applied sciences

MDPI

Systematic Review

Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology: A Systematic Review

Haifa Alanzi * and Mohammad Alkhatib *

Department of Computer Science, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University, Riyadh 11564, Saudi Arabia
* Correspondence: haifaalanzi1995@gmail.com (H.A.); mohkhatib83@gmail.com (M.A.)

Abstract: An identity management system (IDMS) manages and organizes identities and credentials information exchanged between users, identity providers (IDPs), and service providers (SPs) to ensure confidentiality and enhance privacy of users' personal data. Traditional or centralized IDMS rely on a third party to store a user's personal information, authenticate the user, and organize the entire process. This clearly constitutes threats to the privacy of the user, in addition to other issues, such as single point of failure (SPOF), user tracking, and data availability issues. Blockchain technology has many useful features that can contribute to solving traditional IDMS issues, such as decentralization, immutability, and anonymity. Blockchain represents an attractive solution for many issues related to traditional IDMS, including privacy, third-party control, data leakage, and SPOF, supported by Distributed Ledger Technology (DLT) security features and powerful smart contracts technology. The current study presents a systematic literature review and analysis for recently proposed solutions that adopt the traditional centralized approach, as well as solutions based on blockchain technology. The study also aims to provide a deep understanding of proposed IDMS solutions and best practices, and highlight the research gaps and open issues related to IDMSs and users' privacy. In particular, the current research focuses on analyzing the blockchain-based solutions and illustrating their strengths and weaknesses, as well as highlighting the promising blockchain technology framework that can be utilized to enhance privacy and solve security issues in a centralized IDMS. Such a study is an important step towards developing efficient solutions that address the pressing needs in the field.

Keywords: identity management; blockchain; distributed ledger technology; self-sovereign identity; privacy

Citation: Alanzi, H.; Alkhatib, M. Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology: A Systematic Review. *Appl. Sci.* **2022**, *12*, 12415. https://doi.org/10.3390/app122312415

Academic Editor: Gianluca Lax

Received: 6 October 2022
Accepted: 26 November 2022
Published: 4 December 2022

1. Introduction

Today, digital identities are essential for users on the internet to obtain services from electronic service providers (SPs). Digital identity represents the user's personality in the digital world and carries their necessary data that allows the identity holder to access various resources on the internet provided by SPs [1]. Managing and protecting the user's identity, as well as related transactions and data, are critical tasks that need to be considered. The IDMS is an organizational process that aims to achieve these tasks and makes it easy for authorized users to access required services through their digital identity credentials. In addition, IDMS seeks to provide necessary security services, such as privacy, confidentiality, and availability, to counter recently emerged cyberattacks and threats. There are three general basic parties in IDMS: the identity provider (IDP), the SP (or relying party RP), and the user [2]. The digital identity of the user is created by the IDP, as they are responsible for creating the digital identity and certifying it for the SP; the user needs to obtain a service from the SP, which provides the necessary authentication for the user. The SP provides the user with various resources after verifying their identity through the IDP. An IDMS becomes essential for modern applications and e-transactions to organize and manage

identity information and credentials between the involved parties; the user, the SP, and the IDP. Furthermore, the IDMS is required to control the process of user authorization and support the role-based access system. The IDMS can be realized using centralized and decentralized approaches.

A centralized IDM approach is the process of controlling and managing user identities and their relations using other central parties: an IDP and an SP. It is based on two primary operations, authentication and authorization, to provide an identity verification process and to increase access control (AC) security. However, a centralized IDMS suffers from potential risks that threaten users' privacy and decrease system transparency because of its reliance on centralization in controlling and managing users' data. The major risks associated with a centralized IDMS include issues related to user privacy, such as user behavior monitoring, and third-party control, in addition to issues relevant to the availability of data, such as the single point of failure (SPOF) [3].

The decentralized blockchain infrastructure is one of the most important proposed solutions to solve the centralized IDMS issue approaches, as a result of its powerful security features and promising technologies. The blockchain has multiple features that contribute to improving the problems of the current central systems, such as the features of distribution, peer-to-peer (P2P), immutability, and others. Two important concepts were launched in 2013 that served to transform IDMs from centralization to decentralization, Ethereum, and the smart contract. In smart contracts, transactions between parties can be conducted and tasks can be performed without the involvement of a third party, since it is a self-executing program that runs whenever the conditions are met. There are many features of blockchain technology that can enhance user privacy. Decentralization is the most important. In addition, avoiding complete dependence on a central authority reduces the risk of a SPOF. By using the blockchain, the user is protected from relying on third parties, and therefore, the possibility of tracking and studying their behavior is eliminated. However, despite the blockchain's many advantages, it still faces some challenges, such as its scalability.

A study comparing the various solutions offered by this technology is important as the blockchain offers multiple features that can help solve the problems associated with centralizing identity management. Several issues have been addressed in the current systems in which blockchain technology has been applied, as well as addressing research that has compared and uncovered the most suitable method of centralized identity management using various types of blockchain.

This research presents a systematic literature review of recent studies that have proposed blockchain-based solutions for centralized IDMSs across different domains. The aim of this study is to explore blockchain privacy and security solutions, study and compare those solutions, and analyze the results to highlight the current research gaps and best practices. These efforts seek to develop efficient blockchain-based solutions for IDMSs which represent an essential need for the current internet-based applications and businesses.

The remaining sections of this paper are as follows. Section 2: Background; Section 3: Literature Review; Section 4: Method; Section 5: Result and Discussion; and finally, the conclusion is outlined in Section 6.

2. Background

2.1. Overview of IDMSs

Digital identities are needed to identify users when they request access to digital resources. To manage these digital identities, in addition to related information and credentials, an efficient IDMS is required. There are many identity management models that have been created and categorized based on the use of identity and the need for a cross-domain, such as an isolated user identity model, a federated identity model, and a user-centric model [1].

2.1.1. The Isolated User Identity Model (SILO) or Centralized Model

IDMSs have undergone multiple stages of development. First, there was the Isolated User Identity (SILO) model, which is the cornerstone and the most simple model most widely used [4]. It is based on identity management between only two parties, the IDP and the user. The IDP in this system plays the role of the SP, as it allows the user to create a digital identity to obtain services provided in a specific field, which means that the user needs to create several digital identities to obtain services in multiple domains [5]. This is perhaps a major defect in this model owing to the difficulty of managing multiple identities by the user, in addition to full dependence on the IDP, which may cause a violation of user privacy, such as user movements tracking.

2.1.2. Federated Identity Model

Another IDM was then created, which is Federated IDMS [1]. It differs from the previous system as it is based on three parties instead of two: the IDP, the SP, and the user [6]. The IDP here is the responsible party for user identity creation, authentication, and necessary credentials. In this model, the user depends on the IDP to issue credentials related to their identity and authenticate them to the SP. Therefore, there must be an element of trust between the IDP and the SP (Circle of Trust principle), which means that for every IDP in the system, there is a group of trusted SPs that the user can obtain services from [2,4]. Full dependence on the IDP, in addition to being fully informed of all user behaviors and relationships, is a threat to user privacy and may lead to the SPOF. These are serious problems in the centralized identity management approach that depends on a central party to provide the required identity creation and authentication services; the IDP.

2.1.3. User-Centric Model

This model is also referred to as the Open Trust Model, as all parties in the system are required to trust each other [1]. In this model, the user can select the attributes and credentials to be sent, in addition to the ability of choosing the IDP. It is very similar to the federated model, and it also has the same privacy concerns. The second law of identity (justifiable parties) is not satisfied in this model and the sharing policy with SP can be defined by the user, but it is still under the control of the IDP [5]. User privacy is violated in this model because of the IDP control.

2.1.4. Self-Sovereign Identity Model (SSI)

The abovementioned IDM model requires full dependence on a third party, the IDP, to manage and control the identity, in addition to providing the credentials necessary for authentication. This represents a clear threat to the user's privacy, as all user behavior and movements are exposed to the IDP. To raise the level of user privacy in the field of digital identities, and to find a solution to the problems associated with the user's dependence on the IDP (problems related to the centralized approaches), a model based on the principle of decentralization has appeared in the field of IDM. The adoption of a decentralized IDM approach has been instigated by many researchers to find solutions regarding the privacy and SPOF problems in the previous centralized models. The Self-sovereign Identity model (SSI) is an emerging decentralized IDMS that provides the user with the ability to control their identity, as well as its related data and transactions [7]. Unlike the three previously mentioned models of online identity, centralized, federated, and user-centric, SSI provides all three of the basic requirements, security, control, and portability. Therefore, the user is both the controller and the manager of the identity, and there are no external central control parties; reducing the hacking risk. During hacking, when the IDP obtains the data of all users who trust it, the attacker needs to individually hack each user one by one, which necessitates higher costs, more time, and more effort. To develop an efficient decentralized IDM system capable of addressing problems related to privacy, SPOF, and other security issues, an appropriate infrastructure must be made available. Distributed Ledger Technology (DLT), also called blockchain, has been proposed by numerous research

studies as an infrastructure by which to develop an IDM system and find effective solutions to the issues of security, privacy, and SPOF, as well as to give users the freedom to manage and exchange their data privately without the presence of or observation by controlling parties [5].

