no central authority, which allows us to store and handle data without any centralized governance. Some of the authentication components of a digital BC-based IDMS are discussed below. In the following, we discuss some of the commonly used authentication components in developing BC-based IMDS.

1) SMART CONTRACTS

Smart Contracts (SCs) represent electronic contracts that allow multiple anonymous parties to engage in an arrangement. SCs are tamper-proof computer programs that are hosted and implemented on a BC-based network when certain predefined conditions are met. The basic idea of SCs is visually presented in Figure 14. SCs are not controlled by any central authority. When used in multi-party digital agreements, SCs can reduce adversarial risk, boost efficiency, minimize costs, and add new levels of transparency to operations. The agreements make it easier to exchange currency, assets, resources, or any commodity, and this is how transactions are open, permanent, and identifiable. Solidity [173], a high-level programming language, enables smart contracts that run on the Ethereum virtual machine. Some of the significant SCs supported by blockchain systems are Ethereum [174], Solana, Cardano, and IBM's Hyperledger Fabric [46].

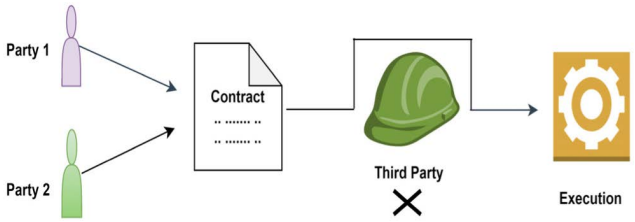

FIGURE 14. Smart contracts between two parties without any third-party involvement.

2) ZERO-KNOWLEDGE PROOFS (ZKPS)

Cryptography is one of the essential aspects of blockchain technology. ZKP is a method of authentication and can be defined as an interactive proof in cryptography. It is a mathematical procedure for ensuring the validity of the data without revealing the data itself. This permits a user to prove that their specifics satisfy definite requirements without exposing the actual user details. As shown in Figure 15, the ZKP framework's implementation is split into three phases. A prover (one party) can prove to a verifier (another party) that a statement about some secrete information is valid

TABLE 8. A comparative summary of some of the notable generic BC-based IDMS solutions of academic literature (decentralized: DT, not mentioned: -).

Ref.	Contribution	Type of Network	Approach	Scope	Blockchain	Strengths	Limitations
[56]	Framework	Public	SSI	Identity management	Hyperledger Indy	Removes the need for numerous travel cards and interoperable ticketing systems. Provide users more control.	Do not conduct a detailed stakeholder analysis even though various stakeholders are included in the study.
[76]	Framework	-	SSI	Identity management, Trust model	-	Automates the digital identity trustworthiness logic and claims.	The initialization of the trust score is based on some pre-trusted digital ids, which breaks the decentralization feature to some extent.
[77]	Scheme	Public	-	Identity management	Bitcoin	Replaces Merkle tree with accumulators that offer quick proofs, and batching techniques.	Employs a lower transaction per the second method.
[139]	Scheme	Public	-	Identity management, Access control	Ethereum	Provide a public certificate for authentication. Remote admin can maintain the system.	No protocol is mentioned by which the key will be exchanged.
[140]	Framework	Public	-	Identity management, Authentication	Ethereum	No need for a third-party authenticator. Supports user anonymity.	An organization must have key generator architecture, which is not feasible for small organizations.
[141]	Scheme	Public, Private	DT	Identity management	Ethereum	Provide privacy criteria. Facilitates user control over the privacy criteria.	A third-party application is used without mentioning any digital or security standards of the application.
[142]	Scheme	Private	-	Identity management, Authentication	Ethereum	Scalable. The security of the model is verified via standard security models.	One user can collect different node certificates which can be used misleadingly.
[143]	Framework	-	SSI	Identity management	-	Robust user verification through the W3C framework. Users have control over the application. Users can act as anonymous users.	Service providers use irreversibly transformed biometrics of a user, but the transformation process is obscured or not mentioned.
[144]	Framework	Private	-	Identity management, Authentication	-	Dedicated to the mobile communication network.	A third-party mobile app is used where no security standard is mentioned.
[145]	Framework	Private	-	Identity management, Authentication	Ethereum	The user is linked with all smart components via blockchain. Provides robust data integrity.	The author mentioned data will be managed efficiently but there is no support against their claim.
[146]	Scheme	Public	-	Identity management	Ethereum	Provides a low-cost SSI solution for the authentication system of banking services.	Do not deal with the integrity part of the shared data.
[148]	Protocol	Consortium	-	Access control	Hyperledger Fabric	Efficient in preserving user privacy with a lower computation cost.	Not tested on any public blockchain; thus, scalability remains a concern.
[149]	Scheme	Private, Public	SSI	Identity management, Privacy preserving	-	Provides faster verification and proofing time.	Do not address the consensus mechanism and user authentication clearly.
[150]	Framework	Public	-	Identity management	Ethereum	Secrete transfer of the possession of the attribute in minimal overhead. The verification process requires less calculation.	Too many privacy attributes with similar key-value pairs increase the complexity of the scheme.

TABLE 8. *(Continued.)* **A comparative summary of some of the notable generic BC-based IDMS solutions of academic literature (decentralized: DT, not mentioned: -).**

Ref.	Contribution	Type of Network	Approach	Scope	Blockchain	Strengths	Limitations
[151]	Scheme	Public	-	Authentication	Bitcoin	Offers lower transaction and bandwidth costs with improved and secure face-to-face identity proofing using smartphones validated against a blockchain.	The system faces poor scalability issues. Authentication is not properly discussed.
[152]	Framework	-	-	Identity management	-	Adjusts Government identity in a digital certificate by binding with biometric authentication in a smartphone.	Brings ambivalence about its actual implementation in the mobile communication world due to confidentiality and integrity issue.
[153]	Scheme	Consortium	-	Identity management, Authentication	-	Provides non-repudiation property. Lower computation cost.	The system's feasibility and scalability are not properly discussed.
[154]	Scheme	Public	-	Identity management, Authentication	-	Simple three-staged mobile-based biometric authentication solution for SSI.	Not scalable due to local storage of fingerprints and data. The experiment was performed with only 20 fingerprint samples.
[155]	Scheme	-	-	Identity management, Authentication	-	Performed multiple authentications and security tests to check the fault tolerance of the system.	No mention of the blockchain type or its data access property.
[156]	Scheme	Private	-	Authentication	Ethereum	Resolves the single-point failure issue. Uses identity-based cryptography instead of public-key cryptography, which improves the architecture's authentication process.	Large system overhead. Lower operational efficiency.
[157]	Scheme	-	-	Identity management	Ethereum	Provides a smart contract with the capability for running a public key infrastructure and IDMS.	Has privacy and adaptability issues. Do not provide any access control mechanism.
[158]	Scheme	-	SSI	Identity management	Ethereum	Provides interoperability and reliability. Functions well from the viewpoint of service providers through analyzing various security measures.	Needs three smart contracts to operate, thus increasing the cost. The energy consumption and computation, storage cost is not discussed.
[160]	Scheme	-	-	Identity management	-	Focuses on ensuring transparency of user's attributes.	The conceptual design does not provide sufficient specifications for an accurate implementation on a blockchain.
[161]	Scheme	Public	DT	Identity management, Privacy-preserving	Ethereum	Provides decentralized storage of user identities without any third-party involvement.	Necessitates the association of identities with a coherently centralized registration contract that brings the threat of external attacks.
[162]	Scheme	Consortium	-	Authentication, Privacy-preserving	-	User privacy-preserving scheme with a strong feature set.	Do not work in cross-blockchain mode.
[163]	Scheme	Public	SSI	Authentication, Access control	Ethereum	Provides a fine-grained authorization scheme of digital information using a hierarchical deterministic protocol that reduces cost.	Do not address any kind of security threats. Relies on the social network services authorization to recover lost SSI, which can also misbehave.

TABLE 8. *(Continued.)* **A comparative summary of some of the notable generic BC-based IDMS solutions of academic literature (decentralized: DT, not mentioned: -).**

Ref.	Contribution	Type of Network	Approach	Scope	Blockchain	Strengths	Limitations
[165]	Framework	Public	SSI	Identity management	Hyperledger Indy	Addresses the limitations of the KYC process and requirements of SSI.	Do not address any security issues and provides a theoretical assumption without solid implementation. To perform initial verification of the client, the system relies upon third-party sources, such as banks, and the government.
[166]	Protocol	Consortium	DT	Authentication, Access control	Hyperledger Fisco	Provides in-depth analysis of the various security issues of the proposed distributed authentication protocol for smart grid.	Relies heavily on the internal security properties of blockchain itself, and did not emphasize its security model through a feasibility study.
[167]	Scheme	Consortium	-	Access control, Privacy-preserving	Ethereum	Performs security analysis of the proposed system in detail.	Do not discuss mentioned public elements.
[168]	Scheme	Public	-	Authentication	Distributed Ledger	Preserves privacy in the verification stage by keeping the identity of the user anonymous.	Do not discuss the technical aspects of the architecture in a detailed way.
[169]	Patent	-	DT	Identity management	-	Provides an increased level of confidentiality.	Not specific to any domain.

without exposing anything other than the statement's credibility [175]. The prover computes proof that contains its statement in the Witness Phase. After that, the proof is sent to the verifier. During the Challenge Phase, the verifier poses a series of questions to the prover. The prover answers these questions in the Response Phase, which the verifier might use to approve or disapprove the generated proof [176]. A true ZKP must possess the following three fundamental properties:

- Completeness – It means that an authentic prover will be able to convince the verifier, given that the statement is accurate.
- Soundness – It means that no deceitful prover can prove the trustworthy verifier about the statement, except with some insignificant probability, given that the statement is fabricated.
- Zero-knowledge – It means that for an accurate statement, the verifier will not get any additional information other than the truthfulness of the statement.

3) PUBLIC KEY CRYPTOGRAPHY (PKC)

To encrypt and decrypt data, public and private PKC utilize keys. The keys are just big numbers that are coupled but asymmetric. The key can be shared with everybody. The private key is stored secretly in the key pair. If a message is encrypted with the private key, then it is decrypted with the public of the sender at the receiver side and vice versa. Blockchains make extensive use of asymmetric cryptography. In contrast to symmetric cryptography, which employs a shared key, asymmetric cryptography employs a pair of private-public keys. Typically, the public key correlates to the user's public address on the blockchain, enabling the user to sign a transaction with his private key so that every other node on the blockchain can validate its legitimacy. The critical public key infrastructure (PKI) manages public keys and verifies that users and their keys are correctly mapped. An asymmetric PKI system requires users to have access to a public key and recipients to have access to a private key in order to decrypt the information. In reality, there are two approaches to public key infrastructure authentication [177]. In a centralized approach, the certificate is managed by a hierarchically structured central certificate authority. On the other hand, in decentralized authentication, users can select other parties as trustworthy to sign their certificates. This social trust process is called the PGP web of trust (WoT). PKI is in charge of making online interactions safer by verifying the identification of network endpoints and encrypting data flow via the network's communication channels. It accomplishes this by encrypting and decrypting data using private and public keys, which are supported by digital certificates. PKI is based on digital certificates, which are generally issued by a certificate authority, which is a trusted third party. To maintain a safe authentication process, they have the authority to issue or revoke the certificate at any moment. This reliance

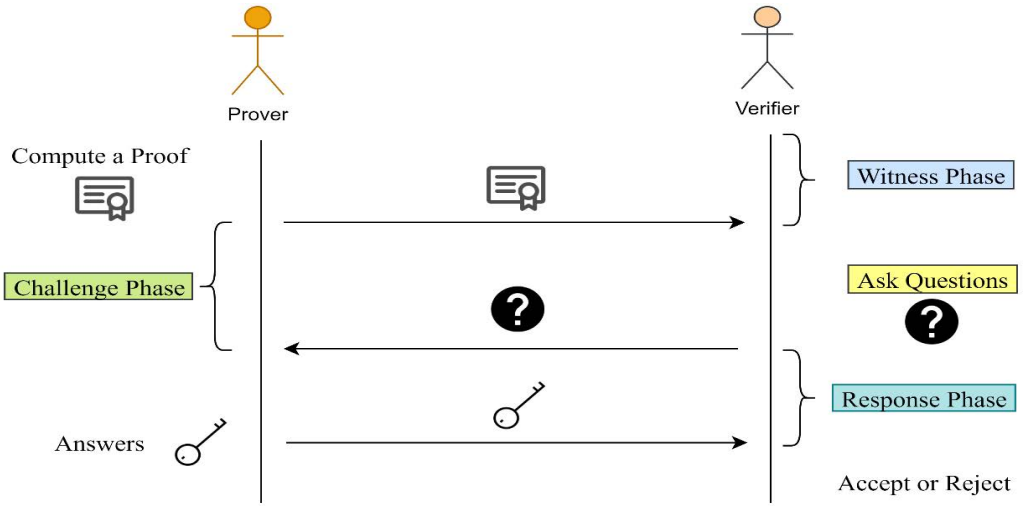

FIGURE 15. The framework of zero-knowledge proof [176].

on a single trusted party causes a slew of issues. The first is that the CAs are not subject to any kind of official oversight. Second, the CA systems are well-known targets for hackers because of their capacity to impersonate another user or a website. An attacker has access to all of the data intended for the recipient if a private key is compromised. Because blockchain operates on tens of thousands of machines at the same time, it eliminates the vulnerabilities associated with traditional PKI systems.

4) ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

ECC is a modern family of public-key cryptography systems. ECC is based on elliptic curve theory that enables the generation of cryptographic keys that are quicker, smaller, and more efficient. ECC cryptography is often seen as a natural modern successor to the RSA cryptosystem, as it requires fewer keys and signatures to achieve the same level of security as RSA and enables swift key generation, key agreement, and signatures. Several studies [9], [126], [163], [178] have adopted this scheme for the authentication of digital identity in their proposed BC-based IDMS.

