International Journal of Distributed Systems and Technologies
Volume 14 • Issue 1

Using Smart Contracts in the Proposed Blockchain Framework for an Identity Management System Based on the Internet of Things

Sara Jeza Alotaibi, Institute of Public Administration, Jeddah, Saudi Arabia*

ABSTRACT

Blockchain technology has revolutionized various sectors such as trade finance, education, healthcare, the internet of things (IoT), and user identification with its groundbreaking potential. Its transformative influence on privacy, data integrity, and transactional reliability has significantly enhanced user authentication sharing across industries. Consequently, there is a pressing demand for a robust framework capable of providing seamless authentication between devices, cloud servers, and IoT base stations. This article presents into the critical need for such a framework, meticulously evaluating its feasibility in light of the scarce existing solutions that meet industry guidelines. The proposed framework reconciles two contrasting perspectives, thoroughly examining 11 distinct factors and highlighting key features uncovered through rigorous research. The findings have implications for the future of secure authentication.

KEYWORDS

Blockchain, Framework, Identity Management, Model, User Authentication

INTRODUCTION

Users are becoming increasingly active in this brand-new realm of cloud computing technologies (Abreu et al., 2022; Sanka et al., 2021; Saif & Islam, 2022; Reyna et al., 2018). Millions of people use computers and mobile devices regularly to engage in various activities, including online shopping, research, sharing memories on social media, and engaging in various financial transactions (Sanka et al., 2021; Fakhri & Mutijarsa, 2018). A user's digital footprint increases in proportion to the number of transactions he completes online (Saif & Islam, 2022). In actuality, most internet transactions require revealing a person's personal data. For instance, to attempt transactions with online retailers such as Amazon Pay, Google Wallet, PayPal, and Paytm, users must submit login information such as personal information and financial data (Toufaily et al., 2021; Dittmann & Jelitto, 2019). This results in sharing end-users' personal information kept in a sizable database (Reyna et al., 2018).

DOI: 10.4018/IJDST.322095 *Corresponding Author

Additionally, most machines are found in the internet environment, where they rely completely on obtaining a person's data without giving the owner any notice (Gunanidhi & Krishnaveni, 2022; Liu et al., 2021). The third parties then acquire access to clients' private information without their consent (Rubio et al., 2003). Additionally, there is a danger that information kept on cloud storage systems will be disclosed to third parties without the subject's knowledge or consent (Puthal et al., 2020).

Identity documents are used by everyone and disseminated without authorization (Dhar et al., 2022). Loans, bank accounts, sim cards, and ticket bookings require identity credentials (Choi & Kim, 2020). Government entities, banks, and credit agencies are the weakest link in the identity management system due to data theft and hacking (Chalaemwongwan & Kurutach, 2018; Choi & Kim, 2020; Gong-Guo & Wan, 2021). The current identity management system is not trustworthy or safe. Using a passport, voter ID, or pan card, you must always confirm your identification. Multiple IDs can lead to data breaches and privacy problems (Noh & Rhee, 2020). Therefore, the blockchain may pave the route to self-sovereign identification through decentralized networks, which provide privacy, trust, and security where identity papers are safeguarded and validated, and permissioned participants endorse identity documents (Wang et al., 2020).

All of these claims illustrate how far the online identity management system is from attaining sustainability (Kinai et al., 2020). Consequently, the usage of Blockchain-based identity management is necessary (Xu et al., 2021). As a result, the blockchain has the potential to do away with middlemen while yet enabling individuals to maintain their identities on their own. But, before switching to blockchain, it's important to comprehend how identity management functions and the problems with the current system (Cheng & Shaoqin, 2020).

The blockchain architecture best serves a digital credential ecosystem that facilitates the issuance, security, storage, and verification of learning credentials through time and across various professional, cultural, and geographic contexts (Puthal et al., 2020; Zubair et al., 2020; Sharma et al., 2020; Sharma, 2020; Wang et al., 2021). Receivers should be able to manage all elements of their credentials in a completely self-sovereign environment, including how they are identified as unique persons in the credential, where they are kept, and with whom they are shared (Zubair et al., 2020; Sharma et al., 2020; Sharma, 2020). Since personal information and identities are shared online, users should control their digital credential records and be able to choose to share all or parts of them in exchange for access to the services they desire—without constantly turning to a third party intermediary to validate or correlate such information or identities to other data—thereby providing a single, secure user authentication record of identity achievement that is dispersed across numerous organisations and is accessible (Kim et al., 2020; Wang et al., 2020; Lee et al., 2021; Liu et al., 2021). After its secretive creator, Satoshi Nakamoto envisioned it in a white paper and subsequently utilized it to construct the cryptocurrency Bitcoin, blockchain technology became widely used in 2008 (Frizzo-Barker et al. 2020; Attaran, 2020). However, the ramifications of the technology stretch well beyond its use as the foundation of a cryptocurrency because it was one of the first widespread deployments of decentralization (López Peña & Muñoz Fernández, 2019). The blockchain technology provides transparency, security, and many other advantages that enhance the value of various sectors' enterprises (Kleinknecht, 2021). As a result, it is ready to completely change identity management as it now exists.

With its built-in features, Blockchain has, over the past ten years, offered a potential method for decentralised Identity Management Systems (IMS) in Internet of Things (IoT) networks (Wang et al., 2021; Ismail et al., 2022; Xue et al., 2022; Geetha & Balakrishnan, 2021; Patel et al., 2019; Cheng et al., 2022; Xue et al., 2022; Nikhitha & Kumara, 2020). IMS has recently become a significant responsibility for government and enterprises to provide an effective, decentralized mutual authentication and privacy protection for IoT users. IoT is one significant shift corporate IMS must manage. The Internet of Things (IoT) is the integration of physical things into information networks, according to Ismail et al. (2022), smart devices can engage actively in corporate operations and interface with services through the internet in this way (Ismail et al., 2022). When discussing the Internet of Things, the idea of identity includes individual identities and IoT products and services.

In mind of creating trust and implementing access control across IoT devices, data, and network resources, secure machine-to-machine (M2M) communication requires dependable procedures (Xue et al., 2022). To allow authenticity and to guard against security breaches, the connecting IoT devices must be individually recognized. IoT, IMS, and related problems have already been covered in several recent research studies (Geetha & Balakrishnan, 2021; Patel et al., 2019; Cheng et al., 2022; Xue et al., 2022). According to Patel et al. (2019), a strong and extensible framework is needed to provide safe Identity Management, since there are so many types of entities that communicate within IoT networks. Finally, all entities and their identities must be handled in a scalable fashion to change space and network needs over time, according to Cheng et al. (2022), to facilitate governance and inter-operability between users and several various devices. As a result, we focus the central topic of the research on developing a conceptual model, which may be addressed by reviewing all current system frameworks and literature on the hypothetical Blockchain Framework for Identity and Access Management System based on the Internet of Things. As a result, the following question forms the basis of the research:

What conceptual framework may be used to offer direction while building the Blockchain Framework for Identity and Access Management System?

This article is divided into the following four sections. First, a review of the relevant literature is provided. Second, a critical analysis of frameworks and models is conducted, with comparison of varying criteria and selected components, emphasizing how the chosen framework is suggested based on characteristics associated with this area of study. Lastly, a summary of the findings is presented.