2.2. Blockchain

Blockchain was invented in 2008 by an unknown entity who went under the pseudonym Satoshi Nakamoto [8]. Blockchain technology is a technology that is built on several technologies, which include: blockchain data structure, public key infrastructure PKI, distributed ledger technology DLT, and a consensus mechanism [9]. Blockchain technology has many characteristics that have contributed to its widespread adoption and significance today, the most important of them being the decentralization feature. Using decentralization correctly is one of the most important steps towards solving the SPOF problem, which poses one of the biggest challenges to centralized systems. There is also a significant impact factor in the field of data protection associated with blockchain technology, since the data stored cannot be deleted or modified once it has been stored on the blockchain [10,11].

Blockchain is one of the most important decentralized technologies. It has been widely spread in the recent years and has been used in many domains, such as IOT [12–16]; supply chain [17–20]; AC and Identity Management in [21–26], cloud IDM in [27], ad-hoc network (VANET) in [28–30], healthcare in [31–33], internet of connected vehicles in [34,35], and even for the undirected graph authentication, as discussed in [36]. Blockchain is a type of DLT which makes it very difficult to modify or hack any data and transactions stored on the blockchain platform through a secure and tamper-proof way [5]. The main components of blockchain technology are:

- A block: A block of data which has a 32-bit randomly generated number (nonce) and cryptographic hash, which is like a fingerprint of the block data. The first block of the chain is called the Genesis Block, and it does not contain a previous hash, because it is the original and the first block on the chain, and thus it is the only block with this feature [37].
- Miners: The blockchain technology requires miners to solve complex math algorithms to generate the cryptographic hash from the random nonce for each block created.
- Nodes: The nodes can be any electronic device holding all of the blockchain transactions copies.
- Chain: Group of blocks.
- Consensus protocol: Operations implementation rules.

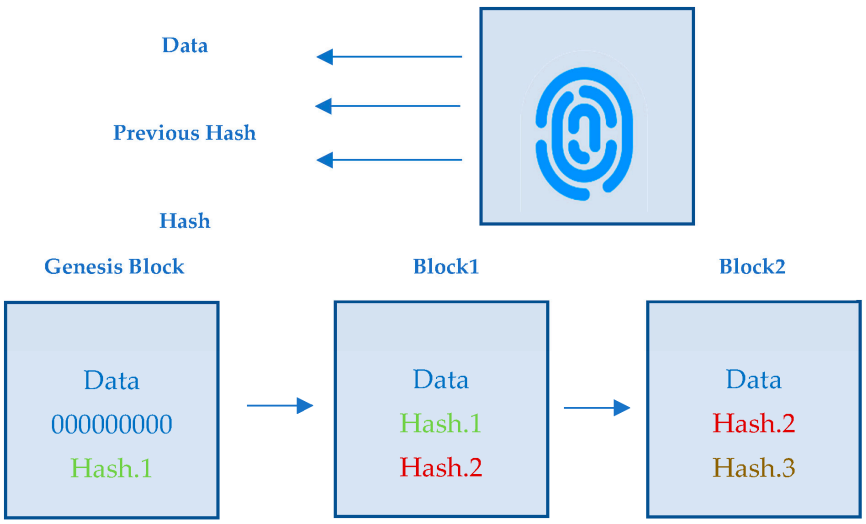
The blockchain distributes the data blocks over multiple nodes on the internet [2]. Therefore, it is working to publish and transmit data in the form of multiple blocks linked together. Each of the blocks contains the hash of the previous block, and that is why it is called a chain of blocks (blockchain) because all the blocks are cryptographically linked to each other through the hash, so if anyone tries to tamper with one of the blocks, the hash of the block will no longer match up and the chain of blocks will be invalid, which is an immutable ledger feature. Blockchain features such as decentralization, immutability, and individual control of data, help to solve the most important issues of centralized IDMs by giving the user full control of their data to increase privacy by limiting third-party control, which is the main shortcoming of centralized IDM systems. The security and transparency features avoid the central authority issue while no single entity owns the data. Another important feature is that the blocks on a blockchain cannot be modified, and that is a very important feature in the field of security as it has a major role in reducing attacks [38].

A Distributed P2P Network is one blockchain feature where each device in the network is connected to all the other devices in the same network, and each device has a copy of the blockchain. Therefore, with each new block created in the chain, a copy of the block will be sent to all the peers under a cryptographic role. This is a very important security feature where any system errors or tampering of any block will be detected because the blockchain constantly checks all its peers to make sure that there are no issues. If any of the

peers has a tampered block, the majority of the peers will compare the block and replace the tampered block with the original one. As a result of this feature, it is difficult to hack the block, since the hacker would have to tamper with more than 50% of the blocks at the same time in order to succeed [39,40]. In addition to the security features provided by blockchain technology, it eliminates the need for a third party to process transactions, and hence, supports decentralization via the use of smart contracts technology. A smart contract is a conditional transaction process in the blockchain that occurs when the condition is met (a self-executed program). Smart contracts provide many advantages, such as increasing performance, saving time, and, most importantly, increasing privacy compared to other traditional methods [41]. Smart contracts are run on many blockchain platforms such as Hyperledger Fabric, Waves, Ethereum, and NEO.

Many IDM solutions have been designed without using DLT. As a result, there have been some issues related to central authority or third-party control, as in [3,6,42–44]. On the other hand, some research attempts have proposed solutions based on blockchain technology. However, proposed blockchain-based IDM systems have certain issues related to centralization when a private blockchain is used [13]; these pertain to private BC, central authority in [45], data availability in [46], and key management issues in [47].There are many challenges in the field of user privacy in central identity management, such as relying on the third party to create, verify, and authenticate the identity and its attributes, in addition to the increased risk of user tracking, because the user needs the third party every time they want to obtain a service from the service provider. The SPOF is also one of the most important challenges facing central identity management.

Integrating blockchain with identity management has many promising features that may help in solving and improving the system quality and user privacy. Decentralization, transparency, and immutability are among the most important characteristics that support this improvement, but there are also challenges that still need to be addressed, such as scalability of the blockchain system.



3. Literature Review

The current paper aims to present a comprehensive discussion and review for both traditional IDM systems that adopt the centralized approach, and the blockchain-based IDMSs that rely on the decentralized DLT to improve privacy and achieve self-sovereign identity concepts.

3.1. Traditional IDMSs

In [3], a study concerning Digital Identity and IDM Technologies, the author illustrated a variety of technologies used in the field of IDM. Among the several competing standards in the IDM field, the security assertion markup language (SAML) was the only applicable

choice, as it had a high level of acceptance at that time. This is because it was part of the solution to the problem of single sign-on. Later, another technology emerged and received some attention in the community, called the WS-Federation. As users need to have multiple identities for different service providers, the multiple identities used can cause a degree of inconvenience to the user in terms of managing them. The author concluded that both are similar in functionality but had different names: IDP and the service provider in SAML; security token service and relying party in WS-Federation.

Microsoft CardSpace is a claim-based IDM system proposed by Microsoft to satisfy the seven laws of identity. It gives the user the right to control their digital identities and choose the card after they have completed the SP policy through the identity selector. The identity selector is the intermediary between the user, the IDP, and the SP, as they retrieve the security policy after the user picks the card and completes the user authentication with the IDP on behalf of the user, and then forwards the security token to the SP to log the user in after they have received it from the IDP. The system guarantees the integrity of security tokens through an xml-signature and preserves the confidentiality of the IDP and SP security policies by making transactions over an SSL/TLS channel. However, this model violates user privacy, as it requires presenting the user credentials to the identity selector. Another drawback for this model is that the user must carry out the authentication step every time before a token is issued [42].