5) BIOMETRIC AUTHENTICATION

Biometrics, including fingerprint, face, voice, and iris recognition, ensures that the person starting a transaction is who they say they are during the authorization stage. However, keeping biometric data information might be an issue because if the storage facility is penetrated, all biometric data is at risk. Most of today's secure biometric solutions for consumer devices are incorporated into sensors and protected using secure elements and trusted execution environment modules. When a live biometric sample is presented, access to a private key that may be used for authentication is granted by registering the public key attached to the biometric. It is then used to validate a signature based on a basic challenge-response authentication protocol [179].

6) MUTUAL AUTHENTICATION

Mutual authentication is a security procedure that requires both the client (principal A) and the server (principal B) to verify each other's identities before actual communication occurs. A connection may only be established in a mutual authentication procedure if both principal A and B interchange, authenticate, and trust each other's certificates.

7) SESSION KEY AGREEMENT BASED AUTHENTICATION

A session key is generated during authentication to encrypt/decrypt subsequent confidential messages sent between the user and the service provider after authentication [15]. Once the session key has been established between communicating parties, a secured communication channel is set up with mutual authentication protocol.

8) IDENTITY-BASED CRYPTOGRAPHY

Identity-Based Cryptography (IBC) was first proposed by Adi Shamir [180]. The most notable feature of IBC is that a user can establish a public key from a user's personal identity information, such as a phone number, and email address. An entrusted third-party server can derive the associated private key from the public key. Its advantage is that it eliminates the requirement for digital certificates that link public keys to the user's identity. In Table 9, we present a summary of all the reviewed articles applying smart contract, ZKP, PKC, IBC, biometric, mutual, and session key agreement-based authentication components. It is clearly shown that smart contracts and PKC are mostly used for authentication.

B. INTEGRITY

A user has to provide some identity attribute to the third-party during authentication. Public key cryptography can be used to protect the integrity of specific user attributes. It assures that a message is received in its original form without alteration. Even though the data is dispersed over

P2P networks, it is constantly validated and updated. Furthermore, the blockchain network has no single point of failure, making it impossible for adversaries to compromise the data set's integrity. Some of the integrity components of a digital BC-based IDMS are discussed below.

TABLE 9. A comparative summary of the authentication components in the existing literature.

Authentication	Addressed Literature
Smart Contract	[4], [9], [14], [15], [19], [20], [40], [112], [116], [119], [120], [123], [124], [130], [138]–[142], [146], [150], [155]–[158], [160]–[163], [166], [167], [169], [181], [182]
ZKP	[137], [138], [145], [146], [148]–[151], [169]
PKC	[4], [9], [13], [14], [20], [40], [116], [117], [129], [130], [133], [138], [144]–[146], [148]–[152], [155], [157], [158], [161]–[163], [165], [167], [168], [181]–[184]
Biometric	[15], [16], [77], [138], [143], [152]–[154], [184]
Mutual	[9], [15], [19], [20], [40], [121], [124], [129], [144], [164], [166], [182], [183]
Session Key Agreement	[15], [20], [40], [116], [124], [129], [139], [162], [183]
IBC	[164], [167], [185]
ECC	[9], [126], [134], [163], [178]

1) TRACEABILITY

Blockchain technology has emerged as a potential solution for implementing traceability by creating an information trail and providing data immutability and security. A timestamp is used in every transaction in a blockchain network. The order of each transaction may be monitored using this timestamp. It also protects the communication parties against replay attacks from outsiders [186]. Blockchain technology makes use of smart contracts to ensure the traceability of transactions. Some of the areas where the use of blockchain traceability in terms of IDMS can be utilized are supply-chain management, agriculture, food, and manufacturing [187], [188].

2) IMMUTABILITY

The immutability of blockchain is its greatest distinguishing feature. One of the primary values of blockchain technology is the ability to create immutable ledgers. Any centralized database is vulnerable to attack from adversaries, and they require assistance from a third party to keep the database secure. Every block carries a hash of the block before it. From the initial (genesis) block to the present block, a chain of blocks is created. Because all following blocks must be regenerated, it is computationally impractical to change information once it is in the chain.

In a blockchain network, when a transaction is completed, the data associated with that transaction is added to the data block. After the data has been added to the blockchain network's data block, it will not change anything. Before being put in the data block, all transactions are validated using the security policy. This mechanism facilitates protection against different types of security attacks [148]. In Table 10, we present a summary of all the reviewed articles addressing integrity components such as data immutability, and traceability.

TABLE 10. A comparative summary of the integrity components in the existing literature.

Integrity	Addressed Literature
Data Immutability	[2], [4], [9], [13]–[15], [19], [20], [117], [128], [137], [138], [142], [145], [148]–[153], [156]–[158], [160]–[162], [166], [169], [181], [189]
Traceability	[7], [9], [148], [190], [15], [16], [20], [112], [120], [128], [133], [141]

C. PRIVACY

Blockchain technology provides considerable privacy benefits as a distributed database, including data integrity, anonymity, traceability, manageability, transparency, portability, and network stability. Through anonymity, blockchain encryption paired with the digital signature offers ''Privacy by Design.'' The usage of private and public keys is a crucial component of privacy in the blockchain. It uses symmetric cryptography to protect transactions among users. Some of the privacy components of a digital BC-based IDMS are discussed below.

1) DATA MINIMIZATION

A data minimization option is one of the fundamental characteristics of the BC-based system. It refers to reducing data collection and utilization to the bare minimum required to complete the job at hand. The needed data types for the authentication of an organization vary depending on the organization's kinds [191]. The blockchain system aims to provide or support minimal usage of data for authentication purposes in IDMS solutions.

2) USER ANONYMITY

Anonymity provides the feature of hiding or masking the identity of a user. In a BC-based IMDS, when a user wants to make a transaction and other relevant tasks, it can be performed anonymously. On the blockchain, anonymity refers to whether or not a node's identity is publicly visible. Users are pseudonymous on public permission-less blockchains like Bitcoin [37] and Ethereum [174] because they hide their identity behind a pseudonym, the public wallet address. Users on private permissioned blockchains like Hyperledger Fabric [46] are generally familiar with one another. However, this anonymity property is only applicable when user authenticity is irrelevant to the communication party. In Table 11, we present a summary of all the reviewed articles addressing privacy components such as user anonymity, and data minimization.

TABLE 11. A comparative summary of the privacy components in the existing literature.

Privacy	Addressed Literature
User Anonymity	[2], [4], [9], [13]–[15], [20], [77], [112], [116], [117], [124], [128], [134], [137], [138], [140], [142], [143], [146], [148]–[153], [155], [156], [158], [160]–[163], [165], [168], [169], [178], [181], [183]
Data Minimization	[4], [9], [20], [137], [140], [141], [143], [145], [148]–[151], [153], [156], [158], [161], [162], [165], [167]

D. TRUST

Blockchain shifts trust from third-party organizations and individuals to trust in a secured and distributed technology. There is always a risk for each trustworthy partnership that one party can breach another party's security policy. Concerning IDMS, the assessment of digital records, statements, and certification requirements relies on the service provider's information or another dependent party's correctness and legitimacy. The service provider trusts the authenticity of a digital identity [76]. To answer the question "why identity management ties with blockchain*?*" blockchain identification allows for a substantial distinction between authentication agents' and authorizing agents' roles, thus deteriorating these agents' likelihood of interference with the subject.

Bitcoin, and blockchains in general, operate under the assumption that all nodes are equally untrustworthy and that their weight in the collaborative decision-making process is purely determined by their computational resources, commonly known as the proof of work consensus protocol [37]. Blockchain enables individuals to accumulate data on a cryptographically secured blockchain rather than on servers with vulnerability. To avoid the requirement for a central authority to enable trust in a system, there must be some method that establishes trust amongst the concerned parties, which can be accomplished by distributed consensus among the involved parties. A distributed consensus protocol ensures trust in the blockchain [160]. Multiple nodes using a consensus mechanism check the data's authenticity. In the context of digital Identities, this decentralization is desirable. Some of the trust components of a digital BC-based IDMS are discussed below.

1) NON-REPUDIATION

Non-repudiation is an assurance that something can't be denied. The objective of the non-repudiation service is the collection, maintenance, supply, and testing of an indiscriminate proof of communications from the sender to the recipient. In a blockchain, there are two sides to non-repudiation: first, the information that has been transferred cannot be disputed, for example, a message that A sent to B, thus A cannot deny the behavior. The other is that it is impossible to deny the information recipient. Likewise, A delivered a message to B, but B cannot assert that this message was not received. Digital signatures in blockchain systems employ asymmetric encryption techniques which are typical of elliptical curve equations [43] to ensure that information is not repudiated [192].

2) CONSENSUS ALGORITHMS

Consensus mechanisms are a key element for negotiation and agreement management. The consensus mechanism in blockchain technology allows all nodes to coordinate in the same DL and achieve consistency. It verifies the validity of the blocks and their corresponding transactions. Essentially, the consensus mechanism ensures that each new block added to the blockchain represents the final, agreed-upon version of the truth. Whenever a transaction is completed, it must be validated by individuals known as miners. Generally, all miners run a full node to validate and relay blockchain transactions effectively. Because both miners and non-miners use running nodes to validate and relay, they are all involved in the consensus process. Some of the familiar consensus mechanisms are Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT). We discuss them below.

a: PROOF-OF-WORK (POW)

The consensus mechanism, in this case, requires peers in the network to attempt to solve a computationally costly and complex mathematical challenge. Each peer in the system contributes computational and processing power to the solution of the mathematical problem. The peer who solves the problem first wins the block race and then mines a new block. After a block has been broadcast to the network, each peer confirms the solution and adds it to his blockchain. The likelihood of winning is proportional to the participants' processing capacity [193]. In the PoW mechanism, miners who create and operate nodes must exert a certain amount of work to verify a transaction against other miners and get a reward. The fundamental characteristic of the PoW consensus mechanism is that it is difficult to identify a solution to a complicated mathematical problem but incredibly easy to verify. As a result, once a hash is generated, it can be quickly confirmed, and the consensus is obtained rapidly [194]. The fundamental characteristic of the PoW algorithm is that it is difficult to identify a solution to a complicated mathematical problem but incredibly easy to verify. As a result, once a hash is generated, it can be quickly confirmed, and the consensus is obtained rapidly. Nevertheless, PoW is a computationally intensive technique that consumes a large amount of electricity since all mining nodes try to solve the complicated problem. However, only one node can mine a block.

b: PROOF-OF-STAKE (POS)

In the PoS consensus mechanism, arbitrary winners are chosen from the miners based on the number of tokens held by them. It improves the efficiency of blockchain networks by removing the energy-intensive computational mining process associated with PoW protocols. It employs a pseudo-random selection process to choose a node to serve as the validator

for the next block. It depends on several parameters such as the coin-age selection, the randomization procedure, and the node's wealth. In the PoS algorithm, a user's mining power is defined by the total number of coins he possesses. Each new block is preceded by an auction to determine the prospective miner. Users submit bids on the block, and the highest bidder is chosen as a miner. Thus, in contrast to PoW, the hashing power is substituted by the user's total asset holdings. The more coins an individual possesses, the more likely he is to win the block race.

c: DELEGATED PROOF-OF-STAKE (DPOS)

DPoS is a democratic expansion of PoS, where all token owners select a group of delegates to perform the validation of a transaction. With DPoS blockchain consensus methods, coin holders elect delegates, or witnesses, using their coin balances. Once elected, these delegates have the authority to make critical network-wide decisions. For example, elected delegates can establish protocol rules and verify transactions. The delegates must agree on which transactions to reject and which to authorize. Cyberwealth determines voting power. Those who possess more coins or tokens will exert a more significant influence on the network than those who possess fewer.

d: PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)

PBFT consensus mechanism is a technique to attain the consensus set for the blockchain for a distributed network even if certain nodes are malevolent [195]. PBFT is largely intended to offer Byzantine state machine replication tolerant of malevolent nodes in the system (Byzantine faults) that fail or broadcast inaccurate information to their peer nodes [194]. To avoid spoofing, replay attacks, and identifying damaged communications, PBFT employs encrypted messages [196]. Without doing difficult mathematical computations, PBFT can reach distributed consensus. The approach is intended for use in asynchronous systems. It is optimized to assure excellent speed and fast execution time, although with a minor delay. The PBFT model's nodes are all organized sequentially. One of them is considered the main node (the leader), whereas the rest are known as backup nodes. All nodes in the system communicate with each other. The purpose of all honest nodes is to reach an agreement on the system's state based on the majority's opinion.

Some other consensus protocols are Proof of Capacity (PoC), Proof of Authority (PoA), Quorum-Chain, Plenum. PoC is a consensus technique that assures a party has set aside a specified amount of storage space for a specific purpose. The main advantage of a PoC system over PoW and PoS systems is its efficiency. PoA is a reputation-based consensus method that provides a realistic and efficient solution for blockchain networks, particularly private blockchain networks. Though each can incorporate different blockchain systems, not all can be incorporated into every blockchain technology. In Table 12, we present a summary of all the reviewed articles addressing trust components such as non-repudiation, and various consensus protocols such as proof of work (PoW), practical byzantine fault tolerance (PBFT), proof of stake (PoS), and several others.

TABLE 12. A comparative summary of the trust components in the existing literature.