BACKGROUND AND RELATED WORK

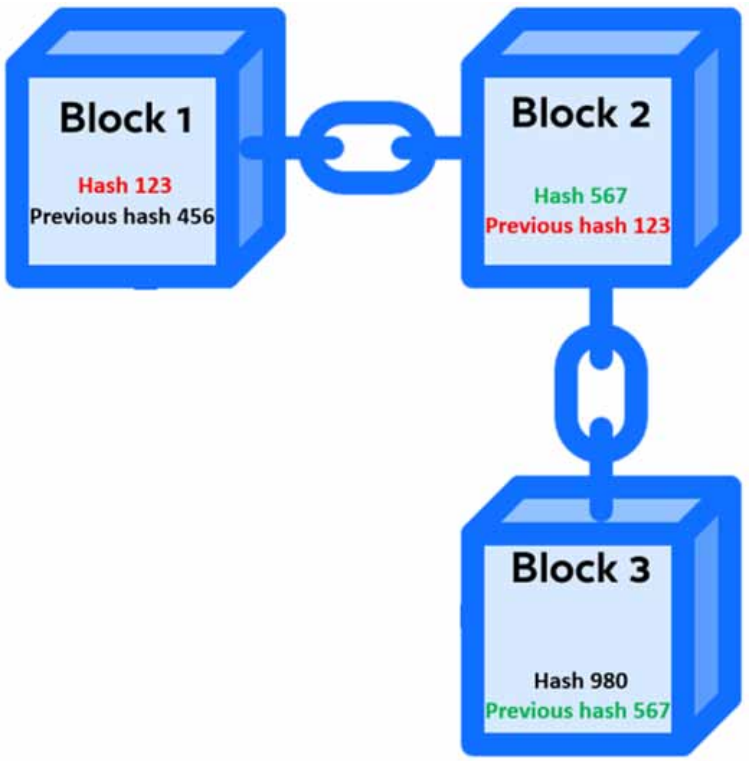
Blockchain technology has gained popularity in recent years as a distributed ledger because of various factors (López Peña & Muñoz Fernández, 2019). For instance, at the beginning of the twenty-first century, blockchain technology was known for its capacity to make the use of cryptocurrencies, such as Bitcoin, easier. The idea of blockchain was initially introduced in 1991, with Satoshi Nakamoto replicating the technology with the launch of the first cryptocurrency to use a blockchain, Bitcoin (Frizzo-Barker et al., 2020; Attaran, 2020).

When it comes to defining the term ‘blockchain’, it is acknowledged as a decentralized data ledger that benefits from safe sharing. This specific technology facilitates a diverse set of consumers’ engagement in data (Baig et al., 2020). Regarding blockchain cloud services, transactional data from many sources can be easily gathered, combined, and shared (Khan & Salah, 2017). Data is divided into various blocks, chained together, with each block assigned a unique identification code, most notably as a cryptographic hash, which is then shared (Iqbal & Matulevičius, 2021). By eliminating data duplication and maintaining data integrity with a single source of truth, such technology improves overall security (Janssen et al., 2020).

A blockchain, when properly defined, may be considered a distributed database that enables its users, or ‘nodes’, to safely and instantly transfer data as blocks (Bhutta et al., 2021). As can be seen in Figure 1, each brick is connected to the one before it, forming a chain (Kim et al., 2019; Park et al., 2019; Alhassan et al., 2020; Yang et al., 2021) As a result, as illustrated in Figure 1, a blockchain is built from several blocks, each of which contains data that must be saved and includes a hash (specifically, a unique code identifying the material housed within the block) and a hash record relating to the chain’s preceding block (Park et al., 2019; Alhassan et al., 2020). If any of the blocks are the target of interference, whether on the block fingerprint or hash, they alert all following chain blocks to the tempering, with the block whose hash was changed no longer matching earlier records. Tampering is impossible with this kind of connection (Alemany et al., 2022).

PCs, Servers, laptops, desktop wallets, smartphones, and other connected devices can all be categorized as nodes on the blockchain (Gupta et al., 2021). Each node has a connection to the blockchain in some fashion, and they are all in continual communication with one another, exchanging

Figure 1.
Blockchain components



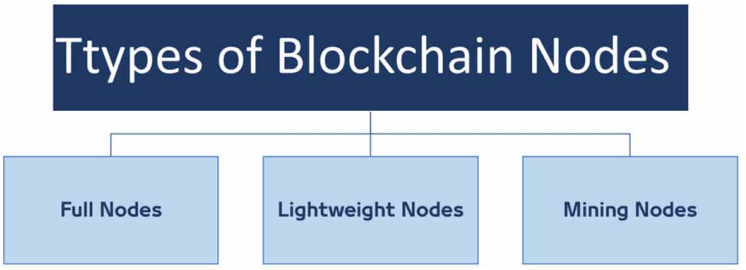
the most recent data being added to the blockchain (Ray et al., 2021). A crucial part of a blockchain's infrastructure is its nodes. They provide additional ledger validation and enable transparent viewing of network-based transactions or data (Urien, 2021). Nodes' primary advantages are ensuring the blockchain's data is accurate, safe, and accessible to authorized parties (Bhaskar et al., 2020).

We refer to each user as a node in a blockchain network (Dutta et al., 2020). Blockchain nodes have much to offer because the network is decentralized and lacks a single authority (Bajoudah et al., 2019). There are several types of blockchain nodes, and particular hardware configurations are needed to host or link each (Chen et al., 2021). Nodes can be broadly categorized into three categories: complete nodes, lightweight nodes, and mining nodes (Figure 2). These types comprise a constellation of several clustered nodes (Malik et al., 2019).

Full Nodes

Full nodes serve as a server in a decentralized network. Their primary responsibilities include ensuring that other nodes maintain their consensus and confirming transactions (Khan & Salah, 2017). They can safely allow unique features, such as quick transmission and private transactions, since they also maintain a copy of the blockchain (Kshetri & Voas, 2018). Full nodes vote on proposals while deciding on the future of a network. Additionally, this complete node's unique feature is downloading blocks from the start and deleting the oldest ones after reaching a certain threshold, leaving just their headers and chain placement (Furneaux 2018). Furthermore, full nodes could offer a potential method for user identity verification in decentralized apps (Gupta et al., 2021). This indicates that these nodes have the democratic right to select any node to verify the end user's identity (Khan & Salah, 2017). The person in charge of this particular node can manually verify the documentation (Alemany et

Figure 2.
Types of blockchain nodes

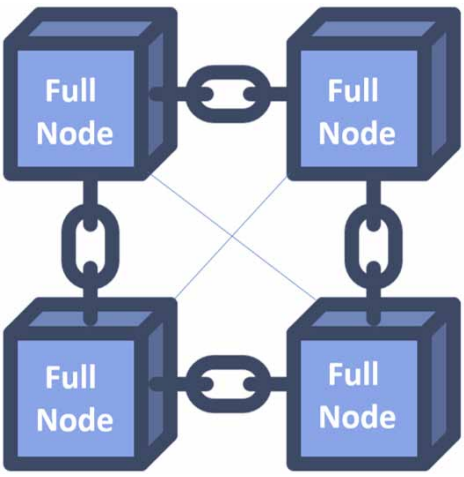


al., 2022). The master node may select a different node if the current node cannot provide quality service (Ray et al., 2021). This strategy is compatible and efficient in dealing with the decentralized identification issue (Furneaux 2018). We cannot avoid blockchain nodes since they are necessary for the technology to work properly (Kshetri & Voas, 2018). A full node serves as the primary server for all decentralized blockchain networks and keeps all data held on a blockchain (Alemany et al., 2022). All of the complete nodes in a network verify, validate, and accordingly store every block on a blockchain (Ray et al., 2021).