Another research study, this time conducted by the Liberty Alliance project, was a single sign-on federated IDMS proposed in 2001. The project proposed several frameworks: the identity federation framework (ID-FF), the identity web services framework (ID-WSF), the identity service interface specification (ID-SIS), the Liberty identity assurance framework (LIAF), and the identity governance framework (IGF). The authentication and authorization frameworks were separated in the system. The user in the Liberty Alliance system was monitored by the IDP, as they knew who all the services providers were accessed by the user, which violated user privacy [6].

In [48], researchers introduced Shibboleth, which is a Federated IDMS, and its single sign-on framework, but it does not support single sign-off. The proposed system tries to increase user privacy by using a short-term, random ID to maintain anonymity. Unlike the previous project, the authentication and authorization frameworks can be combined. In Shibboleth, IDP discovery is performed by the SP using the WAYF technique, which can increase the risks to the user by connecting with a fake IDP, redirecting them via a malicious SP. This also increased the risk of stolen credentials.

The OpenID system is an open-source IDMS, released in 2005. It supports SSO and uses the concept of a global identifier to enable the user to contact any OpenID-enabled SP. The system does not use any proof of rightful possession, which makes it vulnerable to the risk of credential theft. In addition, it may create other risks such as directing the user to a fake IDP via a malicious SP, and the risk of a man-in-the-middle (MITM) attack [44].

Reference [43] suggested two proposed solutions in the implementation layer to improve the level of authentication with the user in a claim-based IDMS. A proof-of-authenticity method and challenge-response method appeared as suggested solutions to solve the problem of the malicious IDP, which may cause considerable damage to the SP and the user. The authors suggested a proof-of-authenticity method as the first solution, which uses an additional authentication layer through creating a random secret value by the SP, and then sends it to the user (known only to the user and the SP) after each complete authentication. The challenge-response method is the second proposed solution where the user has to accept a challenge sent by the SP, and they must respond with the expected result computed by using a private signature key or shared secret key between the SP and the user. Both proposed solutions had a positive impact on solving the problem studied by the authors, where, in addition to enhancing the user authentication, they also increased the level of privacy in the claim-based IDM system.

The previously reviewed studies had many features that improve the quality and performance of the system, but they also had many challenges that violate user privacy,

such as data disclosure [42], user monitoring and increasing the risk of credentials being stolen [6], a man-in-the-middle attack, and fake parties [44]. These were in addition to the SPOF, which is one of the main issues associated with the centralized IDM approach.

The next section presents state-of-the-art studies that adopted a decentralized approach for IDMS using the blockchain technology.

3.2. Blockchain-Based IDMSs

In [13], the authors presented a new IDM approach based on a private blockchain, which aims to provide an efficient and simple protocol that meets all the needs of Internet of Things (IOT) organizations. Researchers implemented a Hyper-ledger Fabric for the smart homes model and wrote the chain codes using Golang language. The main functions of the IDM systems are split into three phases to allow simultaneous execution: identity registration, identity verification, and identity revocation; the three phases employed smart contracts to interact with the blockchain. The author discussed how this approach would enhance IOT entities communications by including a consortium membership service and identity management protocol. The author chose to use a private blockchain in the model to achieve more security and better scalability; however, in terms of characteristics, it was more like centralization than decentralization, and that increased the risk of SPOF and central authority issues.

The authors in [49] developed a decentralized IDM system prototype using the Hyperledger Indy blockchain as a proof-of-concept in the public transportation sector, based on self-sovereign identity principles. The proposed system can reduce the need for using multiple travel cards for the people who travel frequently and who use several modes of transportation within multiple jurisdictions. The system aims to give the users full identity control by creating a direct identity layer based on the principles of decentralization using a blockchain-based IDM system to provide a Single European Transport for users. The proposed system will provide the ability to create many decentralized identifiers for any person, in addition to creating a key pair for each user so they can securely share the data.

In [45], researchers proposed a blockchain-based decentralized IDM system for the public sector in South Korea by providing a mobile application by which to create electronic identity cards, issued and managed by a national central authority. The user stores their driver licenses on their device and verifies their identity through the app by using a one-time QR code. The client server in the system is developed by using Hyper-ledger Fabric V1.0 to increase the privacy level. Amazon web service (AWS) is used in the system to provide a faster process and increase efficiency. Data for any identity in the system is linked to a central government agency in South Korea to complete the identification process. User data is stored in a database in the form of keys and values paired on a hash map, in addition to the chain code. The developer also used a modern user interface to make users feel more comfortable using the system. The application is very effective in using blockchain, but it appears to be centralized, even with blockchain, as the national central authority is the data manager, and license requirement in the verification process might be a disadvantage because such an application is not appropriate for many e-commerce systems or for obtaining online services as there will be licenses or other types of formal document involvement.

Authors of [46] used a smart contract to design a cross-domain self-sovereign identity management system. The system contains three types of smart contracts; each one built to perform a specific function. The services smart contract SSC is the first contract and the basis contract in the system which controls the publishing of a user identity contract, and it is created and published when the SP joins the system. The second is the identity smart contract ISC, which is requested by the user from the SP after they have been identified and verified, and their address is recorded in the SSC. The ISC is controlled by the user after it is published. The Recovery Smart Contract (RSC) is also created at the same time. The RSC is automatically created for each ISC to give the user the ability to recover their lost password from a list of friends. The system, as proposed by the designer, performs better

compared to three other systems using the same concept, but it also has a limitation in that it uses the address of the ISC as a universal unique identifier UUID, which is not readable by users, and, as the system stores the full attributes information in the user device, that will decrease the availability of information when the user is offline.

In the study presented in [47], a hybrid methodology was proposed as a part of the Impilo project for data management in healthcare by combining a central database and decentralized infrastructure "blockchain". The new approach tries to create ownership and management of data on the patient side to increase security of electronic health records and keep it shareable at the same time. Patient information is stored on a central database during the validation process, and the transaction is stored on the blockchain. The system operation begins by logging into the Impilo app and storing the registration information in a new file, and then communicating with the DB to store the medical information. The blockchain will generate a new hash, communicate with both sides, and then store the transaction details on the chain if the verification process is correctly completed. In this approach, the decryption key of medical information in a database is the user login password; so, if an attacker knows the user login password, they will have access to all the user information, and this decreases the security of the database.

In [50], researchers proposed a framework to solve the centralized problem of access control and its related privacy and ethical issues, and to give users full control of their IOT devices. The proposed framework is based on two main concepts: a blockchain and a machine learning algorithm. The researchers addressed two problems in IoT environment access control: centralized access control (AC) and security policy management. The proposed framework distributes the security policy (a set of guidelines and security rules) in the blockchain by using a smart contract instead of storing it in a server, as in a traditional AC, and improves it by using an online learning mechanism of machine learning algorithms to solve the problem of a non-contextual security policy. An online learning machine type is used to detect any AC rules which do not satisfy the security policy, or which may lead to any security threat.

Authors in [36] used the private Ethereum network to design a cryptographic authentication scheme. The authors developed a smart contract and published it on a private chain, and then evaluated the scheme's functions by using web3j and a proof of security model. The research introduced a transitively closed undirected graph authentication (TCUGA) scheme to update the certificates by the signatory with no re-signing process needed by using a trapdoor hash function and allowing the administrator to prove the certificate relationships "even when they are not in the same equivalence class" after they are received from the signatory.

A permissioned blockchain-based IDM user authentication scheme was introduced in [33] to solve key management and authentication issues in e-health systems by using a key distributed mechanism of personal biometrics. The proposed system contains four main members: the founder, the user (U), the registration center (RC), and the medical server (MS), in addition to the smart contract that provides access control functions. It has two major mathematical problems: the computational Diffie-Hellman problem (CDHP) and the discrete logarithm problem (DLP). The proposed scheme is provided with a mutual authentication equation and achieves anonymity by making the user's identity hidden. The designer tested the proposed system and guaranteed the security requirements by using the Scyther tool, which is an automatic verification tool for security protocols.

An attempt to solve traditional banking issues by developing a blockchain-based IDM and access control (BIMAC) framework was presented in [51]. The researchers used an MVC (Model-View-Controller) structure for this purpose. The implemented framework improved user experience by creating a user login to many bank accounts without the need to remember all their accounts and passwords. The prototype applied the concept of self-sovereign identity in the open banking field and provided an efficient authentication framework.