Trust		Addressed Literature
Non-Repudiation		[9], [13], [15], [19], [121], [124], [138], [145], [153], [162], [166], [169]
Consensus Protocol	Proof of Work	[12], [116], [134], [139]–[143], [145], [146], [150], [151], [161], [163], [169], [178], [197]
	Practical Byzantine Fault Tolerance	[20], [40], [117], [120], [144], [148], [162], [166]
	Proof of Authority	[4]
	Proof of Capacity	[14]
	Proof of Concept	[18], [167], [168]
	Proof of Stake	[6], [23], [112], [126], [129], [160], [198]
	Plenum	[165], [199]
	Quorum-Chain	[129], [181]
	Others	[2], [9], [15], [77], [137], [157]

E. SIMPLICITY

Automating processes for issuing digital identities to users increases the system's efficacy and reduces time and manual efforts. Integration of blockchain technology for IDMS solutions can result in the simplification of digital identity management for all stakeholders. Holders of BC-based digital identities can reap the benefits of this simplicity by moving away from centralized data administration. IdPs can benefit from the increased simplicity due to the automation of procedures for issuing BC-based digital identities to users, which can significantly decrease the time and manual effort necessary to issue identities. The benefits of BC-based SSI management for identity verifiers include a more cost-effective and simplified client onboarding and data verification process. Components such as better scalability, interoperability, minimized cost, and lower energy consumption of the mining process of blockchain technology can increase the simplicity of the BC-based SSI solutions [3], [158].

1) SCALABILITY

Scalability can be defined as the capacity to safeguard a large volume of transactions, an increasing number of nodes, or information without jeopardizing network synchronization, security, usability, or integrity of the data. For the BC-based IDMS solution to become a global framework for digital identity management, the underlying blockchain platform must execute millions of transactions per second, even if claim issuing and some portions of the verification algorithm are performed off-chain. The scalability issue must be addressed before blockchain can be used in any business environment. Due to the modest processing rates of transactions, the need for massive storage space, and a

significant amount of computational power, many public blockchain platforms lack scalability regarding significant numbers of clients and the intensity of transactions [200]. In many real-world business settings, scalability is the most significant barrier to using public blockchains. This explains why computationally costly consensus processes are used in many blockchain-based systems. As the number of nodes increases, the number of transactions increases too; hence more transactions participate in the consensus process. This will inevitably affect the transactions' throughput, latency, and computational energy consumption [201]. However, private blockchains provide adequate scalability regarding a larger number of clients and transaction volumes. Private blockchains are more suited to standard enterprise application settings than public blockchains [202].

2) INTEROPERABILITY

The phrase blockchain interoperability means that information may be seen and accessed across different blockchain platforms. It is simple to understand why blockchain interoperability is not merely desirable, but vital in a world where companies are more dependent on cooperation and connection [29]. To achieve interoperability regarding the verification of identities, the BC-based IDMS solutions should be capable of managing user attributes, data sources, and policies from heterogeneous sources [203]. Cross-chain technology is about building blockchain communication through interoperable blockchain development and implementation. As the developers are looking to speed up blockchain mainstream adoption, the number of blockchain interoperability initiatives is increasing with the integration of projects like cosmos and Polkadot.

3) COMPUTATIONAL AND STORAGE COST

Galvin Wood [174] defines a computational cost as the total cost associated with completing a blockchain transaction. The blockchain community views the computational cost as a critical breakthrough. This has a favorable effect on the PoW and PoS consensus protocols, resulting in a more transparent and efficient mining system [204]. Miners in a blockchain system bear the brunt of growing storage costs, which are generally not adequately balanced by the transaction costs of users. Inadequate storage costs are mostly the result of negative externalities and unjust delay-based pricing [205].

4) ENERGY CONSUMPTION

One of the primary concerns with blockchains is that they require an extravagant amount of energy, mostly during the mining process [206]. Consensus mechanisms such as proof-of-work (PoW) and proof-of-stake are inefficient in terms of energy use. Due to the competitive nature of miners for building blocks by solving complicated mathematical puzzles, PoW is known for requiring a significant amount of electrical energy. To ward off malicious attackers, PoW chains rely on network resource consumption. The blockchain is a P2P method, which means that no intermediaries are involved in the transaction, and it requires a massive number of hash calculations to achieve the best outcomes. In general, it is seen that a significant quantity of energy is wasted during the blockchain process, this energy being in the form of electricity, which degrades the performance. Thus, in order to improve the performance of blockchain, energy loss must be minimized [207]. In Table 13, we present a comparative summary of the addressed simplicity component of all the reviewed articles. In the next section, we provide a security analysis of the proposed academic BC-based IMDS solutions in terms of various attack types and their addressing in the literature.

TABLE 13. A comparative summary of the simplicity components in the existing literature.

Simplicity		Addressed Literature
Scalability		[4], [9], [13]–[15], [18], [19], [40], [56], [76], [116], [117], [121], [138]–[146], [151], [157], [158], [160], [162], [165]–[167], [169], [181]–[183]
Interoperability		[5], [9], [18], [56], [138], [154], [158], [165]
Computing Cost	Low	[4], [9], [13], [14], [19], [40], [56], [76], [77], [112], [117], [137], [138], [142], [144], [146], [148]–[150], [152], [153], [157], [163], [183]
	High	[18], [124], [139], [140], [145], [156], [165]
	Moderate	[15], [16], [116], [141], [162]
	System Dependent	[5], [20], [120], [121], [151], [161]
	Consensus Dependent	[20], [129]
Storage Cost	Low	[14], [15], [19], [40], [77], [117], [141], [151], [152], [157], [163], [181]
	High	[18], [145], [156]
	Moderate	[16], [139], [142], [162], [183]
	System Dependent	[121], [151], [161]
Energy Consumption		[15], [16], [19], [121], [139]

VI. SECURITY ANALYSIS OF THE REVIEWED BC-BASED IDMS IN ACADEMIC LITERATURE

Even though the attributes of blockchain technology may provide us with more dependable and efficient services in terms of digital identity management, the security risks and obstacles that lie behind this novel approach are also essential topics that we must address. The blockchain network is usually regarded as safe and scalable, however, the amount of hash processing power that supports the blockchain is directly proportionate to its security level. The more miners participate in the mining process, the more difficult it is for an attacker to attack the blockchain [208]. Thus, security is critical for potential consumers to accept blockchain technologies. As blockchain is expanding beyond cryptocurrencies and smart contracts, it is continuously integrating the internet of things, the electronic healthcare sector, vehicular ad-hoc

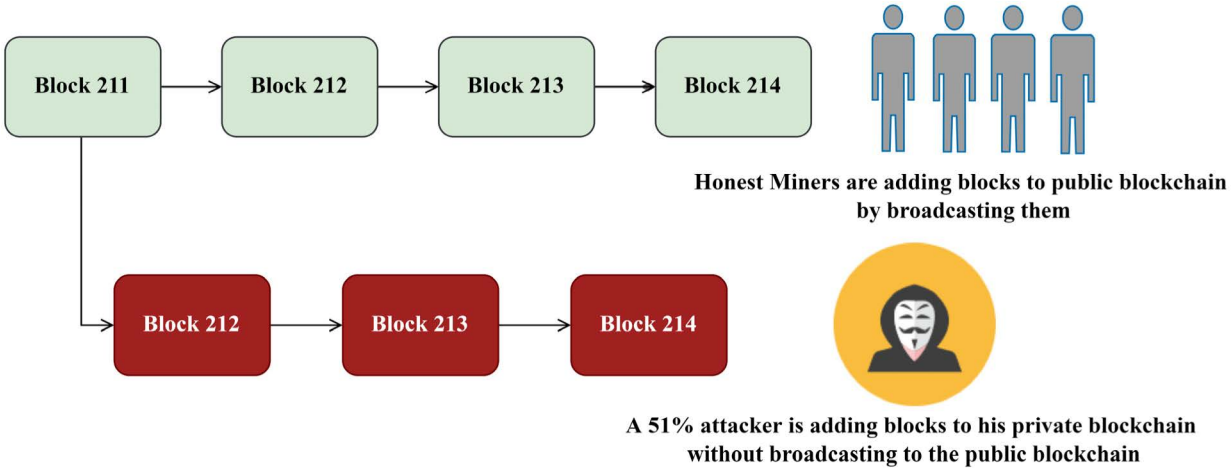

FIGURE 16. Illustration of a 51% attack on a blockchain network.

networks, and cloud computing domains under its application. These large-scale systems store sensitive data and user information. A potential vulnerability in the blockchain system could result in unexpected attacks, jeopardizing the system's overall security and privacy. Hence, it is essential to conduct a systematic investigation of the adversarial methods that could harm the users of those fields. Saad et al. [193] in their survey discuss various attacks (e.g. network attacks and application attacks) that might cause harm to the blockchain network in general. In this section, we analyze several types of network security threats on the blockchain network and classify each evaluated paper based on the attacks addressed in their BC-based IDMS approach. To the best of our knowledge, this is the first survey that performs a security analysis of the proposed BC-based IDMS solutions in the academic literature by discussing various attack mechanisms.

A. 51% ATTACK

A 51% attack, also known as a majority attack, happens when a single malicious user or group gets control of more than 50% of the hashing power on a PoW-based blockchain, potentially causing network disruption. Typically, this is accomplished by renting mining hash power from a third party. Successful attackers obtain the power to prevent new transactions from being completed and to reorder new transactions. It also enables unscrupulous agents to effectively rewrite sections of the blockchain and reverse their transactions, resulting in a problem known as double-spending. Using this approach, an attacker can produce blocks quicker than the other nodes on the network. The attacker may spend funds on the network being constructed by honest miners but not be included in the private blockchain, as shown in Figure 16. The attacker can then broadcast the private blockchain and finish the transaction [208]. The more confirmations a transaction receives, the more difficult it becomes to break, as the number of new blocks mined to bring the network to its current state grows more significant and intensive. As a blockchain network grows and adds more mining nodes, the likelihood of a 51% attack decreases. This is because the cost of launching a 51% attack increases in lockstep with the network hash rate (i.e., the amount of computational power committed to the network). In essence, the larger the network and the more nodes that are a part of it, the more hash power is required to control more than 50% of it. In [190], the authors discuss the 51% attack and introduced a trust-authority node in the proposed architecture. It is primarily designed to prevent malicious voting with a greater degree of voting authorization.

B. MAN IN THE MIDDLE ATTACK (MITM)

In a MITM attack, the attacker often a third party, maliciously takes control of the communication channel so that the message is intercepted, read, and manipulated without any suspicion by either communicating side [52]. Cryptocurrencies like bitcoin employ DL of transactions to move and store funds. Each bitcoin transaction is sent to a blockchain address secured with a pair of encryption keys. An open-ended public key allows all parties to send funds to the address, while a hidden private key allows the address owner to transfer the cash to others. In a MITM attack, a malicious actor breaches communication between two parties and steals or tampers the information they share through bitcoin or a digital wallet. Numerous researches has been conducted and addressed this attack type in their BC-based digital identity and authentication management process [15], [19], [20], [116], [129], [138], [151], [153], [156]. Xu et al. [129] integrate *nonce,* a random number with the blockchain address of the recipient during the authentication request step. During the authentication response step, that *nonce* is decrypted and matched to prevent the MITM attack. Odelu [153] incorporates personal biometrics and a fuzzy extractor for user registration in the proposed system. Upon receiving the response from the authentication server, the user utilizes his secret credentials to confirm the authentication server, thus resisting the MITM attack.

C. IMPERSONATION ATTACK

An attack by impersonation is a type of deception in which attackers present themselves as a recognized or trusted individual to deceive an employee to transfer money to a fake account and share sensitive information. Three types of attacks are used in impersonation: passive, active, and simultaneous [209]. Strong identification and authorization scheme are needed to resist this attack in blockchain and several studies have addressed this attack in their proposed system [7], [10], [15], [20], [126], [138], [153], [156], [158], [178]. Ao et al. [156] utilize IBC and elliptic curve discrete logarithm problem techniques and formulated a mathematical structure that prevents the impersonation attack. In another paper, Hong and Kim [158] integrate a random secret code along with each authentication request to resist the impersonation attack. Xiang et al. [15] integrate mutual authentication and session key agreement process and mathematically formulate an authentication scheme that prevents impersonation attacks.

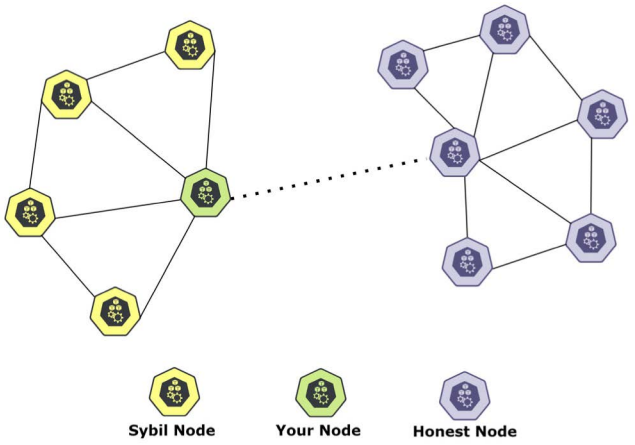

FIGURE 17. Illustration of a Sybil attack on a network.

D. REPLAY ATTACK

It is an active attack method. An attacker logs the communication session and resends an entire session or portion of the session to the authentication server to trick the authentication server. A replay attack is one of the most frequent blockchain vulnerabilities. Replay attacks are possible because the blockchain of a particular cryptocurrency might undergo changes that result in hard forks or chain bifurcations. When a hard fork occurs, the protocol and ledger are separated, and two larger books are generated that are regulated by two distinct protocols. As a result, the blockchain is partitioned into two instances: one that runs the inherited version of the software and another that runs the upgraded version. Several studies e.g., [7], [15], [19], [20], [116], [126], [129], [150], [156], [210] have addressed this replay attack for resistance in their proposed BC-based IDMS solution. Ao et al. [156] devise a system where the challenge number and the private key are random in each authentication process. Therefore, the message signatures and authentication information are different each time, preventing replay attacks. Lansky et al. [126] formulate a system where the cryptographic keys are a factor of the timestamp at a specific time *t1*. The eavesdropped message cannot be used at any later time *t2*, hence preventing the replay attack in the system.