Figure 3 depicts a typical blockchain network with four complete nodes connecting it. Because every full node will keep a copy of every blockchain transaction, full nodes are data-intensive (Ray et al., 2021). As a result, they are more expensive and demand more sophisticated energy and computing resources (Gupta et al., 2021). The number of active complete nodes on the Bitcoin network is reportedly over 10,000 (Khan & Sala, 2017; Furneaux, 2018; Kshetri & Voas, 2018; Alemany et al., 2022; Gupta et al., 2021; Ray et al., 2021).

Full nodes have unique tasks that set them apart from other types of nodes and are crucial to a blockchain network's overall security and validity (Khan & Sala, 2017; Furneaux, 2018; Kshetri & Voas, 2018; Alemany et al., 2022; Gupta et al., 2021; Ray et al., 2021;Urien, 2021). Included in two salient distinctive qualities are:

Figure 3.
Full blockchain node



- Validation of signatures in each block transaction: Upon adding a new block to a blockchain, a full node examines each digital signature to confirm the transaction's authenticity. We refer to the transaction sender's private key to sign each transaction as a digital signature.
- A full node has the power and decision-making influence to reject new transactions or blocks, making it a key decision enforcer of consensus rules. This includes whether other network nodes have verified the arriving node. Incorrectly structured blocks or duplicate transactions are two reasons to reject newly generated transactions (potentially fraudulent transactions).

Lightweight Nodes

Lightweight nodes are known as 'light nodes' and are utilized in day-to-day bitcoin transactions Kshetri & Voas, 2018; Alemany et al., 2022; Gupta et al., 2021; Ray et al., 2021;Urien, 2021;Bhaskar et al., 2020; Dutta et al., 202; Chen et al., 2021; Bajoudah et al., 2019; Malick et al., 2019; Gourisetti et all., 2020). These nodes rely on full nodes to supply them with the essential sets of information when they connect with the blockchain. They only check the most recent block's status rather than storing a copy of the blockchain (Alemany et al., 2022). Additionally, they broadcast transactions for processing to other nodes in the network (Gupta et al., 2021). Light nodes serve a similar function as full nodes, but instead of storing the entire blockchain's history, they generally store a block header that attempts to verify and support earlier transactions (Ray et al., 2021). The block header gives a detailed summary of a single block and information about its linked preceding block (Urien, 2021). The block's timestamp and a unique identification number are two pieces of information in the block header, which is also known as a nonce (Dutta et al., 2020).

Light nodes may contact full nodes, typically their parent nodes, as seen in Figure 4, and validate transactions included in a particular block (Chen et al., 2021). In contrast to full nodes, light nodes rely solely on full nodes to supply them with verified data. Light nodes do not maintain a copy of a blockchain's entire history (Dutta et al., 2020). Adding light nodes helps a blockchain's network expand and become more decentralised (Gupta et al., 2021). Light nodes need much less energy to operate and maintain since they store and process less data than full nodes (Alemany et al., 2022). Compared to complete nodes, this enables a blockchain network to expand more sustainably (Gupta et al., 2021; Ray et al., 2021; Urien 2021; Bhaskar et al., 2020; Dutta et al., 2020).

Mining Nodes

Mining nodes are nodes that generate blockchain blocks. Bitcoin miners—a common term in the modern-day world—are categorized as nodes (Gourisetti et al., 2020). As seen in Figure 5, the function of these miners is to carry out tasks like discovering a nonce that fulfills for the present network difficulty. Using high-performance computing systems for computational power, the first entity to announce their results and receive validation from all complete nodes is entitled to add a new block to the blockchain structure (Chen et al., 2021; Bajoudah et al., 2019; Malik et al., 2019).

The maintenance and validity of upcoming blocks are not the responsibility of mining nodes; they are solely responsible for adding new blocks to the blockchain, unlike full nodes (Bajoudah et al., 2019; Malik et al., 2019; Gourisetti et al., 2020; Niya et al., 2019). Users can collaborate with others while increasing their chances of earning rewards over time by using mining nodes (Gourisetti et al., 2020). It is important to note that mining uses electricity, and miners often incur hefty startup expenses when acquiring the necessary computer power (Chang et al., 2019). Because of this, mining pools—which pool the hashrate from many users and sources—have become increasingly popular (Wamba et al., 2019).

Table 1 compares the three types of nodes based on four criteria: proposing new blocks, sending new transactions, and holding the complete data history of the blockchain.

End users have complete control and authorization through identity management, leveraging the blockchain technology (Xu et al., 2021). This access provides them with the necessary means

Figure 4.
Light nodes and full nodes

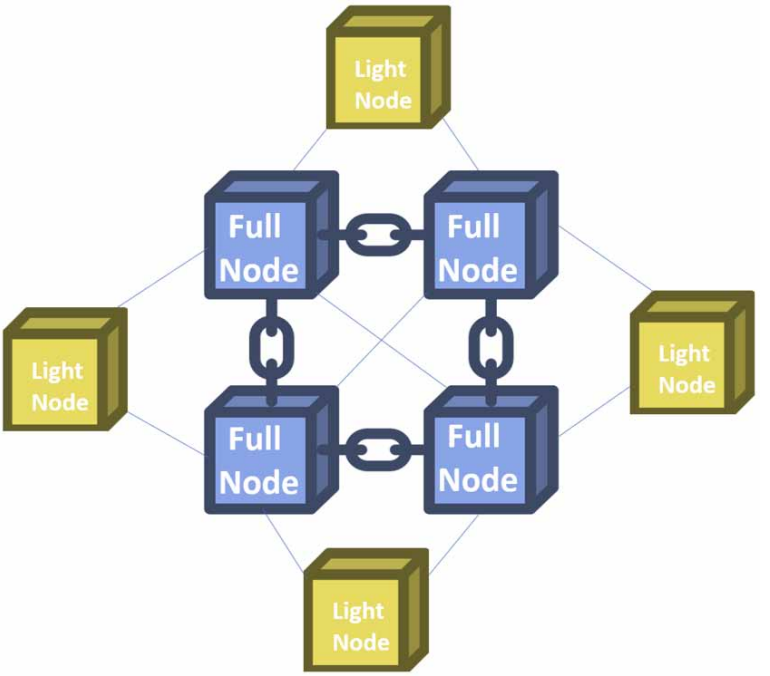


Figure 5.
Mining node, light nodes, and full nodes

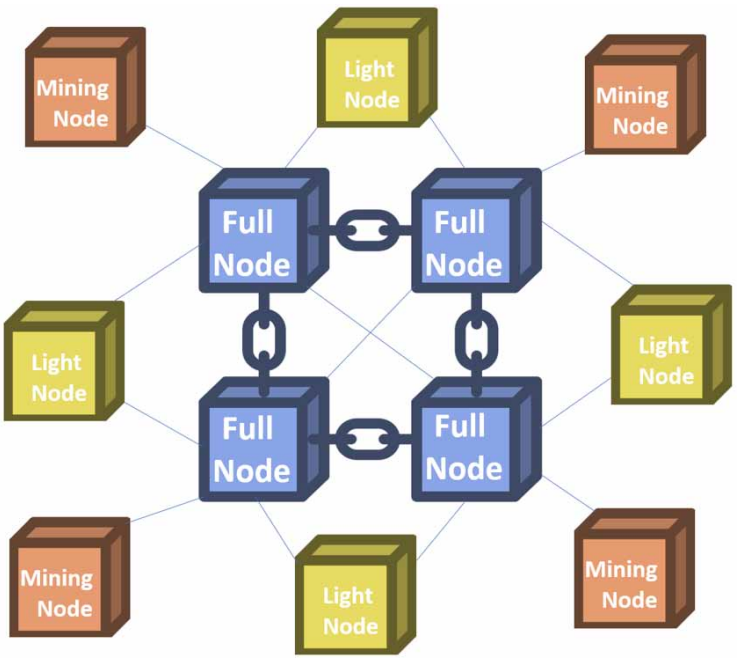


Table 1.
Comparison of the three types of nodes

Types of Blockchain Nodes	Proposing New Blocks	Sending New Transactions	Holding the Complete Data History of the Blockchain
Full Nodes	NO	YES	YES
Light Nodes	NO	YES	NO
Mining Nodes	YES	NO	NO

to communicate their information for transactions (Wang et al., 2021; Ismail et al., 2022). At the same time, it will protect the preserved data from theft and accidents. It facilitates operations and is beneficial for maintaining a recent digital clone (Alladi et al., 2022). When businesses use blockchain for identity management, it will be feasible to ensure the authenticity and veracity of data (Meng et al., 2021; Hewa et al., 2020).