In [28], the authors tried to solve the problem of traffic disruption caused by malicious vehicles through incorrect information propagation. As a way to maintain privacy, they suggested using a blockchain-based authentication scheme and asymmetric key encryption to secure vehicle communication. Additionally, elliptic curve cryptography was used to increase transactions pseudonymity. According to the study of [34], it has been found that when cooperating with unauthorized vehicles, it is possible to steal information, compromise privacy, and exploit a variety of threats in terms of security. The authors proposed a blockchain-based Internet of Vehicles (IoV) protocol that was developed on the Ethereum platform, to improve the privacy of vehicle data and relationships with the help of blockchain technology. However, too much IoV information stored in the blockchain will affect the system's scalability. [35] In addition, the paper discussed the increased difficulty of managing certificates for vehicular communications, along with the cost of anonymizing vehicle identities. This study proposes a blockchain-based pseudonym management solution which has the ability to reuse existing pseudonyms in order to simplify pseudonym management. Additionally, in [30], the authors attempted to enhance vehicle privacy and trust relationships. As a result of the use of blockchain technology by these authors, they proposed a blockchain-based anonymous reputation system (BARS), which is based on a reputation evaluation algorithm.

A proof-of-concept IoT identity management system for a business case scenario was implemented by the authors in [12], to ensure the integrity of the data provenance records in the organization-networked IOT resources using blockchain and smart contracts. Solidity language is used to code the proposed blockchain model and it is deployed in Kaleido.

The authors of [21] proposed a Hyperledger fabric blockchain system to enhance Modbus, one of the Industrial Internet of Things IIoT protocols that faces many security challenges, such as SPOFs. On-chain authentication and authorization are supported by the designed decentralized identity system. By providing both security and scalability for Modbus connections, it can be used in a system with more than one organization.

Self-sovereign Identity, blockchain, and Inter Planetary File technologies were used by [17] to improve food supply chains. By using SSI concepts, the study proposed a way to manage certifications throughout the supply chain. A certificate is issued by a certifying body and stored in IPFS, with only some key information being stored on the chain; verifiers need this information to verify whether a certificate is valid in the chain. To improve supply chain security, the authors in [18] also implemented a Hyperledger Fabric framework to ensure each registered device in the supply chain is tracked and to improve system security. Furthermore, reference [19] proposed a supply chain traceability system, though this proposed system tracks and validates both sides of the transaction. Additionally, reference [20] used a permissioned blockchain network in order to take advantage of smart contract features and to increase supply chain management security. The proposed framework provides the user with control over the data and increases identity protection by using cryptographic proof.

In recent years, telehealth has become a necessity, especially since the COVID-19 pandemic started. In [31], the authors addressed the problem of trusting e-health application service providers and not knowing whether they comply with regulations to ensure privacy and security. Blockchain technology was used to provide authentication and identification processes to users and service providers across a variety of health domains. A smart contract was implemented in the proposed system using Ethereum.

In edge computing, the privacy and security of user data are two of the most important factors that need to be considered. As discussed in [22], the authors used smart contracts as a means of presenting the Access Management System by using blockchain technology.

In order to improve the Internet of Things HIoT privacy, the authors in [15] proposed verifiable anonymous identity management systems (VAIM), through which they improved blockchain identity management and enhanced the unlinkability of the system by using zero-knowledge proof (ZKP) algorithms.

User privacy has been affected by third-party dependencies in identity management systems in a variety of fields, including the Internet of Things. An SPOF is also one of the most important issues resulting from third-party control. Using Hyperledger Fabric, the authors in [13] implemented a smart-home-based scenario architecture to improve the quality and efficiency of home sensors and to enhance IoT centralization issues. A proposed architecture would divide the functions of the system into three main parts: registration, authorization, and revocation. The authors tried to improve the scalability of the system by splitting the functions.

The authors in [32] attempted to solve the problem of electronic health records information being exposed, which poses a threat to the privacy of the users and those whose records are accessed. The authors implemented a proof of concept through the use of Hyperledger Fabric's permissioned blockchain technology to ensure anonymity for the EHR data and to enhance privacy for patients.

Using a DNS-like approach, the authors of [23] proposed a DNS-IDMs architecture that is implemented on Ethereum's permissioned ledger. In order to enhance the privacy of the user, users and service providers would be able to create identity attribute claims and verify them using the services of real-world identity attribute benefactors. By using blockchain transactions, users can also control and manage their identities.

There are many security challenges associated with large-scale IoT systems due to centralization concepts, such as unauthorized access requests to IoT-enabled devices, which are an issue of access control. To make the system more flexible and adaptable, reference [14] implemented a private blockchain POC prototype using Ethereum and smart contracts. BlendCAC was the name of the framework proposed by the authors.

An Ethereum-based IDM cloud protocol was proposed by [27], an improved version of CIDM (Consolidated Identity Management). The proposed protocol attempts to solve the third-party reliance problem in traditional identity management systems. Smart contracts were used in the proposed system to increase data transmission privacy and to enhance system flexibility.

The authors of [24] provided a method that allows users to sign transactions using a different Ethereum identity in order to enhance user untraceability by granting the user the right to delete their data and allow them to discard their identity afterward. The proposed method represents identity through web3js-based implementation and data erasing can be requested by the user or an end of service.

It was proposed in [25] that attribute trust could be enhanced by using an Attribute Trust-enhancing Identity Broker (ATIB) architecture in order to enhance the aggregation of system attributes by following the ten SSI principles. As part of the proposed proof of concept, the service providers role would be enhanced with the help of the protocol manager, which is the main component in the proposed architecture that will be able to support the implementation of many identities and access protocols to the system.

In [26], the authors proposed a method of integrating distributed identity provider technology (OLYMPUS) with blockchain technology while utilizing smart contract technology as a means of evolution of distributed identity provider technology. It was proposed that the proposed architecture will improve system security and enhance the privacy of users.

As a result of a combination of a cryptographic authentication scheme and blockchain technology, reference [36] proposed a transitively closed undirected graph authentication scheme (TCUGA). The proposed scheme manages vertices and edges, and it can prove the absence of any edge between two vertices.

A permissioned blockchain was used with attribute-based access control (ABAC) and an identity-based signature (IBS) in order to improve the security of an Internet of Things system [16]. In this paper, a cross-domain blockchain-based IoT access control system was proposed to address some of the challenges related to IoT systems, such as SPOFs, information leaks, and Distributed Denial of Service (DDoS).

By adopting an existing technology, the authors in [33] enhanced E-health identity authentication and solved some major security issues, including reply attack and an MITM attack. In order to provide a secure mutual authentication and key distribution system, the proposed authentication scheme is implemented in permissioned blockchains.

A fine-grained AC scheme was proposed in [29] to enhance Vehicular Ad Hoc Network (VANET) data sharing. In order to increase data sharing security and decrease SPOFs, a combination of blockchain technology, IPFS, and ciphertext-based attribute encryption (CP-ABE) is proposed. A smart contract is also used in the proposed scheme in order to increase the scalability of the systems.

In [52], a private blockchain was used to help the agricultural sector and farmers in India to ensure that their communication with their customers can take place directly with them without any intervention from third parties in the process. The proposed model was built on Hyperledger Fabric to enable direct communication between the farmer and the customer at the same time.

4. Method

To achieve the study's key aim of exploring the use of a public blockchain platform to integrate the principle of decentralization with IDMS, we conducted a systematic review following the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) guidelines, which help in analyzing the steps of the systematic review by identifying specific and clear research questions, and following a specific methodology to obtain answers through the use of a sample of research papers that are determined by of exclusion and inclusion criteria [53]. For this purpose, we selected previous studies that use blockchain technology on IDMs. Further elaboration on research and selection strategy explanations is given below:

4.1. Research Need Identification

An objective of this systematic literature review is to examine how blockchain-based systems can be used to enhance privacy, as well as improve a system by eliminating or reducing centralization issues in trading systems, such as SPOF risks, central authority issues, and third-party control risks.

4.2. Research Questions

Q1: What are the current issues that threaten user privacy and security in centralized IDMSs?
Q2: Will decentralizing identity management by using distributed ledger technology solve user privacy problems, and if so, why?
Q3: What are the blockchain-based technologies that may be utilized to enhance user privacy?
Q4: What is the most efficient blockchain-based development platform for IDMSs?

4.3. Information Source and Database

We selected multiple databases for the information sources, as shown in Table 1. The literature review was limited to research studies published between 2018 and 2022.

Table 1. Information Source.

Database	Website
IEEE Xplore Digital Library	https://www.ieee.org
MDPI	https://www.mdpi.com

4.4. Research String

The research strings are described in Table 2.