E. SYBIL ATTACK

Sybil attack [211] refers to a malicious node with several valid IDs. In this attack, a hostile peer can establish several false identities to defraud the system in order to violate its mechanism of confidence and redundancy. Through this attack, the attackers block users' transactions, unsettling the mutual network connection, and track transactions of all the users through scripts and software. This type of attack is likely to occur on blockchain networks such as Ethereum, bitcoin cash, and dash. In this respect, however, every network is unique. By using user validation, a chain of trust mechanism, and building consensus protocols that imply an increased cost per identity this attack can be resisted in a blockchain [17], [19], [161], [166], [210], [212]. Many blockchains employ various consensus methods, including PoW, PoS, and DPoS, to prevent Sybil attacks [166]. However, these consensus methods do not prevent Sybil attacks, they only prohibit an attacker from executing the Sybil attack effectively. Figure 17 depicts that many Sybil nodes surround a single node and prevent this node from connecting to the network's honest nodes or its peers. In this way, an attacker could try to prevent the transmission or receiving of information to the network. Each organization and role owner in the system proposed by [212] has a unique identity and key pair. In the blockchain, both entities are recognized by the transaction signed with their private keys. Thus, an adversary cannot utilize a false identity. Zhong et al. [166] propose a protocol where each entity is limited to a single public key as its identity and a single secret key linked with the public key. Furthermore, the system can validate the public key associated with a username, preventing any attacker from using a counterfeit public key and blocking Sybil attacks.

F. FORGERY ATTACK

After acquiring the identities of a user and the service provider, an attacker can forge himself as a legitimate service provider. An attacker forges the information of proof to deceive the third-party auditor [7]. There are multiple types of forgery attacks possible in cryptography such as cross-site scripting forgery [158], digital signature forgery, etc. Tang et al. [13] in their study have provided the resistance mechanism of forgery attacks through user sign signatures and authority sign signatures. Several studies [7], [139], [158], [213] have proposed the resistance mechanism of forgery attacks in BC-based IDMS. Zhiji Li [213] adopts the aggregate signature method to prevent forgery attacks in the system.

G. REPLACEMENT ATTACK

An attacker tries to pass the data integrity check. It does so, by changing the challenged signature and block with an unchallenged and unaffected block and signature. Articles [7] and [19] formulate several mathematical theorems using cryptographic techniques and incorporate random numbers to resist the replacement attacks in the BC-based IDMS in WSNs and cloud storage.

H. COLLUSION ATTACK

In a collision attack, an adversary benefits at the cost of other participating nodes. This is an attack where the node deliberately has a hidden agreement with an attacker, or that node is compromised by an attacker having a high knowledge of the transaction, aggregation, and consensus algorithm, as shown in Figure 18. The adversary with high knowledge of the system attacks through the compromised node or nodes by exploiting false data injection. Several studies [13], [116], [190] have proposed different solutions for resisting this type of attack in blockchain in the field of healthcare, IoT, and cloud storage. Tang et al. [13] incorporate an identity-based signature method with multiple authorities to resist the collusion attack. Zhu et al. [190] introduced a trust-authority node with the power to refusal of illegal documents to prevent a collusion attack.

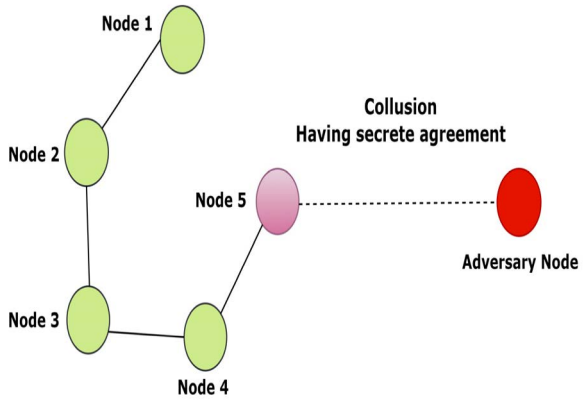

FIGURE 18. Illustration of a collision attack on a network.

I. DOS/DDOS ATTACK

Generally, blockchains are appealing to Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attacks. The risk of a DoS attack on the consortium nodes is an issue for an Ethereum consortium chain. A single source or numerous sources to magnify the effect can launch such an attack [214]. Many BC-based IDMS studies [9], [10], [16], [17], [20], [151], [166] have suggested various mechanisms to resist this attack against the blockchain-enabled system for identity management. In [20], the authors restrict the block size where most of the group signature checks for the transaction input. [166] relies on the inherent decentralized structure of blockchain, such as Ethereum, and its higher transaction cost to prevent DoS attacks.

J. OTHER ATTACK TYPES

Apart from the attack types discussed above, other attack types exist that also cause harm to the BC-based IDMS. One of them is phishing, which is a kind of cryptocurrency fraud in which victims are deceived into disclosing their user identity credentials, private keys, or sensitive personal information [215]. Spoofing attack can be considered as a subset of phishing where the adversary may attempt to spoof a legitimate user's role in order to get access to the user's identity credentials [212]. A malicious third-party auditor can fabricate public audit results for the public cloud storage system [7]. Offline password-guessing tries to recover passwords from the password (hashed) storage file of a target system. While hashes of the passwords cannot be reversed, an adversary can run the hash algorithm forward many times. The adversary can generate possible passwords and match the output to the desired hash to deduce the original password [216].

In Table 14, we provide a comparative summary of the proposed academic BC-based IDMS solutions resistance against the abovementioned attack scenarios. In the next section, we provide a detailed discussion about various issues and challenges associated with implementing BC-based IDMS solutions and provide future research directions based on the discussion.

VII. DISCUSSION AND FUTURE RESEARCH DIRECTIONS

While BC-based digital identity management has been extensively researched and acknowledged in various areas such as IoT, WSN, cloud computing, medical healthcare, etc., there still exists a plethora of constraints and challenges. Undoubtedly, BC-based IDMS eliminates unwanted information exposure to third parties and offers numerous beneficial properties such as interoperability, immutability, transparency, portability, and secure timestamping that can be used to establish trust. Though identity management has been intensively investigated and implemented in practice, it continues to face various constraints and issues. While blockchain technology has the potential to alleviate some of these constraints, there are still several challenges, implications, and issues that require further investigation. More significantly, blockchains and the associated fundamental components discussed in this paper can improve data integrity, privacy, authentication, trust, and simplicity. However, they do not resolve all issues, and a thorough analysis of the security risks and challenges associated with blockchain adoption is necessary. As blockchain is a relatively new technology, it has many limitations yet to overcome. Some issues, challenges, implications, and future research directions are discussed in this section.

A. SCALABILITY

Scalability refers to the blockchain's ability to operate without experiencing slow processing times, system bloat, or lags,

even on a vast network [194]. A blockchain network's data blocks need to store a backup of the transaction data to provide performance efficiency and transparency. As a result, the size and the number of blocks increase gradually concerning the number of transactions. This is a complex task to support the increasing number of transactions and at the same time provide the optimum performance for the communication parties. There are always some scopes of research to design effective load-balancing techniques and scalability. Any ideal blockchain network aims to provide data availability and transparency by implementing proper data storage expanding capability. In the initial phase of blockchain network development, the blockchain architecture was designed using a single-chain network. In a single-chain network, processing power entirely depends on a lone node. Resource processing by a single node is infeasible for the growing nature of data transfer in a blockchain network. In recent times, some parallel chain and cross-chain architectures [217], [218] have been used to content with the limitation of the single-chain network. Side-chain technology improves scalability and data transparency, but some concerns are raised regarding the security of using a side-chain network. There is a research scope to design a better solution using a side- chain blockchain network. By design, a BC-based IDMS solution is distributed, decentralized, and fault-tolerant, hence, lowering the cost of deployment and maintenance. However, scalability appears to be the primary barrier to public blockchain adoption. Numerous unique solutions for IDMS utilizing blockchain technology are now either frameworks, prototypes, or schemes with the promise of scalability in future research. Scalability and optimization are critical for the widespread adoption of distributed IDMS. Gao et al. in their study [162] address this scalability problem in BC-based identity authentication. Liu et al. [219] optimize the scalability of blockchain-based industrial IoT via deep reinforcement learning.

B. EXCLUSION OF INTERMEDIARIES

Each BC-based IDMS provides a decentralized solution that circumvents the control of the centralized authorities. However, the majority of these decentralized and distributed solutions still rely on a central server or intermediary to store the user data and for key revocation. Removal of certificate authority in its entirety may jeopardize various identity management functions, for and lookup services, which is also stated in [33]. Permissionless blockchain ecosystems, like bitcoin, do indeed eliminate the need for intermediaries in processes such as auditing. However, several sectors, like national registrations, voting systems, and trade platforms, will almost certainly remain dependent on third parties. While blockchain technology has the potential to significantly diminish the function of these intermediaries and alter the trust relationships that were previously required, it is unlikely that they will ever be entirely eliminated. Blockchain technology can even assist its users in minimizing their trust in intermediaries in a variety of ways. In [220], Tseng and Shang discuss the sustainable management of the functionalities of the intermediaries in diverse areas such as IDMS, supply chain, and agriculture. Tan et al. [221] discuss the concept of disintermediation of intermediaries in BC-based business models. In a fully BC-based user-controlled system without any intermediary, improper identity management by users can have an adverse impact on the validity and data flow in the infrastructure.

C. LEAKAGE OF PERSONAL DATA

When a user provides personal data to a relying party, the relying party may share the data with third parties outside the IDMS context. This is a severe issue for any IDMS that shares personal user data. This can be reduced by minimizing the data disclosure. For instance, ZKPs are used by many researchers [77], [148] to share sensitive data with reliant parties that contain only the bare minimum information. Separately, systems that keep less data on the chain may be more privacy-preserving in general, however, this is dependent on the specific architecture employed and the type of stored data such as plain-text, encrypted, references to external repositories, and hashes [51]. Kumar et al. [184] suggested using double encryption of encrypted biometric facial image features using an elliptic encryption curve. Methods such as ZKP and Proxy Re-Encryption utilized in [138], [150] to preserve the privacy attributes of a user can also be used in IDMS architecture.

D. IDENTITY REVOCATION

A blockchain is immutable in its functionalities. So, what if a user needs to change or delete something about his or her identity? The term ''revocation'' refers to the act of deleting or modifying a credential. Identity revocation is one of the difficult challenges to resolve in SSI systems since no central server can simply revoke users' cryptographic keys. The market-offered solutions discussed in this study do not store anonymous credentials or cryptographic keys. The systems depend on the user to secure the data on his or her smartphone or computer. Nevertheless, this technique, which depends on users to safeguard credentials, entails unavoidable risks, in terms of non-technical users [86]. The existing on-device solution utilized in some of these systems is not persistent in the event of device failure or loss. For instance, BlockStack and ShoCard do not have any end-user key management functionality. While Sovrin and uPort have advanced the concept of key recovery, their work is still ongoing. However, in academic literature, several studies [40], [77], [117], [128], [197] have explored this identity and certificate revocation task in many areas such as mobile networks, IoT, and healthcare systems. The use of multiple blockchains in a single network, as proposed by Maldonado-Ruiz et al. [178], can also be another direction for future research. Developing a secure, cost-effective, and functioning IDMS is not a straightforward task. To promote SSI, new, effective, and well-analyzed solutions are required.

TABLE 14. A comparative summary of all the reviewed academic BC-based IDMS solutions that addressed common attack types in the blockchain, (- addressed, x - not addressed).