The fundamental components that make up various forms of blockchain technology are depicted in Figure 6.

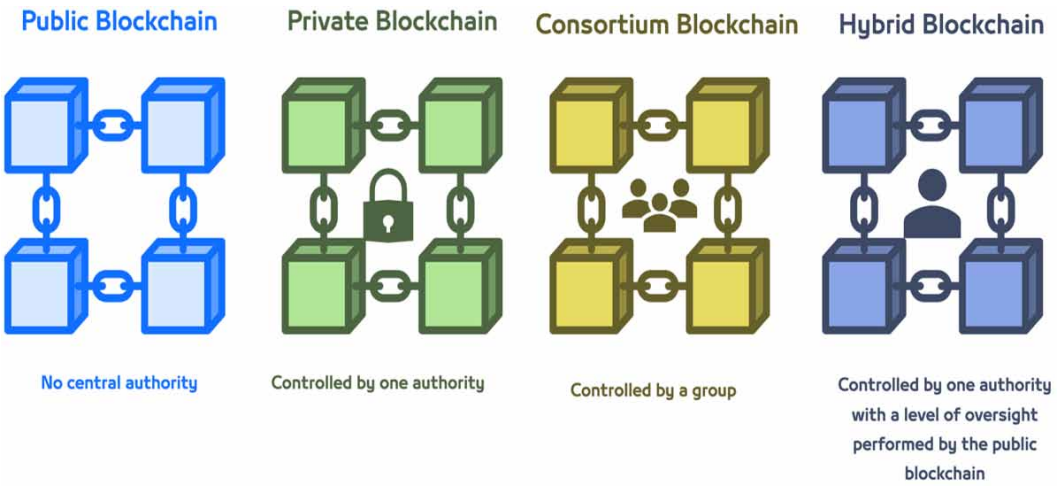
Public Blockchains

Public blockchains are entirely decentralized, permissionless, and open to all users (Hewa et al., 2020). With no access constraints, such blockchains provide all blockchain nodes an identical level of access, creation, and validation (McGhin et al., 2019). A secure network is given because the data is not changeable following network publishing, which lowers the chance of a 51% assault, and because no one node controls the network because of its decentralized structure (Hewa et al., 2020; McGhin et al., 2019; Gasimov & Aliyeva, 2021).

Private Blockchains

Created and maintained by certain companies according to their needs, we can see private blockchains as an additional layer of security that accomplishes access capabilities by permitting specific actions by various identified members (Hewa et al., 2020; McGhin et al., 2019). This particular blockchain is

Figure 6.
Different types of blockchain structure



preferred by people that need privacy, security, and a specific identification system—even though it is not as extensively used as the public blockchain. Furthermore, compared to the public blockchain, such a blockchain offers more network management flexibility, higher levels of accountability, and less network latency (Gasimov & Aliyeva, 2021).

Consortium Blockchains

In general, consortium blockchains are characterised as permissioned blockchains managed by several organizations (Alladi et al., 2022). As a result, they benefit from higher decentralization and security compared to private blockchains. However, creating consortiums can be challenging since it requires collaboration between several groups, which poses a variety of difficulties in addition to potential security and trust problems (Hewa et al., 2020; McGhin et al., 2019).

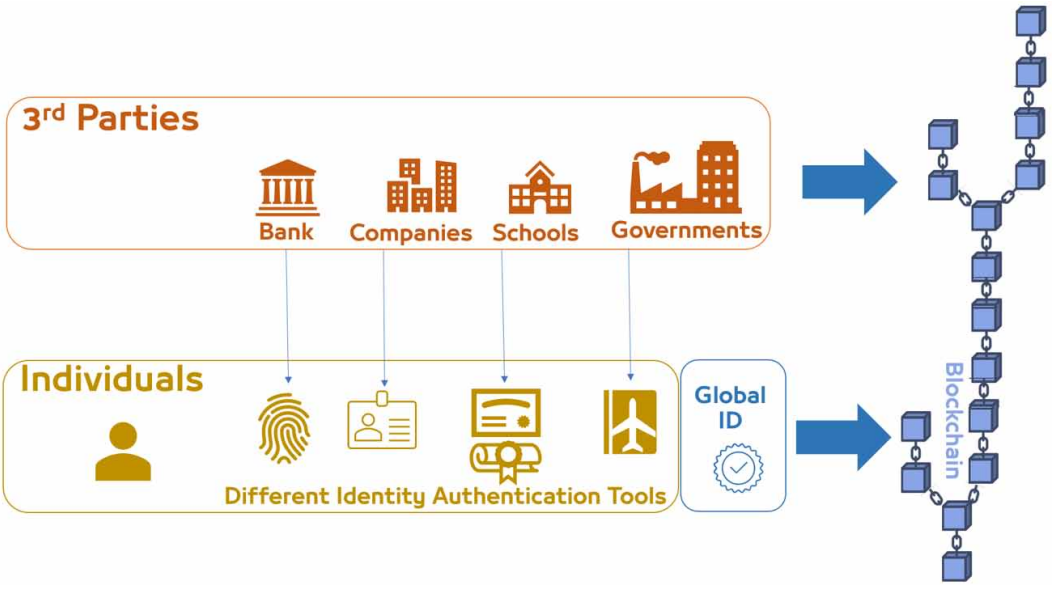
Hybrid Blockchains

This sort of blockchain is viewed to be managed by a single entity while still having oversight from the public blockchain; this is thought to be required when it comes to carrying out various transaction validations utilising various new technologies, such as the IoT (Chang et al., 2020). The proposed blockchain concept for identity management systems illustrates this form of blockchain (Liang et al., 2021).

Additionally, blockchain technology offers a variety of significant benefits for identity management, including those related to usability, efficiency, privacy, and security. In addition, its utilization is common when monitoring elements like data amount, quality, and validity (Zheng et al., 2019; Guo et al., 2020). As demonstrated in the accompanying diagram, this offers more transparency and allows for creating a distinctive and global ID (Kinai et al., 2020; Xu et al., 2021; Cheng & Shaoqin, 2020; Wang et al., 2021).

The current identity management system confronts several significant obstacles. Identity theft is one of the most significant problems (Hao et al., 2021; Qu et al., 2021; Sun et al., 2022; Bao et al., 2020; Gong-Guo & Wan, 2021; Fang et al., 2022; Kim et al., 2022; Srivastava et al., 2019; Dhar et al., 2021). Identity theft rises when people share personal information online with illegitimate sites

Figure 7.
Designing a global ID with blockchain



or services. Internet apps store data on centralized servers, making it easier for hackers to obtain sensitive data (Qu et al., 2021).