Table 2. Research String.

Database	Keywords	NO	Open Access	After Deleting Duplicate	After Reading Paper
IEEE	"Identity management systems AND blockchain"	319	38	38	14
	"Identity management system AND smart contract"	101	11	2	0
	"Ethereum AND identity management system"	41	5	4	0
MDPI	"Identity management systems AND blockchain"	26	26	26	11
	"Identity management system AND smart contract "	7	7	1	0
	"Ethereum AND identity management system"	2	2	0	0

4.5. Criteria Selection

The study only included research written in the English language from 2018 until the present day. In addition, surveys papers or systematic review papers were not considered. Instead, papers that proposed systems were considered, as shown in Table 3.

4.6. Inclusion and Exclusion Criteria

We followed the PRISMA flow diagram in the study selection process, as shown in Figure 1, and by following the inclusion and exclusion criteria of the current systematic review described in Table 3, the authors extracted approximately 496 studies relevant to blockchain-based IDM systems. Following the two main inclusion criteria, only 71 papers fulfilled the research aims. After downloading and reading the abstracts, 46 more papers were excluded during screening. Only 26 research articles were assessed and recognized against the research criteria. The current systematic followed the PRISMA standards for data extraction and selection, as shown in Figure 1.

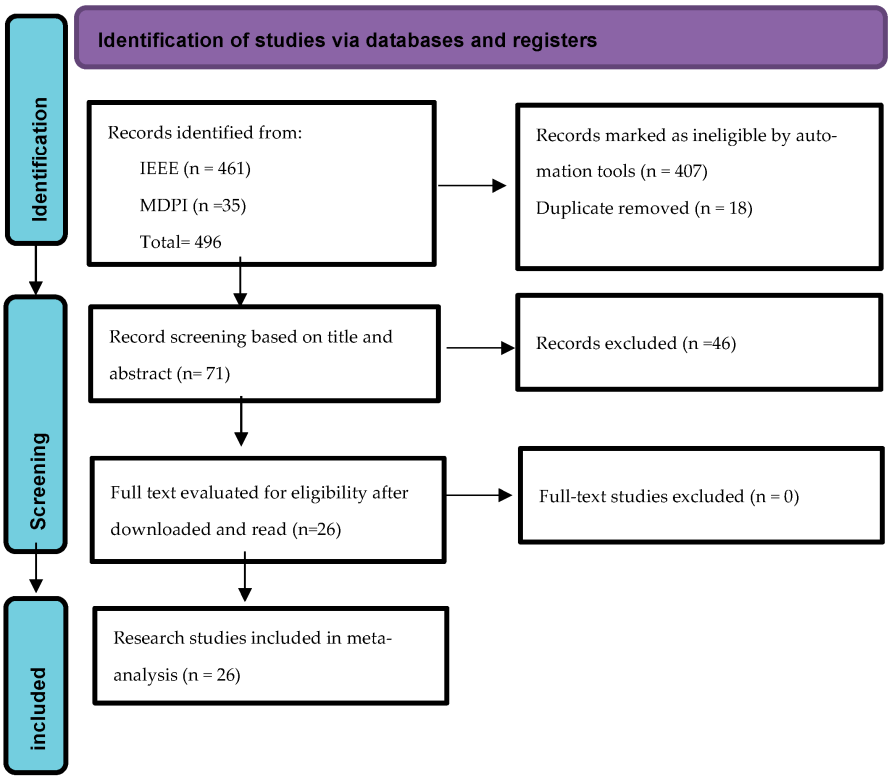


Figure 1. PRISMA flow diagram of the study selection process.

Table 3. Criteria selection.

Inclusion Criteria	Exclusion Criteria
Written English	Studies written in other languages
Studies From 2018 until now	Studies before 2018
Original research paper	Survey, systematic review papers
Proposed solution implemented	Proposed solutions not implemented

5. Results and Discussion

In this section, the research review will be discussed, and the results are presented in detail. The results are presented in multiple sub-sections according to the field to which they belong.

5.1. Study Characteristics

The current systematic review focused on developing blockchain-based solutions for privacy and security issues in IDMSs. To highlight important characteristics of the reviewed studies, we designed Tables A1 and A2 for the two databases considered in this study. Each table contains Title, Author with Year, Type, Publisher, the use of BC, and the use of SC. Due to the role blockchain types play in solving existing research problems, the tables indicate which type of blockchain was used in each research, in addition to the possibility of using smart contracts.

5.2. Discussion and Result

In this section, we present the information collected from the research papers after the systematic review. In Section 5.2.1, we review the domains in which blockchain technology was adopted to enhance privacy and security of IDM, and then Section 5.2.2 discusses the blockchain types and technologies that were applied to address different issues related to privacy and security in order to highlight the best practices and efficient solutions, as well as to provide an understanding of the potential solutions that can be offered by blockchain technologies. Section 5.2.3 discusses the research and issues addressed via using smart contracts technology, as it represents a cornerstone and powerful blockchain technology that can effectively contribute to developing efficient solutions for problems relevant to the privacy issue. Finally, in Section 5.2.4, the research questions are answered in detail.

5.2.1. Domain

The current systematic review surveyed the previously proposed IDMS solutions that adopted a decentralized approach. Previous literature has illustrated that the use of blockchain technology improved the security and privacy of IDMSs in many domains, such as IOT [12–16]; supply chain [17–20]; AC and Identity Management in [21–26], cloud IDM in [27], ad-hoc network (VANET) in [28–30], healthcare in [31–33], internet of connected vehicles in [34,35], and even for the undirected graph authentication, as discussed in [36].

5.2.2. Issues and Blockchain Type

This section sheds light on the different blockchain types adopted in previous research and the security issues addressed by each type. This assists in understanding the potential solutions that can be addressed by particular blockchain types or technology.

The majority of the reviewed studies adopted access control and IDM to find solutions for system issues by using the Ethereum blockchain type. In [27], the IDMS adopted by cloud users relies too much on third-party services. Studies published in [24] and [18] suffered from third-party issues, especially trackability, and both used Ethereum in their solutions. In [20], authors used Ethereum-based IDM Protocol as a solution for the U.S. beef cattle supply chain. By utilizing Ethereum blockchain, the authors in [19] provided a solution for identifying the root cause of system problems. An Ethereum-based food

supply chain system was proposed in [17]. Other studies have also used the Ethereum blockchain type to improve their systems, such as [14,23,29,31,34,36].

Other types of blockchain have also been used in some of the studies reviewed. A permissioned blockchain was used in [15] as a solution for the same third-party issue in a different domain. Trust relationships between SPs, users, and IDPs in ABC systems have many privacy concerns, and the authors in [26] tried to improve this by using Hyperledger technology. The later blockchain type was used by [16] to solve three main issues: (1) single failure point; (2) privacy information leak; (3) Distributed Denial of Service (DDoS) attack of the delegate node. In addition, [30] preserved a vehicle's identity privacy by using blockchain to prevent fake message distribution. Communication and computational overheads in healthcare systems were discussed by [33], using a permissioned blockchain to improve them. The reviewed studies proposed solutions to enhance and improve centralized systems by using blockchain technology in a different way, but there are still open issues that need to be addressed and enhanced, such as enhancing the scalability of blockchain-based IDMS platforms, system usability, and privacy enhancement.

5.2.3. Smart Contract

Smart contracts are a very important concept in the field of blockchains. They provide many important features to enhance system functionality and to increase the speed of operations. In the current review, only seven research papers did not use smart contracts in their proposed solutions: [15,21,25,28,30,32,35]. On the other hand, 18 research papers adopted smart contracts to provide more efficient solutions for the privacy problems in IDMS: [12–14,16–20,22–24,26,27,29,31,33,34,36].

The analysis of statistics related to the previous research shows that there has been an increase in the number of publications over recent years that adopted blockchain technology in the field of IDMS, as depicted in Figure 2. In terms of the blockchain type, the analysis results presented in Figure 3 show that Ethereum has been more frequently used than the other types of blockchain. There are several reasons for this. The smart contract is one of the most important components of an Ethereum system's development and improvement. The Solidity Language is another important reason, along with the fact that Ethereum is involved in several applications, the most important of which is the DApp.