Ref.	Attack Resistance											
	MITM	Impersonation	Replay	Phishing and Spoofing	Forgery	Replacement	51% Attack	Sybil	Collusion	DoS/DDoS	Malicious Auditors	Offline Password Guessing
[2]	x	x	x	x	✓	x	x	x	x	x	x	x
[7]	x	x	✓	x	✓	✓	x	x	x	x	✓	x
[8]	x	x	x	x	✓	x	x	x	x	x	✓	x
[9]	x	x	x	✓	x	x	x	x	x	✓	x	x
[10]	x	✓	✓	x	x	x	x	x	x	✓	x	✓
[13]	x	x	x	x	✓	x	x	x	✓	x	x	x
[15]	✓	✓	✓	x	x	x	x	x	x	x	x	✓
[16]	x	x	x	x	x	✓	x	x	x	✓	x	x
[17]	x	x	x	✓	x	x	x	✓	x	✓	x	x
[19]	✓	x	✓	✓	x	✓	x	✓	x	✓	x	x
[20]	✓	✓	✓	x	x	x	x	x	x	✓	x	x
[112]	x	✓	x	x	✓	x	x	x	x	x	x	x
[116]	✓	x	✓	x	x	x	x	x	✓	x	x	x
[120]	x	x	x	x	x	✓	x	x	x	x	x	x
[121]	x	x	✓	✓	x	x	x	✓	x	✓	x	x
[124]	✓	✓	✓	✓	x	x	x	x	x	x	x	x
[126]	✓	✓	✓	x	x	x	x	x	x	x	x	x
[128]	✓	✓	✓	x	x	x	x	x	x	x	x	x
[129]	✓	x	✓	✓	x	x	x	x	x	x	x	x
[138]	✓	✓	x	x	x	x	x	x	x	x	x	✓
[139]	x	x	x	x	✓	✓	x	x	x	x	x	x
[141]	x	x	x	✓	x	x	x	x	x	x	x	x
[148]	x	x	x	x	✓	x	x	x	x	x	x	x
[150]	x	x	✓	x	x	x	x	x	x	x	x	x
[151]	✓	x	x	x	x	x	x	x	x	✓	x	x
[153]	✓	✓	✓	x	x	x	x	x	x	x	x	x
[156]	✓	✓	✓	x	x	x	x	x	x	x	x	x
[158]	x	✓	x	x	x	x	x	x	x	x	✓	x
[161]	x	x	x	x	x	x	x	✓	x	x	x	x
[166]	x	x	x	x	x	x	x	✓	x	✓	x	x
[167]	x	✓	x	x	✓	x	x	-	x	x	x	x
[168]	x	✓	x	x	x	x	x	x	x	x	x	x
[178]	x	✓	x	x	x	x	x	x	x	x	x	x
[182]	x	x	x	x	✓	x	x	x	x	x	x	x
[190]	x	x	x	x	x	x	✓	x	✓	x	x	x
[210]	x	x	✓	x	x	x	x	✓	x	x	x	x
[212]	x	x	x	✓	x	x	x	✓	x	x	x	x
[213]	x	x	x	✓	✓	x	x	x	x	x	x	x

E. KEY LEAKAGE

Public and private cryptographic keys are intended to ensure that the blockchain system maintains a certain level of privacy. If someone loses the private key, it is nearly impossible or ineffective to regenerate a new key and digital identity. Proper key management in the context of SSI is critical to its widespread adoption, which is also stated in [30]. Users maintain pseudonymous privacy throughout the transaction procedure. However, assuring transactional privacy is difficult because all the information related to a transaction is exposed to everyone which can enable adversaries to access a user's information by connecting with many transactions concurrently. Brengel and Rossow [222], in their study about key leakage, identified two types of leakage, explicit and implicit, that occur on open source platforms, and the wrong usage of cryptographic primitives by users, respectively, and discussed possible solutions. In [223], Feng et al. suggest key management through a multi-party signing protocol, which can also be a future research direction.

F. OVERLOOKING THE CONDITIONAL TRACEABILITY, ACCOUNTABILITY, AND CONTROL FEATURES

Generally, present efforts overlook the importance of user access control, accountability, and conditional traceability. Privacy protection enables users to make payments without being identified by non-participants, enabling the blockchain to be used for diverse criminal activities. As a result, it is vital to divulge the true identity of malicious nodes in some instances. Unlike centralized design, permissionless blockchains, on the other hand, lack a powerful and trusted third party that can provide private insurance while also acting as an arbitral authority [224]. The decentralized architecture increases the opportunities of adversaries and ways to commit misbehavior, making it more difficult to resolve the balance between privacy and responsibility. Nonetheless, previous works seldom address the aforementioned topics.

G. SPEED AND ENERGY CONSUMPTION ISSUE OF CONSENSUS PROTOCOL

The consensus techniques used for trust, and validation affect the speed and computing power necessary to scale and sustain service-level agreements among communicating parties. Before transactions can be accepted, all nodes on the chain must reach a consensus. The number of messages necessary to obtain consensus regarding a single decision increase radically and eventually slows down the network. That's why a good consensus protocol is needed to establish an efficient and flexible BC-based IDMS that will generate sufficient trust in the validity of the identity and does this quickly without slowing down the network. Our study demonstrates that most of the existing IDMS solutions in academic literature utilize the PoW, PoS, and PBFT consensus protocols, see Table 12; however, it is important to develop an energy-efficient and robust consensus mechanism that may be used in place of PoW, PBFT, and PoS. PoW is extremely inefficient in terms of energy consumption. Additionally, PoW creates a race condition in Blockchains, where miners engage for block rewards [225]. Eventually, the race condition facilitates various attacks such as selfish mining, double spending, and 51% attacks. To solve energy inefficiencies and eliminate race conditions, PoS has been recommended as a block mining protocol that utilizes an auction process. However, PoS can result in network centralization and systemic unfairness. While PBFT is a viable alternative to PoW and PoS, it has some significant drawbacks. Due to the low fault tolerance of PBFT-based blockchains, they are particularly susceptible to Sybil attacks. If an attacker places Sybil nodes in a third of the system, they can eventually block the blockchain from reaching consensus. Additionally, private blockchains based on PBFTs have a high message complexity and suffer from limited scalability. As a result, the network never exceeds a few hundred nodes in size. Knowing the attack surface of consensus protocols enables the construction of a meta-consensus procedure that results in hybrid consensus [193]. The hybrid consensus process enables the network designer to swap consensus protocols while balancing risks and other considerations such as service quality. Additionally, academics are continuously striving to strengthen and optimize the blockchain system's consensus processes, such as proof of entitlement, proof of activity [226], proof of reputation [227], and proof of authorization [38].

H. OVER UTILIZATION OF ETHEREUM BLOCKCHAIN TYPE

The majority of the academic BC-based IDMS proposals used the permissionless Ethereum blockchain. Systems that rely only on the public permissionless Ethereum network are subject to the long-term availability of the Ethereum blockchain. Bitcoin is no longer a viable method for large-scale IDMS solutions due to its heavy network load. As Ethereum's network traffic grows, it, too, may face a similar destiny over the next couple of years. On the other hand, a blockchain-agnostic-based IDMS solution will remain unaffected and shows efficient scalability in diverse areas [129].

VIII. CONCLUSION

Blockchain is still a relatively new tamper-resistant technology. Although it has enormous potential to affect our social life through a wide range of applications, it has already proved its significance in the digital identity management system. The blockchain architecture provides decentralization, data integrity, scalable storage, smart contracts service, transparency, trustworthiness, traceability, immutability, and many other features essential in a particular application like identity management. The notion of BC-based SSI is an exhilarating prospect. This research focuses on analyzing recent cutting-edge developments in the field of BC-based IDMS to provide users with SSI. In this paper, we have provided a comprehensive review of BC-based IDMS solutions. We then outlined and discussed the essential components that an effective BC-based IDMS should ensure. We reviewed sixty-three

significant academic research related to BC-based IDMS, mentioning their strengths and weaknesses by analyzing their utilized methodologies, tools, technologies, and the underlying security of the architectures. Since BC-based IDMSs are also generating much buzz in the commercial market, we have also reviewed and provided a comparative summary of some of the notable market offerings in BC-based IDMS solutions. This paper will help researchers who want to obtain a core idea about the blockchain network, the path to decentralized identity, and the components needed for a robust BC-based digital IDMS solution.

There are always some research challenges and scope to improve the previous implementation by introducing a new scalable network policy, maintaining a chained network, transaction cost, proper selection of consensus protocol, developing standards for blockchain architecture, analyzing security threats, and many other aspects. The majority of retrieved studies on BC-based IDMS use cases are conceptual rather than empirical, for instance, security analysis of the proposed BC-based IMDSs. However, we have found that most of the papers did not perform a practically adequate security analysis of their proposed system but instead performed a conceptual analysis. Empirical research on blockchains is relatively uncommon, primarily justified by the technology's freshness. While conceptual efforts are critical, more convenient research on BC-based IDMS should be done on an empirical basis. Although blockchain gives up some control of disputes, it will make a better and brighter future for everyone if users can use the ethos behind the advantages of blockchain technology.

REFERENCES

[1] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security Privacy*, vol. 16, no. 4, pp. 20–29, Jul./Aug. 2018.

[2] H. Wang and Y. Jiang, "A novel blockchain identity authentication scheme implemented in fog computing," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–7, Aug. 2020.

[3] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In search of self-sovereign identity leveraging blockchain technology," *IEEE Access*, vol. 7, pp. 103059–103079, 2019.

[4] I. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, and K. N. Qureshi, "Health-ID: A blockchain-based decentralized identity management for remote healthcare," *Healthcare*, vol. 9, no. 6, p. 712, Jun. 2021.

[5] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment," *J. Med. Syst.*, vol. 42, no. 8, pp. 1–14, Aug. 2018.

[6] K. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha, "WiP: A novel blockchain-based trust model for cloud identity management," in *Proc. IEEE 16th Int. Conf. Dependable, Autonomic Secure Comput., 16th Int. Conf. Pervasive Intell. Comput., 4th Int. Conf Big Data Intell. Comput. Cyber Sci. Technol. Congress (DASC/PiCom/DataCom/CyberSciTech)*, Aug. 2018, pp. 716–723.

[7] J. Xue, C. Xu, J. Zhao, and J. Ma, "Identity-based public auditing for cloud storage systems against malicious auditors via blockchain," *Sci. China Inf. Sci.*, vol. 62, no. 3, pp. 1–16, Mar. 2019.

[8] Y. Zhang, C. Xu, X. Lin, and X. Shen, "Blockchain-based public integrity verification for cloud storage against procrastinating auditors," *IEEE Trans. Cloud Comput.*, vol. 9, no. 3, pp. 923–937, Jul. 2021.

[9] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. A. El-Latif, "DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems," *IEEE Access*, vol. 8, pp. 111223–111238, 2020.

[10] G. Deep, R. Mohana, A. Nayyar, P. Sanjeevikumar, and E. Hossain, "Authentication protocol for cloud databases using blockchain mechanism," *Sensors*, vol. 19, no. 20, pp. 1–13, 2019.

[11] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health Informat. J.*, vol. 25, pp. 1398–1411, Dec. 2019.

[12] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.

[13] F. Tang, S. Ma, Y. Xiang, and C. Lin, "An efficient authentication scheme for blockchain-based electronic health records," *IEEE Access*, vol. 7, pp. 41678–41689, 2019.

[14] T. Mikula and R. H. Jacobsen, "Identity and access management with blockchain in electronic healthcare records," in *Proc. 21st Euromicro Conf. Digit. Syst. Design (DSD)*, Aug. 2018, pp. 699–706.

[15] X. Xiang, M. Wang, and W. Fan, "A permissioned blockchain-based identity management and user authentication scheme for e-health systems," *IEEE Access*, vol. 8, pp. 171771–171783, 2020.

[16] G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, "On the design and implementation of a blockchain enabled e-voting application within IoT-oriented smart cities," *IEEE Access*, vol. 9, pp. 34165–34176, 2021.

[17] M. P. Andersen, J. Kolb, K. Chen, G. Fierro, D. E. Culler, and R. A. Popa, "WAVE: A decentralized authorization system for IoT via blockchain smart contracts," Univ. Calif. Berkeley, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2017-234, 2017.

[18] M. A. Bouras, Q. Lu, S. Dhelim, and H. Ning, "A lightweight blockchain-based IoT identity management approach," *Future Internet*, vol. 13, no. 24, pp. 1–14, 2021.

[19] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 241–251, Apr. 2020.

[20] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K.-K.-R. Choo, "HomeChain: A blockchain-based secure mutual authentication system for smart Homes," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 818–829, Feb. 2020.

[21] V. L. Lemieux, "Evaluating the use of blockchain in land transactions: An archival science perspective," *Eur. Property Law J.*, vol. 6, no. 3, pp. 392–440, Dec. 2017.

[22] G. Sladić, B. Milosavljević, S. Nikolić, D. Sladić, and A. Radulović, "A blockchain solution for securing real property transactions: A case study for Serbia," *ISPRS Int. J. Geo-Inf.*, vol. 10, no. 1, p. 35, Jan. 2021.

[23] A. S. Yadav and D. S. Kushwaha, "Blockchain-based digitization of land record through trust value-based consensus algorithm," *Peer Peer Netw. Appl.*, vol. 14, no. 6, pp. 3540–3558, Nov. 2021.

[24] F. Ullah and F. Al-Turjman, "A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities," *Neural Comput. Appl.*, pp. 1–22, Feb. 2021.

[25] S. Soner, R. Litoriya, and P. Pandey, "Exploring blockchain and smart contract technology for reliable and secure land registration and record management," *Wireless Pers. Commun.*, vol. 121, no. 4, pp. 2495–2509, Dec. 2021.

[26] C. Papantoniou and B. Hilton, "Enterprise solutions criteria in the age of GeoBlockchain: Land ownership and supply chain," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, Jan. 2021, pp. 5307–5316.

[27] B. Houtan, A. S. Hafid, and D. Makrakis, "A survey on blockchain-based self-sovereign patient identity in healthcare," *IEEE Access*, vol. 8, pp. 90478–90494, 2020.

[28] M. Shuaib, S. Alam, M. S. Alam, and M. S. Nasir, "Self-sovereign identity for healthcare using blockchain," *Mater. Today, Proc.*, pp. 1–15, Mar. 2021.

[29] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," *Comput. Structural Biotechnol. J.*, vol. 16, pp. 224–230, Jan. 2018.

[30] R. Soltani, U. T. Nguyen, and A. An, "A survey of self-sovereign identity ecosystem," *Secur. Commun. Netw.*, vol. 2021, pp. 1–26, Jul. 2021.

[31] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Blockchain-based identity management systems: A review," *J. Netw. Comput. Appl.*, vol. 166, Sep. 2020, Art. no. 102731.

[32] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1008–1027, Nov. 2020.

[33] K. Gilani, E. Bertin, J. Hatin, and N. Crespi, "A survey on blockchain-based identity management and decentralized privacy for personal data," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 97–101.

[34] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Comput. Sci. Rev.*, vol. 30, pp. 80–86, Nov. 2018.

[35] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, and R. Ismail, "Blockchain technology the identity management and authentication service disruptor: A survey," *Int. J. Adv. Sci. Eng. Inf. Tech.*, vol. 8, pp. 1735–1745, Sep. 2018.

[36] X. Zhu and Y. Badr, "Identity management systems for the Internet of Things: A survey towards blockchain solutions," in *Proc. IEEE Conf. Internet Things, Green Comput. Commun., Cyber, Phys. Social Comput., Smart Data, Blockchain, Comput. Inf. Technol., Congr. Cyberma*, 2018, vol. 18, no. 12, pp. 1568–1573.