Second challenge: username and password. A new online service requires a new username and password (Gong-Guo & Wan, 2021; Noh & Rhee, 2020). It's hard to remember several service login credentials (Kinai et al., 2020). In addition, keeping several authentication profiles up to date is difficult (Fang et al., 2022; Kim et al., 2022; Srivastava et al., 2019; Dhar et al., n.d.; Chalaemwongwan & Kurutach, 2018; Choi & Kim, 2020).

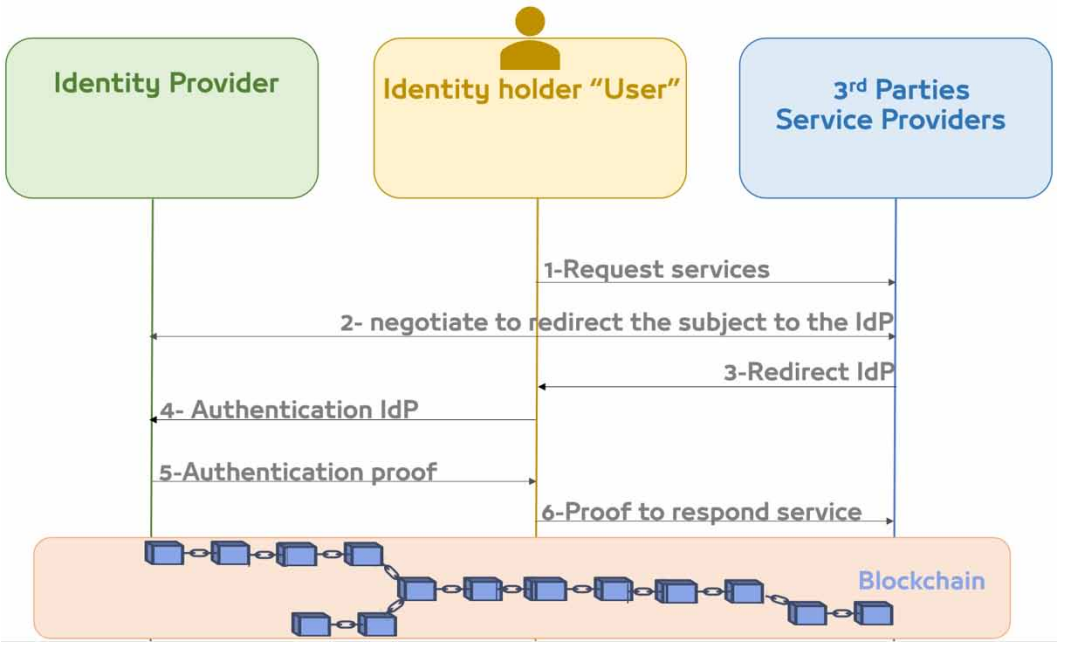
The third major issue is user control over personally identifiable information (PII) (Kim et al., 2022; Srivastava et al., 2019; Dhar et al., 2021; Chalaemwongwan & Kurutach, 2018; Choi & Kim, 2020; Gong-Guo & Wan, 2021). They have no idea how frequently or in what locations their personal information has been transmitted without their permission (Wang et al., 2021). Thus, an innovative identity management technique is needed (Srivastava et al., 2019; Dhar et al.,2021). By generating a universal ID that can be used for many different things, blockchain identity management enables people to control their identity (Ismail et al., 2022).

As seen in the image below, blockchain provides a potential answer to the aforementioned problems by consumers' confidence that no one else may disclose their PII without their permission (Xue et al., 2022). Digital identities that are secure and owned by the person can be made by anyone, there is no need to create numerous usernames and passwords, and we can protect identities using blockchain.

THE PROPOSED BLOCKCHAIN FRAMEWORK FOR IDENTITY MANAGEMENT SYSTEM BASED ON THE INTERNET OF THINGS

Blockchain systems can transform various aspects, moving away from more centrally protected networks and toward more decentralized structures seen as one of the most revolutionary and groundbreaking aspects of technology (Hao et al., 2021; Qu et al., 2021; Sun et al., 2022; Bao et al., 2020;

Figure 8.
Blockchain offers a potential solution



Gong-Guo & Wan, 2021; Fang et al., 2022; Kim et al., 2022; Srivastava et al., 2019; Dhar et al., n.d.; Chalaemwongwan & Kurutach, 2018; Choi & Kim, 2020; Noh & Rhee, 2020; Wang et al., 2020; Kinai et al., 2020; Xu et al., 2021; Cheng & Shaoqin, 2020). This level of decentralization is based on the idea that all nodes have equal access to network data. Since all nodes have equal access to network data, any extra chance for oversight could have significant effects, especially if it is easy to link a person to a transaction. In other words, when it comes to blockchain infrastructures, decentralization, and privacy are tightly related (Xue et al., 2022).

The European Blockchain Services Infrastructure (EBSI) project is really the most ambitious blockchain infrastructure endeavor in Europe. EBSI is being developed for cross-border government services and will be launched in 2019 by the EC, governments from member states, and the European Court of Auditors, after joining forces as part of the European Blockchain Partnership (Ismail et al., 2022; Xue et al., 2022; Geetha & Balakrishnan, 2021; Patel et al., 2019; Cheng et al., 2022; Xue et al., 2022; Nikhitha & Kumara, 2020). The longer-term plan is making EBSI compatible with other governmental and commercial blockchain systems. EBSI, taken at face value, appears to be an effort by policymakers to interact with the technology and learn how to control it by simply using it themselves (Xue et al., 2022). Because EBSI is a public permissioned blockchain, only trustworthy institutions will add blocks to the chain, but anybody may read and verify (Nikhitha & Kumara, 2020). Consequently, a governance mechanism will be needed for public permissioned blockchains. One of the four foundation use cases of EBSI is the 'Diploma Use Case', which involves storing cryptographic evidence of digital degrees on a blockchain network (Patel et al., 2019). The European Self-Sovereign Identity Framework (ESSIF) —a pure SSI framework expanded and tailored to European values and legal frameworks, namely the GDPR law and the eIDas trust framework—is the foundation for the use case (Xue et al., 2022). Under this new SSI model, people will get their own digital credentials, which they can store in wallets that they own and manage (Patel et al., 2019). Recipients get complete control over their identities and data in the process (Geetha & Balakrishnan, 2021). Except for the attestation of issuance and any other relevant modifications to the status of a digital credential, no personal information will be maintained on the chain (Nikhitha & Kumara, 2020). Any third party that the citizen has shared a credential with will confirm the issued digital credential's origin (for the holder and issuer) and status (valid, revoked, suspended, or expired) (Ismail et al., 2022).

People need a better way to keep track of their identification than paper documents. People would be able to instantly check and validate their identity with the aid of the suggested framework for Blockchain Identity management (Geetha & Balakrishnan, 2021). This may be accomplished by developing a special ID number enabling organizations to access the user's identification papers (Geetha & Balakrishnan, 2021). After acquiring an ID number, users must submit official IDs to IPFS and have their addresses hashed and registered in the blockchain (Xue et al., 2022). The system will take the personal data from these IDs so the user may self-verify their information (Geetha & Balakrishnan, 2021).

Data is user-owned. It helps users decide what to share with companies (Geetha & Balakrishnan, 2021). Identity seekers cannot access data without consent. At the same time, smart contracts with business logic may calculate a user's trust score based on the data they offer when establishing a self-sovereign identity. Every time a business needs to access a person's personal information for authentication reasons, a notice is sent to the person who has received that identification. Third parties can use the identifying information for identity verification once the user gives permission for the firms to access their records. Additionally, people will track the function that their PII has served.