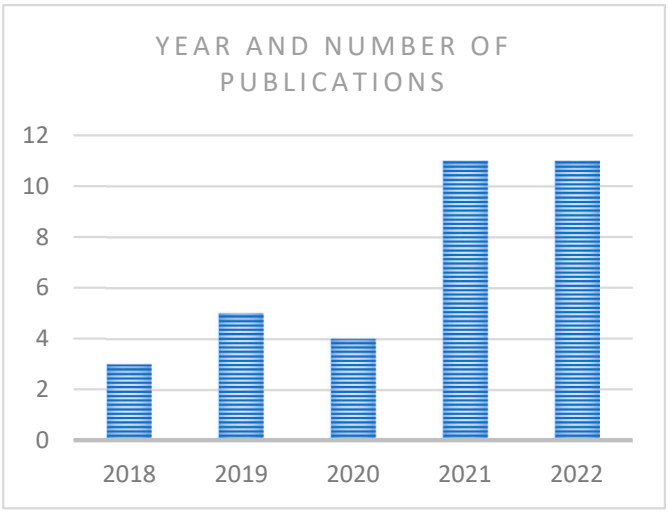


Figure 2. Years and number of publications.

There has been a significant increase in identity control on the proposed blockchain-based systems because of the third-party limitations caused by the decentralization feature. The system is powerful and operates faster when it is using smart contracts as they are self-executed codes, but there is some uncertainty about the security of the stored data. As

a result, there have been many research papers on identity management systems that are trying to reduce the different risks and to mitigate cyberattacks encountered in this field.

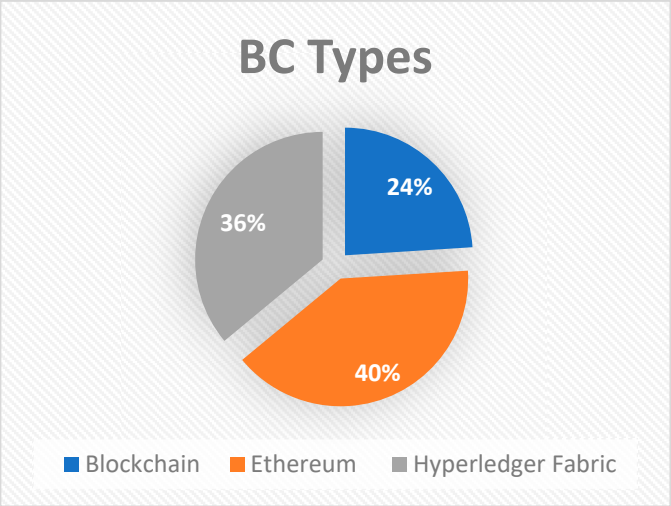


Figure 3. Blockchain Types.

It can be seen from the research articles shown in Tables A1 and A2 that blockchain technology, the underlying technology for decentralized IDMSs, has been proposed as an effective solution for privacy and security issues in a variety of fields, such as IOT, supply chains, ad-hoc networks, cloud IDM, healthcare, internet of connected vehicles, and access control. Previous research has illustrated that blockchain is a powerful technology and has many features that may effectively contribute to enhancing user privacy and increasing the level of self-control over personal data in the field of IDM and relevant applications.

5.2.4. Research Questions and Answers

Q1: What are the current issues that threaten user privacy and security in centralized IDMSs?

Central identity management systems suffer from certain privacy issues, as discussed in the previous section. One of the most important problems is centralization, since it relies upon one central party, which results in the high risk of an SPOF. Third-party control is considered one of the most important threats in centralized systems, since the user is under the control of a third party, which can compromise their privacy, such as monitoring their movements and studying their behavior.

Q2: Will decentralizing identity management by using distributed-ledger technology solve user privacy problems, and if so, why?

Decentralization of identity management by using distributed ledger technology addresses the problem of a SPOF because copies of the system are distributed over multiple peers. As the peers constantly compare and verify the validity of the copies, when one fails, the rest discover the error and recopy the system in the correct chain. Furthermore, technology provides the smart contract, which plays a major role in limiting the control of third parties, as tasks are assigned to the smart contract, and the tasks are automatically executed without the intervention of any third parties.

Q3: What are the blockchain-based technologies that may be utilized to enhance user privacy?

Using the smart contract as an intermediary to carry out tasks between the parties enhances the privacy of the parties, since, for example, users can send tokens through the smart contract to a service provider, whose tokens have attributes certified by third parties. Since a smart contract acts as an intermediary, third parties and service providers cannot

track user relations or actions. Additionally, the user can control how much data is shown in each token created for a service provider through a smart contract. The smart contract can also be used to track all the viewers of the token data by recording their addresses and the time they viewed it. So, yes, this technology enhances user privacy.

Q4: What is the most efficient blockchain-based development platform for IDMSs?

As a result of the research, most of the applications used the public blockchain (Ethereum) because it is open source and has smart contract technology. Furthermore, Ethereum works with a special currency called Ether, and has a special programming language called Solidity.

6. Conclusions

In the domain of IDM, the adaptation of distributed ledger technology has attracted attention due to its ability to enhance user privacy and address issues, such as the SPOF and third-party control. The current work reviewed recent research papers in the area of identity management systems; both traditional and those which have adopted blockchain technology. Many articles covering IDM and blockchain technologies were reviewed in this research. Many reviewed research attempts to provide the user with increased identity control by trying to solve third-party control issues, address the SPOF, and avoid fake message distribution. Furthermore, the review of previous research about IDMS showed that there are still open issues relating to user privacy in the traditional centralized IDMSs, including third-party control and user movement monitoring or tracking, in addition to the problem of the SPOF. This prompted the need to search for an efficient solution to enhance user privacy in IDMSs and avoid other problems associated with the decentralized approach. Decentralized IDM by using blockchain has many advantages, including solving the problem of third-party control by giving each user full control of their private information and activities, improving performance, and saving time by using smart contracts and other blockchain features. In addition, the use of blockchain-based IDMS can avoid the SPOF and ensure that data and services are available to legitimate parties once needed. However, blockchain-based solutions that use a private type have some weaknesses related to privacy, and they inherit certain problems from the centralized approach. In addition, the use of weak authentication methods is a significant issue that needs to be addressed in recently proposed block-chain-based IDMSs.

The systematic literature review presented in this paper discussed and analyzed the recent solutions and current challenges in the field of IDM, while concentrating on the contributions made by using blockchain technology. This aims to provide a better understanding of the role and significance of adopting blockchain technologies in the field of IDM and the advances that can be achieved using this powerful technology. Moreover, the current review attempts to identify the research gaps and open issues, and motivate future research works that may utilize the promising features of blockchain in improving user privacy and addressing other challenges in the field of IDM.

As part of our future work, we intend to implement a system prototype for a decentralized identity management system utilizing the Ethereum blockchain to solve the problems identified in this research and assess its advantages and disadvantages.

Author Contributions: Writing—original draft preparation, H.A.; writing—review and editing, H.A., M.A.; supervision, M.A. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deanship of Scientific Research at IMSIU for founding and supporting this work through the Graduate Student Research Support Program.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The literature review was limited to research studies published in IEEE and MDPI databases. https://www.ieee.org. whttps://ww.mdpi.com.

Acknowledgments: Authors acknowledge the support from Imam Mohammad ibn Saud Islamic University (IMISIU) for this research. The authors extend their appreciation to the Deanship of Scientific Research at IMSIU for founding and supporting this work through the Graduate Student Research Support Program.

Conflicts of Interest: The authors declare no conflict of interes.

Appendix A Included Studies

Table A1. MDPI Included studies.