[37] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, p. 21260, 2008.

[38] B. Cao, X. Wang, W. Zhang, H. Song, and Z. Lv, "A many-objective optimization model of industrial Internet of Things based on private blockchain," *IEEE Network*, vol. 34, no. 5, pp. 78–83, Sep./Oct. 2020.

[39] T. Rathee and P. Singh, "A systematic literature mapping on secure identity management using blockchain technology," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 6, no. 5, pp. 86–91, 2021.

[40] J. Xu, K. Xue, H. Tian, J. Hong, D. S. L. Wei, and P. Hong, "An identity management and authentication scheme based on redactable blockchain for mobile networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6688–6698, Jun. 2020.

[41] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, p. 352, 2018.

[42] R. Qin, Y. Yuan, and F.-Y. Wang, "Research on the selection strategies of blockchain mining pools," *IEEE Trans. Computat. Social Syst.*, vol. 5, no. 3, pp. 748–757, Sep. 2018.

[43] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001.

[44] Y. Romailler and S. Pelissier, "Practical fault attack against the Ed25519 and EdDSA signature schemes," in *Proc. Workshop Fault Diagnosis Tolerance Cryptogr. (FDTC)*, Sep. 2017, pp. 17–24.

[45] F. Fatz, P. Hake, and P. Fettke, "Confidentiality-preserving validation of tax documents on the blockchain," in *Wirtschaftsinformatik* (Zentrale Tracks). 2020, pp. 1262–1277.

[46] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, and S. Muralidharan, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.

[47] J. Moosavi, L. M. Naeni, A. M. Fathollahi-Fard, and U. Fiore, "Blockchain in supply chain management: A review, bibliometric, and network analysis," *Environ. Sci. Pollut. Res.*, pp. 1–15, Feb. 2021.

[48] Y. Zhu, W. Song, D. Wang, D. Ma, and W. C.-C. Chu, "TA-SPESC: Toward asset-driven smart contract language supporting ownership transaction and rule-based generation on blockchain," *IEEE Trans. Rel.*, vol. 70, no. 3, pp. 1255–1270, Sep. 2021.

[49] W. Yao, J. Ye, R. Murimi, and G. Wang, "A survey on consortium blockchain consensus mechanisms," 2021, *arXiv:2102.12058*.

[50] K. Stefanova, D. Kabakchieva, and R. Nikolov, "Design principles of identity management architecture development for cross-border eGovernment services," *Electron. J. e-Government*, vol. 8, no. 2, pp. 189–202, 2010.

[51] L. Lesavre, P. Varin, P. Mell, M. Davidson, and J. Shook, "A taxonomic approach to understanding emerging blockchain identity management systems," 2019, *arXiv:1908.00929*.

[52] A. Garba, Z. Guan, A. Li, and Z. Chen, "Analysis of man-in-the-middle of attack on bitcoin address," in *Proc. 15th Int. Joint Conf. e-Business Telecommun.*, 2018, pp. 388–395.

[53] D. Temoshok and C. Abruzzi, "Developing trust frameworks to support identity federations," U.S. Dep. Commer. Natl. Inst. Stand. Technol., Gaithersburg, MD, USA, Tech. Rep. NISTIR 8149, 2018.

[54] A. Jøsang and S. Pope, "User centric identity management," in *Proc. AusCERT Asia Pacific Inf. Technol. Secur. Conf.*, 2005, pp. 1–13.

[55] M. Kubach, C. H. Schunck, R. Sellung, and H. Roßnagel, "Self-sovereign and decentralized identity as the future of identity management?" in *Open Identity Summit* (Lecture Notes in Informatics), vol. 305, Bonn Germany: Gesellschaft für Informatik, 2020, pp. 35–47.

[56] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala, and M. Avital, "Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation," *Blockchain, Res. Appl.*, vol. 2, no. 2, Jun. 2021, Art. no. 100014.

[57] D. W. Chadwick, "Federated identity management," in *Foundations of Security Analysis and Design V*. Berlin, Germany: Springer, 2009, pp. 96–120.

[58] R. Laborde, A. Oglaza, S. Wazan, F. Barrere, A. Benzekri, D. W. Chadwick, and R. Venant, "A user-centric identity management framework based on the W3C verifiable credentials and the FIDO universal authentication framework," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–8.

[59] E. K. Kiyemba Edris, M. Aiash, and J. K.-K. Loo, "The case for federated identity management in 5G communications," in *Proc. 5th Int. Conf. Fog Mobile Edge Comput. (FMEC)*, Apr. 2020, pp. 120–127.

[60] S. El Jaouhari, A. Bouabdallah, and J. M. Bonnin, "Security issues of the web of things," in *Managing the Web of Things: Linking the Real World to the Web*, 1st ed. Amsterdam, The Netherlands: Elsevier, 2017, pp. 389–424.

[61] D. Recordon and D. Reed, "OpenID 2.0: A platform for user-centric identity management," in *Proc. 2nd ACM Workshop Digit. Identity Manage. (DIM)*, 2006, pp. 11–16.

[62] D. Fett, R. Küsters, and G. Schmitz, "A comprehensive formal security analysis of OAuth 2.0," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 1204–1215.

[63] *PICOS—Privacy and Identity Management for Community Services*. Accessed: Dec. 20, 2021. [Online]. Available: http://www.picos-project.eu/

[64] V. Bertocci, G. Serack, and C. Baker, *Understanding Windows Cardspace: An Introduction to the Concepts and Challenges of Digital Identities*. Boston, MA, USA: Addison Wesley, 2007.

[65] S. Cucko and M. Turkanovic, "Decentralized and self-sovereign identity: Systematic mapping study," *IEEE Access*, vol. 9, pp. 139009–139027, 2021.

[66] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," *Sovrin Found.*, vol. 29, no. 2016, p. 18, 2016.

[67] N. Naik and P. Jenkins, "Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology," in *Proc. 8th IEEE Int. Conf. Mobile Cloud Comput., Services, Eng. (MobileCloud)*, Aug. 2020, pp. 90–95.

[68] C. Brunner, U. Gallersdörfer, F. Knirsch, D. Engel, and F. Matthes, "DID and VC: Untangling decentralized identifiers and verifiable credentials for the web of trust," in *Proc. 3rd Int. Conf. Blockchain Technol. Appl.*, Dec. 2020, pp. 61–66.

[69] M. Sporny, D. Longley, and D. Chadwick. (2019). *Verifiable Credentials Data Model V1.1*. Accessed: Jul. 23, 2022. [Online]. Available: https://github.com/w3c/vc-data-model/

[70] Z. A. Lux, D. Thatmann, S. Zickau, and F. Beierle, "Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 71–78.

[71] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen. (2019). *Decentralized Identifiers (DIDs) V1.0, W3C*. Accessed: Jul. 24, 2022. [Online]. Available: https://www.w3.org/TR/did-core/

[72] Y. Liu, G. Sun, and S. Schuckers, "Enabling secure and privacy preserving identity management via smart contract," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 1–8.

[73] C. Allan. *The Path to Self Sovereign Identity*. Accessed: Jun. 9, 2021 [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[74] A. E. Panait, R. F. Olimid, and A. Stefanescu, "Identity management on blockchain—Privacy and security aspects," in *Proc. Romanian Acad. A, Math. Phys. Tech. Sci. Inf. Sci.*, 2020, vol. 21, no. 1, pp. 45–52.

[75] H. Farahmand. (2018). *Blockchain: The Dawn of Decentralized Identity*. Gartner Research. Accessed: Aug. 3, 2022. [Online]. Available: https://www.gartner.com/en/documents/3876011

[76] A. Gruner, A. Muhle, T. Gayvoronskaya, and C. Meinel, "A quantifiable trust model for blockchain-based identity management," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1475–1482.
[77] N. D. Sarier, "Efficient biometric-based identity management on the blockchain for smart industrial applications," *Pervas. Mobile Comput.*, vol. 71, Feb. 2021, Art. no. 101322.
[78] K. Cameron. (2005). *The Laws of Identity*. Microsoft Corp. Accessed: Jun. 3, 2020. [Online]. Available: https://www.identityblog.com/?p=352
[79] S. E. Haddouti and M. D. E.-C. El Kettani, "Analysis of identity management systems using blockchain technology," in *Proc. Int. Conf. Adv. Commun. Technol. Netw. (CommNet)*, 2019, pp. 1–7, doi: 10.1109/COMMNET.2019.8742375.
[80] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena. (2016). *Uport: A Platform for Self? Sovereign Identity*. [Online]. Available: https://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf
[81] (2021). *Veramo (V3.1.2)*. Accessed: Jul. 25, 2022 [Online]. Available: https://veramo.io/
[82] (2021). *Serto*. Accessed: Jul. 25, 2022 [Online]. Available: https://www.serto.id/
[83] A. Grüner, A. Mühle, and C. Meinel, "On the relevance of blockchain in identity management," 2018, *arXiv:1807.08136*.
[84] P. J. Windley, "Sovrin: An identity metasystem for self-sovereign identity," *Frontiers Blockchain*, vol. 4, pp. 1–14, Jul. 2021.
[85] *Travel Identity of the Future*, ShoCard, Cupertino, CA, USA, 2016.
[86] A. Satybaldy, M. Nowostawski, and J. Ellingsen, "Self-sovereign identity systems: Evaluation framework," *IFIP Adv. Inf. Commun. Technol.*, vol. 576, pp. 447–461, Apr. 2020.
[87] F. Ghaffari, K. Gilani, E. Bertin, and N. Crespi, "Identity and access management using distributed ledger technology: A survey," *Int. J. Netw. Manag.*, vol. 32, no. 2, p. e2180, 2022.
[88] D. van Bokkem, R. Hageman, G. Koning, L. Nguyen, and N. Zarin, "Self-sovereign identity solutions: The necessity of blockchain technology," 2019, *arXiv:1904.12816*.
[89] B. Reid and B. Witteman. (2018). *EverID Whitepaper—Decentralized Identity Platform*. [Online]. Available: https://neironix.io/documents/whitepaper/6176/EverID_Whitepaper_v1.0.2_July2018.pdf
[90] L. Foundation. (2019). *LifeID—An Open-Source, Blockchain-Based Platform for Self-Sovereign Identity*. [Online]. Available: https://lifeid.io/whitepaper.pdf
[91] *SelfKey—The SelfKey Foundation*. Accessed: Nov. 24, 2021. [Online]. Available: https://selfkey.org/
[92] *JOLOcom—A Decentralized Identity Solution*. Accessed: Nov. 25, 2021. [Online]. Available: https://github.com/jolocom/jolocom
[93] M. Takemiya and B. Vanieiev, "Sora identity: Secure, digital identity on the blockchain," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf.*, vol. 2, Oct. 2018, pp. 582–587.
[94] *IdChainz—The Smart Ledger-Based Identity Management Solution*. Accessed: Nov. 24, 2021. [Online]. Available: https://www.chainzy.com/products/idchainz/
[95] *Civic—Whitepaper*. Accessed: Dec. 8, 2021. [Online]. Available: https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf
[96] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains," in *Proc. USENIX Annu. Tech. Conf. (USENIX ATC)*, 2016, pp. 181–194.
[97] R. Panetta and L. Cristofaro, "A closer look at the EU-funded my health my data project," *Digit. Heal. Leg.*, pp. 10–11, Dec. 2016.
[98] *UniqueID-An Open-Source & Decentralized Identity and Access Management Protocol*. Accessed: Dec. 3, 2021. [Online]. Available: https://uniquid.com/
[99] O. Dib and K. Toumi, "Decentralized identity systems: Architecture, challenges, solutions and future directions," *Ann. Emerg. Technol. Comput.*, vol. 4, no. 5, pp. 19–40, Dec. 2020.
[100] M. Shuaib, N. H. Hassan, S. Usman, S. Alam, S. Bhatia, A. Mashat, A. Kumar, and M. Kumar, "Self-sovereign identity solution for blockchain-based land registry system: A comparison," *Mobile Inf. Syst.*, vol. 2022, pp. 1–17, Apr. 2022.
[101] A. Poikola, K. Kuikkaniemi, and H. Honko, "MyData—A Nordic Model for human-centered personal data management and processing," Work. Paper, 2015.
[102] A. Giaretta, S. Pepe, and N. Dragoni, "UniquID?: A quest to reconcile identity access management and the Internet of Things," in *Proc. Int. Conf. Objects, Compon., Models Patterns*, 2019, pp. 237–251.
[103] M. T. Quasim, M. A. Khan, F. Algarni, A. Alharthy, and G. M. M. Alshmrani, *Blockchain Frameworks*. Cham, Switzerland: Springer, Mar. 2020.
[104] N. Naik and P. Jenkins, "uPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain," in *Proc. IEEE Int. Symp. Syst. Eng. (ISSE)*, 2020, pp. 1–7, doi: 10.1109/ISSE49799.2020.9272223.
[105] *IRMA Issuance and Disclosure Protocol*. Accessed: Nov. 25, 2021. [Online]. Available: https://credentials.github.io/protocols/irma-protocol/
[106] *Idemix*. Accessed: Dec. 12, 2021. [Online]. Available: https://github.com/IBM/idemix
[107] J. C. Nauta and R. Joosten, "Self-sovereign identity?: A comparison of IRMA and Sovrin," Techruption, Groningen, The Netherlands, Tech. Rep. TNO 2019 R11011, Jul. 2019.
[108] B. Hampiholi and G. Alpar, "Privacy-preserving webshopping with attributes," in *Proc. IEEE Symp. Privacy-Aware Comput. (PAC)*, Aug. 2017, pp. 25–36.
[109] M. Schanzenbach, G. Bramm, and J. Schutte, "ReclaimID: Secure, self-sovereign identities using name systems and attribute-based encryption," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun., 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 946–957.
[110] G. Lax and A. Russo, "A lightweight scheme exploiting social networks for data minimization according to the GDPR," *IEEE Trans. Computat. Social Syst.*, vol. 8, no. 2, pp. 388–397, Apr. 2021.
[111] S. Rodriguez Garzon, H. Yildiz, and A. Küpper, "Towards decentralized identity management in multi-stakeholder 6G networks," 2022, *arXiv:2203.00300*.
[112] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud," *IEEE Access*, vol. 8, pp. 70604–70615, 2020.
[113] W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya, "Blockchain-based trust management in cloud computing systems: A taxonomy, review and future directions," *J. Cloud Comput.*, vol. 10, no. 1, pp. 1–34, 2021.
[114] M. Goresky and A. Klapper, "Arithmetic crosscorrelations of feedback with carry shift register sequences," *IEEE Trans. Inf. Theory*, vol. 43, no. 4, pp. 1342–1345, Jul. 1997.
[115] I. Khalil, A. Khreishah, and M. Azeem, "Consolidated identity management system for secure mobile cloud computing," *Comput. Netw.*, vol. 65, no. 2, pp. 99–110, Jun. 2014.
[116] S. Wang, R. Pei, and Y. Zhang, "EIDM: A Ethereum-based cloud user identity management protocol," *IEEE Access*, vol. 7, pp. 115281–115291, 2019.
[117] A. Sabir and N. Fetais, "A practical universal consortium blockchain paradigm for patient data portability on the cloud utilizing delegated identity management," in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Feb. 2020, pp. 484–489.
[118] S. Nayak, N. C. Narendra, A. Shukla, and J. Kempf, "Saranyu: Using smart contracts and blockchain for cloud tenant management," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Sep. 2020, pp. 857–861.
[119] N. M. Ahmad, S. F. A. Razak, S. Kannan, I. Yusof, and A. H. M. Amin, "Improving identity management of cloud-based IoT applications using blockchain," in *Proc. Int. Conf. Intell. Adv. Syst. (ICIAS)*, Aug. 2018, pp. 1–6.
[120] X. Li, J. Zhang, X. Niu, and J. Guan, "Blockchain-based certificateless identity management mechanism in cloud-native environments," in *Proc. ACM Int. Conf.*, 2021, pp. 139–145.
[121] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, Sep. 2018.
[122] J. Chen, Y. Liu, and Y. Chai, "An identity management framework for Internet of Things," in *Proc. IEEE 12th Int. Conf. e-Business Eng.*, Oct. 2015, pp. 360–364.
[123] A. S. Omar and O. Basir, "Identity management in IoT networks using blockchain and smart contracts," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 994–1000.
[124] X. Yang, X. Yang, X. Yi, I. Khalil, X. Zhou, D. He, X. Huang, and S. Nepal, "Blockchain-based secure and lightweight authentication for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3321–3332, Mar. 2022.