Blockchains do not keep user data (Ismail et al., 2022). Only the blockchain will store identity holder-business transactions. For instance, if an immigration authority uses the system to confirm a person's identification, they will publish the transaction to the blockchain and made available to all associated nodes. Assume, for instance, that Ahmed must provide ID to study overseas. As a result, the school centre's identification may be promptly verified thanks to the blockchain-based identity management system. Ahmed will provide the center with the special ID number so they may request

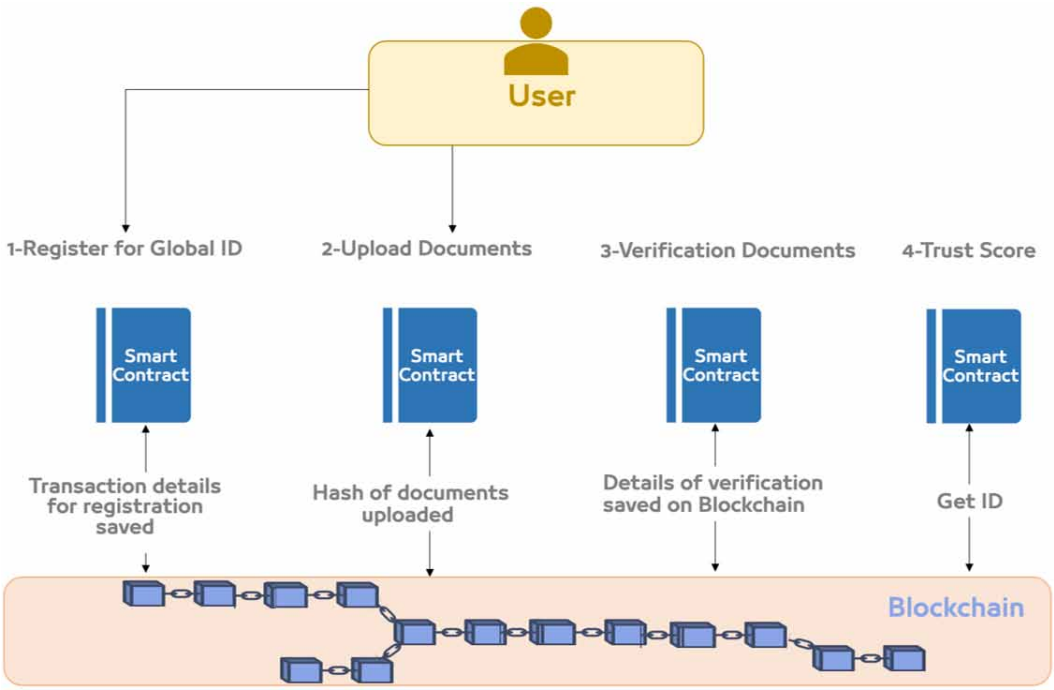
information access. They will record the transaction on the blockchain when he confirms the request and the education hub reviews his supporting documentation.

As previously stated, using blockchain identity management, smart contracts can activate business principles and assign a trust score to each user (Cheng et al., 2022). Organizations can utilize the trust score produced by smart contracts to instantly verify the identity of users (Geetha & Balakrishnan, 2021). By adding more papers to the app, a user can raise their trust rating. It is possible to determine if an account is legitimate or suspect based on the user's trust score (Xue et al., 2022). Additionally, identification must be utilized frequently to keep or improve the trust rating (Ismail et al., 2022). For the first six months after signing up, a user may be regarded as a beginner, allowing them the opportunity to build their trust score (Wang et al., 2020). They must upload the necessary data within that time (Wang et al., 2021; Ismail et al., 2022; Xue et al., 2022a). For instance, if the HSBC Bank has to verify a person's legitimacy before lending him money, they may look at their trust score (Geetha & Balakrishnan, 2021). It saves the bank time and money by determining trustworthiness (Xue et al., 2022b).

The security and privacy level can be increased by successfully deploying the suggested Blockchain Framework for identity management. The immutable and decentralized ledger lets third parties validate user data quickly and cheaply. For instance, if the user has to create a new bank account or submit a loan application, he or she typically has to provide many identification documents to finish the manual verification procedure, which might take weeks. However, a blockchain-based identity might speed up the process by immediately exchanging relevant information (Xue et al., 2022b). In addition, a user might not have to keep track of many IDs, which would cut down on costs and work (Nikhitha & Kumara, 2020).

A tourist must also bring certain documents besides their passport for clearance and security checks at the airport (Gong-Guo & Wan, 2021). An individual may use a common blockchain-based

Figure 9.
Using smart contracts in blockchain



identity throughout the entire process, from purchasing a ticket to clearing security checks, boarding an aircraft, and relocating to a new nation. When identities are decentralized, there is no need for time-consuming security checks or other processes. Therefore, the procedure may be expedited for both tourists and authorities thanks to blockchain identity management.

Additionally, a user may be required to provide several forms of identification evidence, such as proof of age, proof of employment, and proof of address, among others, while engaging in any legal procedure (Noh & Rhee, 2020). People may not need to carry several documents with them everywhere they go with the use of blockchain identity management. Government agencies and legal entities may use a single blockchain-based identification to validate an individual. As a result, doing a comprehensive background check is no longer required.

Additionally, when a person purchases online, they are prompted to enter details like their name, email address, phone number, and shipping address (Patel et al., 2019). Every time customers register for an account at an e-commerce site, they must go through this tedious and time-consuming process again. Therefore, using a single identification number to register for several e-commerce sites can save users time and effort.

There is currently no set standard for doing a background check on employees (Xue et al., 2022b). In the international job market, it is crucial to verify the accuracy of information provided by applicants in resumes, old letters, or reference letters. With the user's consent, the blockchain ecosystem may be used to immediately request the validation of the data included in an employee's résumé. The following four advantages of implementing the suggested blockchain framework for identity management are from the user's perspective (Wang et al., 2021; Ismail et al., 2022; Xue et al., 2022a).

Global ID

Each user that registers on the blockchain identity management system will be given their own unique identification number (Choi & Kim, 2020; Gong-Guo & Wan, 2021; Noh & Rhee, 2020; Wang et al., 2020). They save all personally identifiable information about the user on their device and encrypt using an IPFS-backed unique ID number. Through blockchain identity management, users may immediately identify themselves by sharing unique IDs with any third party.

Consent

Blockchain-based identity management does not store user data. Smart contracts govern data distribution. Therefore, on the blockchain, data modification is not feasible (Kinai et al., 2020; Xu et al., 2021' Cheng & Shaoqin, 2020). A blockchain-connected identity management system protects identity holders too. The user must consent to any data exchange. Users must control their personal info.

Decentralized

Users' personal identifying documents will not be kept on a central server. Users' devices are protected from large-scale data breaches via IPFS, which stores every document that identifies them. Hackers cannot get identifying information by using the Blockchain identity management system supported by IPFS (Xue et al., 2022b). The system will not have a single point of failure (SPOF) since it will be decentralized (Wang et al., 2021). The system's single point of failure is that component; should it malfunction, the entire system will cease to function. Because there is no SPOF, the system is guaranteed to never be compromised.