Study NO	Title	Authors	Year	Type	Publisher	BC Used and Filed	Smart Contract
[28]	EBAS: An Efficient Blockchain-based Authentication Scheme for Secure Communication in Vehicular Ad Hoc Network	Xia Feng et al.	2022	article	MDPI	Blockchain, r secure communication in VANET	no
[12]	Developing an IoT Identity Management System Using Blockchain	Sitalakshmi Venkatraman et al.	2022	article	MDPI	Blockchain, IOT	Yes
[21]	Modbus Access Control System Based on SSI over Hyperledger Fabric Blockchain	Santiago Figueroa-Lorenzo et al.	2021	article	MDPI	Hyperledger fabric blockchain, Modbus access control.	no
[17]	Blockchain and Self Sovereign Identity to Support Quality in the Food Supply Chain	Luisanna Cocco et al.	2021	article	MDPI	Ethereum Blockchain, Food Supply chain	yes
[31]	Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare	Ibrahim Tariq Javed et al.	2021	article	MDPI	Ethereum consortium blockchain, e health	yes
[22]	Blockchain-Enabled Access Management System for Edge Computing	Yong Zhu et al	2021	article	MDPI	Blockchain, edge computing	yes
[34]	ABlockchain-based Authentiaction Protocol For Cooperative Vehicular Ad Hoc Network	A. F. M. Suaib Akhter et al.	2021	article	MDPI	Ethereum blockchain, internet of Vehicles (IoV)	yes
[13]	Alightweight Blockchain based IOT Identity Managemnt Approach	Mohammed Amine Bouras et al.	2021	article	MDPI	consortium blockchain-based identity management, IoT(implement by Hyperledger Fabric)	yes
[32]	Aprivacy-preserving Healthcare Framework Using Hyperledger Fabric	Charalampos Stamatellis et al.	2020	article	MDPI	Hyperledger Fabric's permissioned blockchain framework, healthcare	no
[23]	DNS-IDM: A Blockchain Identity Management System to Secure Personal Data Sharing in A Network	Jamila Alsayed Kassem et al.	2019	article	MDPI	private Ethereum network (permissioned Ethereum ledger)	yes
[14]	BlendCAC: ASmart Contract-Enabled Decentralized Capability-Based Access Control Mechanism For The IOT	Ronghua Xu et al.	2018	article	MDPI	private Ethereum blockchain, AC in IoT devices.	yes

Table A2. IEEE Included studies.

Study NO	Title	Authors	Year	Type	Publisher	BC Used and Filed	Smart Contract
[27]	EIDM: A Ethereum-Based Cloud User Identity Management Protocol	shangping wang et al.	2019	article	IEEE	Ethereum blockchain, cloud IDM	yes
[24]	Burnable Pseudo-Identity: A Non-binding Anonymous Identity Method for Ethereum Pseudonym Management	iván gutiérrez-agüero et al.	2021	article	IEEE	Ethereum, Anonymous Identity	yes
[35]	Through Blockchain: Cost-efficient Privacy Preservation on Intelligent Transportation Systems	shihan bao et al.	2019	article	IEEE	Blockchain, internet of connected vehicles.	no
[15]	VAIM: Verifiable Anonymous Identity Management for Human-centric Security and Privacy in the Internet of Things	gyeongjin ra et al.	2021	article	IEEE	permissioned blockchain, the human internet of things (HIoT)	no
[25]	ATIB: Design and Evaluation of an Architecture for Brokered Self-Sovereign Identity Integration and Trust-Enhancing Attribute Aggregation for the Service Provider	andreas grüner et al.	2021	article	IEEE	Blockchain, IDM(attributes aggregations.)	no
[26]	A Trusted Approach for Decentralized and Privacy-Preserving Identity Management	rafael torres moreno et al.	2021	article	IEEE	Hyperledger fabric, IDM	yes
[36]	A New Transitively Closed Undirected Graph Authentication Scheme for Blockchain-based Identity Management Systems	chao lin1 et al.	2018	article	IEEE	Ethereum, undirected graph.	yes
[16]	Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain	shuang sun et al.	2021	article	IEEE	Hyperledger fabric permissioned blockchain, IOT AC.	yes
[33]	A Permissioned Blockchain-based Identity Management and User Authentication Scheme for E-Health Systems	xinyin xiang et al.	2020	article	IEEE	permissioned blockchain, e-health systems	yes
[29]	FADB: A Fine-grained Access Control Scheme for VANET Data Based on Blockchain	hui li et al.	2020	article	IEEE	Ethereum, Vehicular Ad Hoc Network (VANET)	yes
[18]	A Blockchain-based Framework for Supply Chain Provenance	pinchen cui et al.	2019	article	IEEE	Hyperledger fabric permissioned blockchain, Supply Chain	yes
[19]	Smart Contract-based Product Traceability System in the Supply Chain Scenario	shangping wang et al.	2019	article	IEEE	Ethereum, Supply Chain	yes
[30]	A Privacy-Preserving Trust Model Based on Blockchain for VANETs	zhaojun lu et al.	2018	article	IEEE	Blockchain, vehicular ad hoc networks (VANETs)	no
[20]	A Permissioned Distributed Ledger for the US Beef Cattle Supply Chain	tanvir ferdousi et al.	2020	article	IEEE	permissioned blockchain network, Ethereum Supply Chain	yes

References

1. L'Amrani, H.; Berroukech, B.; Ajhoun, R.; El Idrissi, Y. Identity Management Systems: Laws of Identity for Models′ Evaluation. In Proceedings of the 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, Morocco, 24–26 October 2016.
2. Liu, Y.; He, D.; Obaidat, M.; Kumar, N.; Khan, M.; Choo, K. Blockchain-based identity management systems: A review. *J. Netw. Comput. Appl.* **2020**, *166*, 102731. [CrossRef]
3. Agudo, I. Digital Identity and Identity Management Technologies. *Serb. Publ. InfoReview Joins UPENET Netw. CEPIS Soc. J. Mag.* **2010**, *6*.
4. Jøsang, A.; AlZomai, M.; Suriadi, S. Usability and Privacy in Identity Management Architectures. In Proceedings of the Fifth Australasian Symposium on Grid Computing and e-Research (AusGrid 2007), the Fifth Australasian Information Security