[125] N. Shi, L. Tan, C. Yang, C. He, J. Xu, Y. Lu, and H. Xu, "BacS: A blockchain-based access control scheme in distributed Internet of Things," *Peer Peer Netw. Appl.*, vol. 14, no. 5, pp. 2585–2599, Sep. 2021.

[126] J. Lansky, "BCmECC: A lightweight blockchain-based authentication and key agreement protocol for Internet of Things," *Mathematics*, vol. 9, pp. 52–59, Dec. 2016.

[127] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.

[128] Y. Yang, L. Wei, J. Wu, C. Long, and B. Li, "A blockchain-based multi-domain authentication scheme for conditional privacy preserving in vehicular ad-hoc network," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8078–8090, Aug. 2021.

[129] H. Xu, L. Zhang, Y. Sun, and C.-L. I, "BE-RAN: Blockchain-enabled open RAN with decentralized identity management and privacy-preserving communication," 2021, *arXiv:2101.10856*.

[130] S. Raju, S. Boddepalli, S. Gampa, Q. Yan, and J. S. Deogun, "Identity management using blockchain for cognitive cellular networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[131] H. van der Linden, D. Kalra, A. Hasman, and J. Talmon, "Inter-organizational future proof EHR systems. A review of the security and privacy related issues," *Int. J. Med. Inform.*, vol. 78, no. 3, pp. 141–160, 2009.

[132] H. Li, Y. Dai, and X. Lin, "Efficient e-health data release with consistency guarantee under differential privacy," in *Proc. 17th Int. Conf. E-health Netw., Appl. Services (HealthCom)*, Oct. 2015, pp. 602–608.

[133] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, Apr. 2017.

[134] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 180–184.

[135] P. Maymounkov and D. Mazières, "Kademlia: A peer-to-peer information system based on the XOR metric," in *Proc. Int. Workshop Peer Peer Syst.*, vol. 2429, 2002, pp. 53–65.

[136] J. Dean and S. Ghemawat. *LevelDB-Fast Key-Value Storage Library*. Accessed: Jan. 4, 2022. [Online]. Available: https://github.com/google/leveldb

[137] A. F. Hussein, N. Arunkumar, G. Ramírez-González, E. Abdulhay, J. M. R. Tavares, and V. H. C. de Albuquerque, "A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform," *Cogn. Syst. Res.*, vol. 52, pp. 1–11, Dec. 2018.

[138] B. Sharma, R. Halder, and J. Singh, "Blockchain-based interoperable healthcare using zero-knowledge proofs and proxy re-encryption," in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2020, pp. 1–6.

[139] Y. Ren, F. Zhu, J. Qi, J. Wang, and A. K. Sangaiah, "Identity management and access control based on blockchain under edge computing for the industrial Internet of Things," *Appl. Sci.*, vol. 9, no. 10, pp. 1–16, 2019.

[140] P. Mell, J. Dray, and J. Shook, "Smart contract federated identity management without third party authentication services," 2019, *arXiv:1906.11057*.

[141] J. Alsayed Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, and K. Dahal, "DNS-IdM: A blockchain identity management system to secure personal data sharing in a network," *Appl. Sci.*, vol. 9, no. 15, p. 2953, Jul. 2019.

[142] C. Lin, D. He, X. Huang, M. K. Khan, and K.-K. R. Choo, "A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems," *IEEE Access*, vol. 6, pp. 28203–28212, 2018.

[143] T. Hamer, K. Taylor, K. S. Ng, and A. Tiu, "Private digital identity on block chain," in *Proc. CEUR Workshop*, vol. 2599, 2019, pp. 1–7.

[144] J.-H. Lee, "BIDaaS: Blockchain based ID as a service," *IEEE Access*, vol. 6, pp. 2274–2278, 2017.

[145] K. O. Asamoah, H. Xia, S. Amofa, O. I. Amankona, K. Luo, Q. Xia, J. Gao, X. Du, and M. Guizani, "Zero-chain: A blockchain-based identity for digital city operating system," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10336–10346, Oct. 2020.

[146] Y. Borse, C. Anushka, P. Deepti, and A. Purnima, "Anonymity: A secure identity management using smart contracts," in *Proc. Int. Conf. Sustain. Comput. Sci., Technol. Manag. (SUSCOM)*. Rajasthan, India: Amity Univ., 2019.

[147] I. Damgård, "Commitment schemes and zero-knowledge protocols," in *School Organized by the European Educational Forum*. Berlin, Germany: Springer, 1999, pp. 63–86.

[148] K. Singh, O. Dib, C. Huyart, and K. Toumi, "A novel credential protocol for protecting personal attributes in blockchain," *Comput. Electr. Eng.*, vol. 83, May 2020, Art. no. 106586.

[149] J. Lee, J. Hwang, J. Choi, H. Oh, and J. Kim, "SIMS: Self sovereign identity management system with preserving privacy in blockchain," *Cryptol. ePrint Arch.*, 2019.

[150] X. Yang and W. Li, "A zero-knowledge-proof-based digital identity management scheme in blockchain," *Comput. Secur.*, vol. 99, Dec. 2020, Art. no. 102050.

[151] D. Augot, H. Chabanne, O. Clemot, and W. George, "Transforming face-to-face identity proofing into anonymous digital identity using the bitcoin blockchain," in *Proc. 15th Annu. Conf. Privacy, Secur. Trust (PST)*, Aug. 2017, pp. 25–34.

[152] Z. Gao, L. Xu, G. Turner, B. Patel, N. Diallo, L. Chen, and W. Shi, "Blockchain-based identity management with mobile device," in *Proc. 1st Workshop Cryptocurrencies Blockchains Distrib. Syst.*, Jun. 2018, pp. 66–70.

[153] V. Odelu, "IMBUA: Identity management on blockchain for biometrics-based user authentication," in *Proc. Int. Congr. Blockchain Appl.* Cham, Switzerland: Springer, 2019, pp. 1–10.

[154] J. S. Hammudoglu, J. Sparreboom, J. I. Rauhamaa, J. K. Faber, L. C. Guerchi, I. P. Samiotis, S. P. Rao, and J. A. Pouwelse, "Portable trust: Biometric-based authentication and blockchain storage for self-sovereign identity systems," 2017, *arXiv:1706.03744*.

[155] P. Fan, Y. Liu, J. Zhu, X. Fan, and L. Wen, "Identity management security authentication based on blockchain technologies," *I. J. Netw. Secur.*, vol. 21, no. 6, pp. 912–917, 2019.

[156] W. Ao, S. Fu, C. Zhang, Y. Huang, and F. Xia, "A secure identity authentication scheme based on blockchain and identity-based cryptography," in *Proc. IEEE 2nd Int. Conf. Comput. Commun. Eng. Technol. (CCET)*, Aug. 2019, pp. 90–95.

[157] M. Al-Bassam, "SCPKI: A smart contract-based PKI and identity system," in *Proc. ACM Workshop Blockchain, Cryptocurrencies Contracts*, Apr. 2017, pp. 35–40.

[158] S. Hong and H. Kim, "Vaultpoint: A blockchain-based SSI model that complies with OAuth 2.0," *Electron.*, vol. 9, no. 8, pp. 1–20, 2020.

[159] E. D. Hardt, *The OAuth 2.0 Authorization Framework*, document RFC 6749, Internet Eng. Task Force, 2012, pp. 1–76.

[160] B. Faber, G. C. Michelet, N. Weidmann, R. R. Mukkamala, and R. Vatrapu, "BPDIMS: A blockchain-based personal data and identity management system," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, 2019, pp. 6855–6864.

[161] S. Friebe, I. Sobik, and M. Zitterbart, "DecentID: Decentralized and privacy-preserving identity storage system using smart contracts," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun., 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 37–42.

[162] S. Gao, Q. Su, R. Zhang, J. Zhu, Z. Sui, and J. Wang, "A privacy-preserving identity authentication scheme based on the blockchain," *Secur. Commun. Netw.*, vol. 2021, pp. 1–10, Jun. 2021.

[163] T. Zhou, X. Li, and H. Zhao, "EverSSDI: Blockchain-based framework for verification, authorisation and recovery of self-sovereign identity using smart contracts," *Int. J. Comput. Appl. Technol.*, vol. 60, no. 3, pp. 281–295, 2019.

[164] B. Zhou, H. Li, and L. Xu, "An authentication scheme using identity-based encryption & blockchain," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2018, pp. 556–561.

[165] R. Soltani, U. Trang Nguyen, and A. An, "A new approach to client onboarding using self-sovereign identity and distributed ledger," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1129–1136.

[166] Y. Zhong, M. Zhou, J. Li, J. Chen, Y. Liu, Y. Zhao, and M. Hu, "Distributed blockchain-based authentication and authorization protocol for smart grid," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–15, Apr. 2021.

[167] N. Kaaniche and M. Laurent, "A blockchain-based data usage auditing architecture with enhanced privacy and availability," in *Proc. IEEE 16th Int. Symp. Netw. Comput. Appl. (NCA)*, Oct. 2017, pp. 1–5.

[168] A. G. Abbasi and Z. Khan, "VeidBlock: Verifiable identity using blockchain and ledger in a software defined network," in *Proc. Companion Proc. the10th Int. Conf. Utility Cloud Comput.*, Dec. 2017, pp. 173–179.