A Global Ecosystem

Borderless blockchain identity management. Thus, users can use the platform outside their nation to verify their identity (Ismail et al., 2022; Xue, 2022b). The many components of the proposed framework were taken from prior studies, books, articles, conference papers, and journals related to the blockchain (Dhar et al., n.d.; Chalaemwongwan & Kurutach, 2018; Choi & Kim, 2020; Gong-Guo & Wan, 2021; Noh & Rhee, 2020; Wang et al., 2020; Kinai et al., 2020; Xu et al., 2021; Cheng

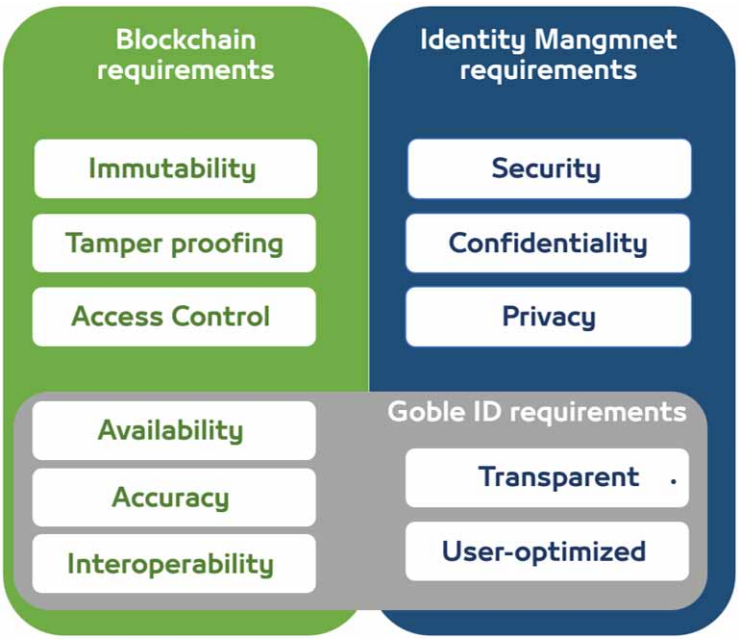
& Shaoqin, 2020; Wang et al., 2021; Ismail et al., 2022; Xue et al., 2022; Geetha & Balakrishnan, 2021; Patel et al., 2019; Cheng et al., 2022; Xue et al., 2022; Nikhitha & Kumara, 2020). Several studies on specific blockchain applications in various fields provide insight into technical issues, such as identity management systems and blockchain consensus methods. The essential elements of the proposed model are derived from these views. The model made it possible to formulate all components related to the examined theories of such views. As a consequence, expert evaluations have been used to rate the model's constituent parts (Dhar et al., n.d.; Chalaemwongwan & Kurutach, 2018; Choi & Kim, 2020; Gong-Guo & Wan, 2021; Noh & Rhee, 2020; Wang et al., 2020; Kinai et al., 2020; Xu et al., 2021; Cheng & Shaoqin, 2020; Wang et al., 2021; Ismail et al., 2022; Xue et al., 2022; Geetha & Balakrishnan, 2021; Patel et al., 2019; Cheng et al., 2022; Xue et al., 2022; Nikhitha & Kumara, 2020).

Such an investigation has aided the model's creation. The accompanying graphs detail 16 features that have been chosen to develop a blockchain model for an identity management system after a thorough analysis of the ideas present in the relevant field (Dhar et al., n.d.; Chalaemwongwan & Kurutach, 2018; Choi & Kim, 2020; Gong-Guo & Wan, 2021; Noh & Rhee, 2020; Wang et al., 2020; Kinai et al., 2020; Xu et al., 2021; Cheng & Shaoqin, 2020; Wang et al., 2021; Ismail et al., 2022; Xue et al., 2022; Geetha & Balakrishnan, 2021; Patel et al., 2019; Cheng et al., 2022; Xue et al., 2022; Nikhitha & Kumara, 2020). In the final section, these components will be more thoroughly examined to identify the most important features to be included in the model.

We have grouped the essential feature of the framework under the two perspectives being considered, as can be seen in Figure 10. First, blockchain encompasses six attributes, namely Access Control (Dhar et al., n.d.; Chalaemwongwan & Kurutach, 2018; Choi & Kim, 2020), Accuracy, Availability (Gong-Guo & Wan, 2021), Immutability (Xu et al., 2021), Interoperability (Wang et al., 2021), and Tamper proofing (Ismail et al., 2022).

Second, identity management encompasses five attributes, namely: Security (Xue et al., 2022a; Geetha & Balakrishnan, 2021; Patel et al., 2019; Cheng et al., 2022), Confidentiality (Patel et al.,

Figure 10.
The proposed framework



2019), Privacy (Cheng et al., 2022), Transparent (Xue et al., 2022), and User-optimised (Nikhitha & Kumara, 2020).

VALIDATING END ASSESSMENT OF THE SUGGESTED FRAMEWORK

A realistic evaluation approach is used to evaluate the framework, which depends on professional groups moving through several stages, as shown in Figure 11. In addition, the realistic evaluation is useful for validating a model with attention paid to the data's sources and verifiers, not just for widely acknowledged relevance but also concerning more contentious topics.

Model evaluation aims to examine the patterns of inter-rater agreement between subject-matter experts regarding the proposed model's various components (Sun et al., 2022; Boa et al., 2020; Gong-guo & Wan, 2021; Fang et al., 2022; Kim et al., 2022; Srivastava et al., 2019). Various experts were questioned for their opinions on the importance of each factor, taking different points of view into account. For analyzing professional views, it is important to utilize software that makes it easier to execute data manipulations and identify various factors recognized as crucial to determining the worth of various elements featured in the suggested model. The Statistical Package for Social Sciences (SPSS) was used exclusively during this stage.

After introducing the list of components for all parts of the recommended paradigm, which specifically lists six components for blockchain and five for identity management. Everything may subsequently be adequately appreciated and comprehended regarding all dimensions.

An online survey was implemented to measure the importance of certain factors on a four-point scale, with 1 being 'Not Important' and 4 representing 'Very Important.' The SPSS software was employed to calculate the overall average opinion, resulting in an appraisal of all relevant aspects.

Figure 11.
Four steps for validating end assessment of the suggested model

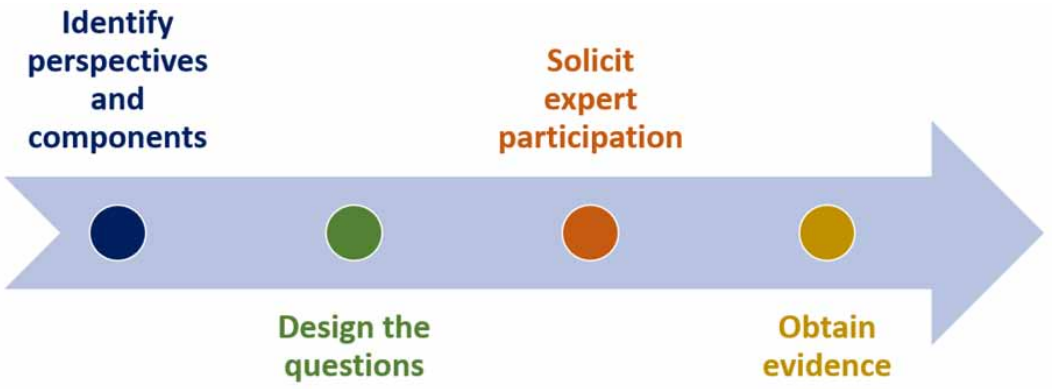
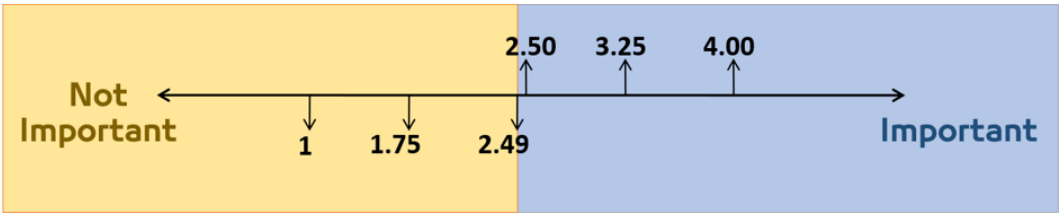


Figure 12.
Measurements with a four-point scale



In November 2022, the survey was made accessible online to 35 experts in total, along with an explanation of the purpose of the questionnaire and the criteria used to choose the experts to participate. The goal and purpose of the questionnaire were also clearly stated, and data confidentiality was guaranteed. The results of one of the sample t-tests, which is concerned with determining whether or not the population mean (μ) may be shown to be equal to a postulated value (μ0), as well as the results of the descriptive statistics are described in the table below. The significance threshold, (alpha), with an usual value of 0.05, is chosen to reach a judgment. Accordingly, for each item:

- if Sig. is less than or equal to α, H0 is rejected; or
- if Sig. is greater than α, H1 is rejected.