Workshop (Privacy Enhancing Technologies) (AISW 2007), and the Australasian Workshop on Health Knowledge Management and Discovery (HKMD 2007). Proceedings, Ballarat, VIC, Australia, 30 January-2 February 2007.
5. Panait, A.; Olimid, R.; Stefane, A. Identity Management on Blockchain—Privacy and Security Aspects. *Proc. Rom. Acad.-Ser. A Math. Phys. Tech. Sci. Inf. Sci.* **2021**, *21*, 45–52.
6. Alrodhan, W. *Privacy and Practicality of Identity Management Systems: Academic Overview*; Vdm Verlag Dr. Müller: Saarbrücken, Germany, 2011.
7. Lim, S.Y.; Tankam Fotsing, P.; Almasri, A.; Musa, O.; Mat Kiah, M.L.; Ang, T.F.; Ismail, R. Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2018**, *8*, 1735. Available online: http://insightsociety.org/ojaseit/index.php/ijaseit/article/view/6838 (accessed on 15 August 2022). [CrossRef]
8. Almeshal, T.A.; Alhogail, A.A. Blockchain for Businesses: A Scoping Review of Suitability Evaluations Frameworks. *IEEE Access* **2021**, *9*, 155425–155442. [CrossRef]
9. Zhu, X. Research on blockchain consensus mechanism and implementation. *IOP Conf. Ser. Mater. Sci. Eng.* **2019**, *569*, 042058. [CrossRef]
10. Maldonado, F.C. *Introduction to Blockchain and Ethereum: Use Distributed Ledgers to Validate Digital Transactions in a Decentralized and Trustless Manner*; Packt Publishing: Birmingham, UK, 2018.
11. Joshi, J.; Nepal, S.; Zhang, Q.; Zhang, L. Blockchain—ICBC 2019. In Proceedings of the Second International Conference, held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, 25–30 June 2019; Springer: Cham, Switzerland, 2019.
12. Bao, Z.; Wang, Q.; Shi, W.; Wang, L.; Lei, H.; Chen, B. When Blockchain Meets SGX: An Overview, Challenges, and Open Issues. *IEEE Access* **2020**, *8*, 170404–170420. [CrossRef]
13. Bouras, M.A.; Lu, Q.; Dhelim, S.; Ning, H. A Lightweight Blockchain-Based IoT Identity Management Approach. *Future Internet* **2021**, *13*, 24. [CrossRef]
14. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. BlendCAC: A Smart Contract Enabled Decentralized Capability-Based Access Control Mechanism for the IoT. *Computers* **2018**, *7*, 39. [CrossRef]
15. Ra, G.; Kim, T.; Lee, I. VAIM: Verifiable Anonymous Identity Management for Human-Centric Security and Privacy in the Internet of Things. *IEEE Access* **2021**, *9*, 75945–75960. [CrossRef]
16. Sun, S.; Du, R.; Chen, S.; Li, W. Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain. *IEEE Access* **2021**, *9*, 36868–36878. [CrossRef]
17. Cocco, L.; Tonelli, R.; Marchesi, M. Blockchain and Self Sovereign Identity to Support Quality in the Food Supply Chain. *Future Internet* **2021**, *13*, 301. [CrossRef]
18. Cui, P.; Dixon, J.; Guin, U.; Dimase, D. A Blockchain-Based Framework for Supply Chain Provenance. *IEEE Access* **2019**, *7*, 157113–157125. [CrossRef]
19. Wang, S.; Li, D.; Zhang, Y.; Chen, J. Smart Contract-Based Product Traceability System in the Supply Chain Scenario. *IEEE Access* **2019**, *7*, 115122–115133. [CrossRef]
20. Ferdousi, T.; Gruenbacher, D.; Scoglio, C.M. A Permissioned Distributed Ledger for the US Beef Cattle Supply Chain. *IEEE Access* **2020**, *8*, 154833–154847. [CrossRef]
21. Figueroa-Lorenzo, S.; Añorga Benito, J.; Arrizabalaga, S. Modbus Access Control System Based on SSI over Hyperledger Fabric Blockchain. *Sensors* **2021**, *21*, 5438. [CrossRef]
22. Zhu, Y.; Huang, C.; Hu, Z.; Al-Dhelaan, A.; Al-Dhelaan, M. Blockchain-Enabled Access Management System for Edge Computing. *Electronics* **2021**, *10*, 1000. [CrossRef]
23. Alsayed Kassem, J.; Sayeed, S.; Marco-Gisbert, H.; Pervez, Z.; Dahal, K. DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network. *Appl. Sci.* **2019**, *9*, 2953. [CrossRef]
24. Gutierrez-Aguero, I.; Anguita, S.; Larrucea, X.; Gomez-Goiri, A.; Urquizu, B. Burnable Pseudo-Identity: A Non-Binding Anonymous Identity Method for Ethereum. *IEEE Access* **2021**, *9*, 108912–108923. [CrossRef]
25. Gruner, A.; Muhle, A.; Meinel, C. ATIB: Design and Evaluation of an Architecture for Brokered Self-Sovereign Identity Integration and Trust-Enhancing Attribute Aggregation for Service Provider. *IEEE Access* **2021**, *9*, 138553–138570. [CrossRef]
26. Moreno, R.T.; Garcia-Rodriguez, J.; Bernabe, J.B.; Skarmeta, A. A Trusted Approach for Decentralised and Privacy-Preserving Identity Management. *IEEE Access* **2021**, *9*, 105788–105804. [CrossRef]
27. Wang, S.; Pei, R.; Zhang, Y. EIDM: A Ethereum-Based Cloud User Identity Management Protocol. *IEEE Access* **2019**, *7*, 115281–115291. [CrossRef]
28. Feng, X.; Cui, K.; Jiang, H.; Li, Z. EBAS: An Efficient Blockchain-Based Authentication Scheme for Secure Communication in Vehicular Ad Hoc Network. *Symmetry* **2022**, *14*, 1230. [CrossRef]
29. Li, H.; Pei, L.; Liao, D.; Chen, S.; Zhang, M.; Xu, D. FADB: A Fine-Grained Access Control Scheme for VANET Data Based on Blockchain. *IEEE Access* **2020**, *8*, 85190–85203. [CrossRef]
30. Lu, Z.; Liu, W.; Wang, Q.; Qu, G.; Liu, Z. A Privacy-Preserving Trust Model Based on Blockchain for VANETs. *IEEE Access* **2018**, *6*, 45655–45664. [CrossRef]
31. Javed, I.T.; Alharbi, F.; Bellaj, B.; Margaria, T.; Crespi, N.; Qureshi, K.N. Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare. *Healthcare* **2021**, *9*, 712. [CrossRef]
32. Stamatellis, C.; Papadopoulos, P.; Pitropakis, N.; Katsikas, S.; Buchanan, W.J. A Privacy-Preserving Healthcare Framework Using Hyperledger Fabric. *Sensors* **2020**, *20*, 6587. [CrossRef] [PubMed]

33. Xiang, X.; Wang, M.; Fan, W. A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems. *IEEE Access* **2020**, *8*, 171771–171783. [CrossRef]
34. Akhter, A.F.M.S.; Ahmed, M.; Shah, A.F.M.S.; Anwar, A.; Kayes, A.S.M.; Zengin, A. A Blockchain-Based Authentication Protocol for Cooperative Vehicular Ad Hoc Network. *Sensors* **2021**, *21*, 1273. [CrossRef] [PubMed]
35. Bao, S.; Cao, Y.; Lei, A.; Asuquo, P.; Cruickshank, H.; Sun, Z.; Huth, M. Pseudonym Management Through Blockchain: Cost-Efficient Privacy Preservation on Intelligent Transportation Systems. *IEEE Access* **2019**, *7*, 80390–80403. [CrossRef]
36. Lin, C.; He, D.; Huang, X.; Khurram Khan, M.; Choo, K.-K.R. A New Transitively Closed Undirected Graph Authentication Scheme for Blockchain-Based Identity Management Systems. *IEEE Access* **2018**, *6*, 28203–28212. [CrossRef]
37. de Ponteves, H.; Eremenko, K.; Ligency Team. Blockchain A-Z™: Learn How To Build Your First Blockchain. September 2021. Available online: https://www.udemy.com/course/build-your-blockchain-az/#instructor-1 (accessed on 11 June 2022).
38. Shobanadevi, A.; Tharewal, S.; Soni, M.; Kumar, D.D.; Khan, I.R.; Kumar, P. Novel identity management system using smart blockchain technology. *Int. J. Syst. Assur. Eng. Manag.* **2022**, *13* (Suppl. 1), 496–505. [CrossRef]
39. Lastovetska, A. Blockchain Architecture Basics: Components, Structure, Benefits & Creation. 5 January 2021. Available online: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture (accessed on 1 November 2022).
40. Buterin, V. The Meaning of Decentralization. [Online] Medium. 2017. Available online: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 (accessed on 26 October 2022).
41. Wüst, K. Do you need a Blockchain? In Proceedings of the Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 20–22 June 2018.
42. Alrodhan, W.; Mitchell, C. Improving the Security of CardSpace. *EURASIP J. Inf. Secur.* **2009**, *2009*, 1–8. [CrossRef]
43. Alrodhan, W.; Mitchell, C. Enhancing User Authentication in Claim-Based Identity Management. In Proceedings of the 2010 International Symposium on Collaborative Technologies and Systems, Chicago, IL, USA, 17–21 May 2010.
44. Dai, Z.; Zhou, W. *The Federated Identity and Access Management Architectures: A Literature Survey*; Deakin University, School of Information Technology: Geelong, VIC, Australia, 2005.
45. Sung, C.; Park, J. Understanding of blockchain-based identity management system adoption in the public sector. *J. Enterp. Inf. Manag.* **2021**, *34*, 1481–1505. [CrossRef]
46. Niu, J.; Ren, Z. A self-sovereign identity management scheme using smart contracts. *MATEC Web Conf.* **2021**, *336*, 08005. [CrossRef]
47. Bouras, M.; Lu, Q.; Zhang, F.; Wan, Y.; Zhang, T.; Ning, H. Distributed Ledger Technology for eHealth Identity Privacy: State of the Art and Future Perspective. *Sensors* **2020**, *20*, 483. [CrossRef]
48. Ferdous, M.S.; Poet, R. A Comparative Analysis of Identity Management Systems. In Proceedings of the 2012 International Conference on High Performance Computing & Simulation (HPCS), Madrid, Spain, 2–6 July 2012.
49. Stockburger, L.; Kokosioulis, G.; Mukkamala, A.; Mukkamala, R.; Avital, M. Blockchain-enabled Decentralized Identity Management: The Case of Self-sovereign Identity in Public Transportation. *Blockchain Res. Appl.* **2021**, *2*, 100014. [CrossRef]
50. Outchakoucht, A.; Es-Samaali, H. Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 417–424. [CrossRef]
51. Liao, C.H.; Guan, X.Q.; Cheng, J.H.; Yuan, S.M.; Blockchain-Based Identity Management and Access Control Framework for Open Banking Ecosystem. pp. 450–466. Available online: https://ssrn.com/abstract=4039865 (accessed on 5 October 2022).
52. Desabathina, N.V.M.; Merugu, S.; Gunjan, V.K.; Kumar, B.S. Agricultural Crowdfunding Through Blockchain. In *ICDSMLA 2020*; Kumar, A., Senatore, S., Gunjan, V.K., Eds.; Lecture Notes in Electrical Engineering; Springer: Singapore, 2022; Volume 783. [CrossRef]
53. Tetzlaff, J.; Page, M.; Moher, D. Pns154 the prisma 2020 statement: Development of and key changes in an updated guideline for reporting systematic reviews and meta-analyses. *Value Health* **2020**, *23*, S312–S313. [CrossRef]