[169] S. Chari, G. Hasini, A. Kundu, K. K. Singh, and D. Su, "Protection of confidentiality, privacy and financial fairness in a blockchain based decentralized identity management system," U.S. Patent 10 715 317, Jul. 14, 2020.
[170] V. K. Madisetti and A. Bahga, "Method and system for identity and access management for blockchain interoperability," Patent Appl. 15 830 099, Oct. 4, 2018.
[171] N. S. Hyun, H. S. Chae, S. H. Kim, K. J. Kim, M. S. Yang, and Y. M. Seo, "Blockchain-based digital identity management method," U.S. Patent 10 992 478, Apr. 27, 2021.
[172] A. Ebrahimi, "Identity management service using a blockchain providing certifying transactions between devices," U.S. 9 722 790 B2, May 9, 2017.
[173] C. Dannen, *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*. Berkeley, CA, USA: Apress, 2017, pp. 1–185.
[174] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2017.
[175] F. Li and B. McMillin, *A Survey on Zero-Knowledge Proofs*, 1st ed., vol. 94. Amsterdam, The Netherlands: Elsevier, 2014.
[176] X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie, and X. Peng, "A survey on zero-knowledge proof in blockchain," *IEEE Netw.*, vol. 35, no. 4, pp. 198–205, Jul. 2021.
[177] R. Perlman, "An overview of PKI trust models," *IEEE Netw.*, vol. 13, no. 6, pp. 38–43, Dec. 1999.
[178] D. Maldonado-Ruiz, J. Torres, and N. El Madhoun, "3BI-ECC: A decentralized identity framework based on blockchain technology and elliptic curve cryptography," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 45–46.
[179] P. Garcia, "Biometrics on the blockchain," *Biometric Technol. Today*, vol. 2018, no. 5, pp. 5–7, May 2018.
[180] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Appl. Cryptograph. Techn.*, 1984, pp. 47–53.
[181] S. Nayak, N. C. Narendra, A. Shukla, and J. Kempf, "Saranyu: Using smart contracts and blockchain for cloud tenant management," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2018, pp. 857–861.
[182] A. S. Sani, D. Yuan, K. Meng, and Z. Y. Dong, "Idenx: A blockchain-based identity management system for supply chain attacks mitigation in smart grids," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, 2020, pp. 1–5, doi: 10.1109/PESGM41954.2020.9281929.
[183] X. Jiang, M. Liu, C. Yang, Y. Liu, and R. Wang, "A blockchain-based authentication protocol for WLAN mesh security access," *Comput. Mater. Contin*, vol. 58, no. 1, pp. 45–59, 2019.
[184] S. Kumar, S. K. Singh, A. K. Singh, S. Tiwari, and R. S. Singh, "Privacy preserving security using biometrics in cloud computing," *Multimedia Tools Appl.*, vol. 77, no. 9, pp. 11017–11039, May 2018.
[185] W. Ao, S. Fu, C. Zhang, Y. Huang, and F. Xia, "A secure identity authentication scheme based on blockchain and identity-based cryptography," in *Proc. IEEE 2nd Int. Conf. Comput. Commun. Eng. Technol. (CCET)*, Aug. 2019, pp. 90–95.
[186] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019.
[187] T. K. Agrawal, V. Kumar, R. Pal, L. Wang, and Y. Chen, "Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry," *Comput. Ind. Eng.*, vol. 154, Apr. 2021, Art. no. 107130.
[188] M. van Hilten, G. Ongena, and P. Ravesteijn, "Blockchain for organic food traceability: Case studies on drivers and challenges," *Frontiers Blockchain*, vol. 3, pp. 1–13, Sep. 2020.
[189] A. S. Omar and O. Basir, "Smart phone anti-counterfeiting system using a decentralized identity management framework," in *Proc. IEEE Can. Conf. Elect. Comput. Eng. (CCECE)*, 2019, pp. 1–5, doi: 10.1109/CCECE.2019.8861955.
[190] L. Zhu, Y. Wu, K. Gai, and K.-K. R. Choo, "Controllable and trustworthy blockchain-based cloud data management," *Future Gener. Comput. Syst.*, vol. 91, pp. 527–535, Feb. 2019.
[191] L. W. D. C. Jayabodhi, C. Rajapakse, and J. M. D. Senanayake, "Minimization of fraudulent activities in land authentication through blockchain-based system," in *Proc. Int. Res. Conf. Smart Comput. Syst. Eng. (SCSE)*, Sep. 2020, pp. 68–74.
[192] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang, "Digital signature scheme for information non-repudiation in blockchain: A state of the art review," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, pp. 1–15, 2020.
[193] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1977–2008, 2020.
[194] S. Kaur, S. Chaturvedi, A. Sharma, and J. Kar, "A research survey on applications of consensus protocols in blockchain," *Secur. Commun. Netw.*, vol. 2021, pp. 1–22, Jan. 2021.
[195] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, 2002.
[196] S. Alqahtani and M. Demirbas, "Bottlenecks in blockchain consensus protocols," in *Proc. IEEE Int. Conf. Omni-Layer Intell. Syst. (COINS)*, 2021, pp. 1–8, doi: 10.1109/COINS51742.2021.9524210.
[197] A. Lei, Y. Cao, S. Bao, D. Li, P. Asuquo, H. Cruickshank, and Z. Sun, "A blockchain based certificate revocation scheme for vehicular communication systems," *Future Gener. Comput. Syst.*, vol. 110, pp. 892–903, Sep. 2020.
[198] A. Patel, N. Shah, T. Limbasiya, and D. Das, "VehicleChain: Blockchain-based vehicular data transmission scheme for smart city," in *Proc. IEEE Int. Conf. Syst., Man Cybern. (SMC)*, Oct. 2019, pp. 661–667.
[199] M. Aydar, S. Ayvaz, and S. C. Cetin, "Towards a blockchain based digital identity verification, record attestation and record sharing system," 2019, *arXiv:1906.09791*.
[200] A. Jabbar and S. Dani, "Investigating the link between transaction and computational costs in a blockchain environment," *Int. J. Prod. Res.*, vol. 58, no. 11, pp. 3423–3436, Jun. 2020.
[201] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic literature review of challenges in blockchain scalability," *Appl. Sci.*, vol. 11, no. 20, p. 9372, Oct. 2021.
[202] M. Nuss, A. Puchta, and M. Kunz, "Towards blockchain-based identity and access management for Internet of Things in enterprises," in *Proc. Int. Conf. Trust Privacy Digit. Bus.*, 2018, pp. 167–181.
[203] M. Nuss, A. Puchta, and M. Kunz, *Towards Blockchain-Based Identity and Access Management for Internet of Things in Enterprises*, vol. 11033. Cham, Switzerland: Springer, 2018.
[204] S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain inspired RFID-based information architecture for food supply chain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5803–5813, Jun. 2019.
[205] Y. Liu, Z. Fang, M. H. Cheung, W. Cai, and J. Huang, "Economics of blockchain storage," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2020, pp. 1–6, doi: 10.1109/ICC40277.2020.9148934.
[206] E. Ghosh and B. Das, "A study on the issue of blockchain's energy consumption," in *Proc. Adv. Intell. Syst. Comput.*, vol. 1065, Apr. 2020, pp. 63–75.
[207] R. Nair, S. Gupta, M. Soni, P. K. Shukla, and G. Dhiman, "An approach to minimize the energy consumption during blockchain transaction," *Mater. Today, Proc.*, pp. 1–6, Nov. 2020.
[208] S. Aggarwal and N. Kumar, "Attacks on blockchain," *Adv. Comput.*, vol. 121, pp. 399–410, May 2021.
[209] M. Bellare, C. Namprempre, and G. Neven, "Security proofs for identity-based identification and signature schemes," *J. Cryptol.*, vol. 22, no. 1, pp. 1–61, Jan. 2009.
[210] P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A sybil-resistant scalable blockchain," *Future Gener. Comput. Syst.*, vol. 107, pp. 770–780, Jun. 2020.
[211] R. J. Douceur, "The sybil attack," in *Proc. Int. Workshop Peer-Peer Syst.* Berlin, Germany: Springer, 2002, pp. 251–260.
[212] A. Rashid, A. Masood, and A. U. R. Khan, "RC-AAM: Blockchain-enabled decentralized role-centric authentication and access management for distributed organizations," *Cluster Comput.*, vol. 24, no. 4, pp. 3551–3571, Dec. 2021.
[213] Z. Li, "A verifiable credentials system with privacy-preserving based on blockchain," *J. Inf. Secur.*, vol. 13, no. 2, pp. 43–65, 2022.
[214] R. Greene and M. N. Johnstone, "An investigation into a denial of service attack on an Ethereum network," in *Proc. 16th Austral. Inf. Secur. Manage. Conf.*, 2018, pp. 90–96.
[215] A. Averin and O. Averina, "Review of blockchain technology vulnerabilities and blockchain-system attacks," in *Proc. Int. Multi-Conf. Ind. Eng. Modern Technol. (FarEastCon)*, Oct. 2019, pp. 1–6.
[216] E. Conrad, S. Misenar, and J. Feldman, "Identity and access management (controlling access and managing identity)," in *CISSP Study Guide Domain-5*, 3rd ed., vol. 5. Amsterdam, The Netherlands: Elsevier, 2016, pp. 55–66.

[217] J. Kwon and E. Buchma, "Cosmos: A network of distributed ledgers," 2016. [Online]. Available: https://cosmos.network/whitepaper
[218] R. Qin, Y. Yuan, and F.-Y. Wang, "Blockchain-based knowledge automation for CPSS-oriented parallel management," *IEEE Trans. Computat. Social Syst.*, vol. 7, no. 5, pp. 1180–1188, Oct. 2020.
[219] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, "Performance optimization for blockchain-enabled industrial Internet of Things (IIoT) systems: A deep reinforcement learning approach," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3559–3570, Jun. 2019.
[220] C.-T. Tseng and S. S. C. Shang, "Exploring the sustainability of the intermediary role in blockchain," *Sustainability*, vol. 13, no. 4, p. 1936, Feb. 2021.
[221] T. M. Tan, P. Ahokangas, J. Salo, V. Seppanen, and P. Sandner, "Revealing the disintermediation concept of blockchain technology: How intermediaries gain from blockchain adoption in a new business model," in *Impact of Globalization and Advanced Technologies on Online Business Models*. Hershey, PA, USA: IGI Global, 2021, pp. 88–102.
[222] M. Brengel and C. Rossow, "Identifying key leakage of bitcoin users," in *Proc. Int. Symp. Res. Attacks, Intrusions, Defenses*, 2018, pp. 623–643.
[223] Q. Feng, D. He, Z. Liu, D. Wang, and K. K. R. Choo, "Distributed signing protocol for IEEE P1363-compliant identity-based signature scheme," *IET Inf. Secur.*, vol. 14, no. 4, pp. 443–451, 2020.
[224] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu, "Privacy preservation in permissionless blockchain: A survey," *Digit. Commun. Netw.*, vol. 7, no. 3, pp. 295–307, Aug. 2021.
[225] M. Wohrer and U. Zdun, "Smart contracts: Security patterns in the Ethereum ecosystem and solidity," in *Proc. Int. Workshop Blockchain Oriented Softw. Eng. (IWBOSE)*, Mar. 2018, pp. 2–8.
[226] I. Bentov, C. Lee, and A. Mizrahi, "Proof of activity?: Extending bitcoin's proof of work via proof of stake," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 9–11, 2014.
[227] J. Bou Abdo, R. El Sibai, and J. Demerjian, "Permissionless proof-of-reputation-X: A hybrid reputation-based consensus algorithm for permissionless blockchains," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 1, Jan. 2021, Art. no. e4148.

MD. RAYHAN AHMED received the Bachelor of Science (B.Sc.) degree from the Ahsanullah University of Science and Technology (AUST), Dhaka, Bangladesh, in 2015, and the Master of Science (M.Sc.) degree in communication engineering from the United International University (UIU), Dhaka, in 2021. He is currently serving as an Assistant Professor with the Department of Computer Science and Engineering, UIU. Before entering the university faculty profession, he worked as a Software Engineer at Brac IT Services, Dhaka. His research interests include biomedical data analysis, image processing, image segmentation, speech synthesis, machine learning, brain–computer interface, pattern recognition, network security, software-defined networks, and blockchain.

A. K. M. MUZAHIDUL ISLAM (Senior Member, IEEE) received the M.Sc. degree in computer science and engineering from the Kharkiv National University of Radio Electronics, Ukraine, and the D.Eng. degree in computer science and engineering from the Nagoya Institute of Technology, Japan. From January 2011 to January 2017, he worked as a Senior Lecturer with the Malaysia-Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia (UTM), Malaysia. He worked as an Associate Professor and the Head of the Department of Computer Science and Engineering (CSE), University of Liberal Arts Bangladesh (ULAB). He is currently a Professor with the CSE Department, United International University (UIU), Bangladesh. He has published 90 international research publications (including two book chapters, 26 peer-reviewed indexed journals, and 62 conference papers). He has secured several national and international research grants and supervised many B.Eng., master's, and Ph.D. students through their graduation. He is actively involved with BAETE's accreditation process. His research interests include network architecture, communication protocol, cognitive radio networks, wireless sensor networks, the IoT, cloud computing, healthcare, and smart farming. He is a fellow of IEB (FIEB). He is a Chartered Engineer (C.Eng.). He has served as the Program Chair for ICAICT 2016 and 2020, ETCCE 2020, and 2021 international conferences. He has also served as the Secretariat for the ICaTAS 2016 International Conference, Malaysia, and the 7th AUN/SEED-Net 2014 International Conference on EEE.

SWAKKHAR SHATABDA received the B.Sc. degree in computer science and engineering from the Bangladesh University of Engineering and Technology (BUET), in 2007, and the Ph.D. degree from the Institute for Integrated and Intelligent Systems (IIIS), Griffith University, in 2014. His thesis is titled "Local Search Heuristics for Protein Structure Prediction." He worked as a Graduate Researcher at the Queensland Research Laboratory, NICTA, Australia. He is currently a Professor at the Computer Science and Engineering Department, United International University, Dhaka, Bangladesh. Prior to entering the teaching line, he worked as a Software Engineer at Vonair Inc., Dhaka. He has a number of quality publications in both national and international conferences and journals. His research interests include bioinformatics, optimization, search and meta-heuristics, data mining, constraint programming, approximation algorithms, and graph theory.

SALEKUL ISLAM (Senior Member, IEEE) received the Ph.D. degree from the Computer Science and Software Engineering Department, Concordia University, in June 2008, under the supervision of Dr. J. William Atwood. He is currently a Professor and the Head of the CSE Department, United International University, Bangladesh. Previously, he worked as an FQRNT Postdoctoral Fellow at the Énergie, Matériaux et Télécommunications (EMT) Centre, Institut National de la Recherche Scientifique (INRS), Montréal, Canada. His research interests include future internet architecture, blockchain, edge cloud, software-defined networks, multicast security, security protocol validation, and machine learning and AI. He is serving as an Associate Editor for IEEE Access and *Frontiers in High Performance Computing* journals.