The evaluation findings are shown in Table 2. The alternative hypothesis (H1) is accepted for all items since the significance value (Sig.) for each item is less than 0.05 (p.05), which indicates that the null hypothesis (H0) is rejected. Additionally, the mean of all times is observed to be considerably larger than 2.49; as a result, all elements are considered significant in the proposed model.

CONCLUSION

The blockchain ecosystem has an excellent time and cost efficiency. Furthermore, both organizations and customers see reduced costs associated with identity verification (Alladi et al., 2022; Meng et al., 2021; Hewa et al., 2020; McGhin et al.,2019; Gasimov & Aliyeva, 2021). Additionally, everyone on the network has access to the transactions recorded on the blockchain (Ray et al., 2021). Therefore, every transaction that has been made has provable legitimacy (Bajoudah et al., 2019). Additionally, it guarantees the confidentiality of the transactions for all parties linked to the blockchain (Alladi et al., 2022). Instead of storing data on a single server, decentralization distributes information among all network nodes, removing a single point of failure. Users can also request that the company confirm their identification on a cross-border basis (Xu et al, 2021).

We conducted this study to learn more about the blockchain paradigm for managing identities. This study has produced an overview of the blockchain framework for identity management, which is

Table 2.
The expert evaluation findings

	Items	Sig (2-Tailed)	Mean	Attitude	Accepted Hypothesis
Blockchain	Item 1: Immutability	.040	3.63	Very Important	**Alternative**
	item 2: Tamper proofing	.022	3.75	Very Important	**Alternative**
	Item 3: Access Control	.011	3.85	Very Important	**Alternative**
	Item 4: Availability	.032	3.31	Very Important	**Alternative**
	Item 5: Accuracy	.014	3.30	Very Important	**Alternative**
	Item 6: Interoperability	.023	3.54	Very Important	**Alternative**
Idenity managent	Item 7: Security	.031	3.60	Very Important	**Alternative**
	Item 8: Confidentiality	.015	3.80	Very Important	**Alternative**
	Item 9: Privacy	.034	3.62	Very Important	**Alternative**
	Item 10: Transparent	.089	3.53	Very Important	**Alternative**
	Item 11: User-Optimized	.012	3.63	Very Important	Alternative

validated and acknowledged as being able to prove the success of this model. Additionally, it provides expert reviews of the various model components, including techniques, tactics, and analyses.

The results imply that the degree to which the experts adhere to the components of the proposed model is very important. Furthermore, such findings show that the recommended model is based on solid theoretical foundations of research concerning two research approaches.

REFERENCES

Abreu, A. W. dos S., Coutinho, E. F., & Bezerra, C. I. M. (2022). Performance evaluation of data transactions in blockchain. *IEEE Latin America Transactions*, *20*(3), 409–416. doi:10.1109/TLA.2022.9667139

Alemany, P., Vilalta, R., Munoz, R., Casellas, R., & Martinez, R. (2022). Evaluation of the abstraction of optical topology models in blockchain-based data center interconnection. *Journal of Optical Communications and Networking*, *14*(4), 211–221. doi:10.1364/JOCN.447833

Alladi, T., Chamola, V., Sahu, N., Venkatesh, V., Goyal, A., & Guizani, M. (2022). A comprehensive survey on the applications of blockchain for securing vehicular networks. *IEEE Communications Surveys and Tutorials*, *24*(2), 1212–1239. doi:10.1109/COMST.2022.3160925

Attaran, M. (2020). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management*, 1–14. doi:10.1080/20479700.2020.1843887

Baig, M. J. A., Iqbal, M. T., Jamil, M., & Khan, J. (2020). IoT and blockchain based peer to peer energy trading pilot platform. In *2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (pp. 402-406). doi:10.1109/IEMCON51383.2020.9284869

Bajoudah, S., Dong, C., & Missier, P. (2019). Toward a decentralized, trust-less marketplace for brokered IoT data trading using blockchain. In *2019 IEEE International Conference on Blockchain (Blockchain)* (pp. 339-346). doi:10.1109/Blockchain.2019.00053

Bao, Z., Wang, Q., Shi, W., Wang, L., Lei, H., & Chen, B. (2020). when blockchain meets SGX: An overview, challenges, and open issues. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 170404–170420. doi:10.1109/ACCESS.2020.3024254

Bhaskar, P., Tiwari, C. K., & Joshi, A. (2020). Blockchain in education management: Present and future applications. *Interactive Technology and Smart Education*, *18*(1), 29–51. doi:10.1108/ITSE-07-2020-0102

Bhutta, M. N. M., Ahmed, I., Khan, M. A., Rehman, A., Zeshan, U., & Khan, M. A. (2021). A survey on blockchain technology: Evolution, architecture and security. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 61048–61073. doi:10.1109/ACCESS.2021.3072849

Chalaemwongwan, N., & Kurutach, W. (2018). A practical national digital ID framework on blockchain (NIDBC). *2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON),* 497-500. doi:10.1109/ECTICon.2018.8620003

Chang, S. E., Chen, Y. C., & Lu, M. F. (2019). Supply chain re-engineering using blockchain technology: A case of smart contract-based tracking process. *Technological Forecasting and Social Change*, *144*, 1–11. doi:10.1016/j.techfore.2019.03.015

Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How blockchain can impact financial services - The overview, challenges and recommendations from expert interviewees. *Technological Forecasting and Social Change*, *158*, 120166. doi:10.1016/j.techfore.2020.120166 PMID:32834134

Chen, R., Shu, F., Huang, S., Huang, L., Liu, H., Liu, J., & Lei, K. (2021). BIdM: A blockchain-enabled cross-domain identity management system. *Journal of Communications and Information Networks*, *6*(1), 44–58. doi:10.23919/JCIN.2021.9387704

Cheng, G., Chen, Y., Deng, S., Gao, H., & Yin, J. (2022). A blockchain-based mutual authentication scheme for collaborative edge computing. *IEEE Transactions on Computational Social Systems*, *9*(1), 146–158. doi:10.1109/TCSS.2021.3056540

Cheng, Y., & Shaoqin, H. (2020). Research on blockchain technology in cryptographic exploration. *2020 International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE)*, 120-123. doi:10.1109/ICBASE51474.2020.00033

Choi, N., & Kim, H. (2020). Hybrid blockchain-based unification ID in smart environment. *2020 22nd International Conference on Advanced Communication Technology (ICACT),* 166-170. doi:10.23919/ICACT48636.2020.9061430

Dhar, S., Khare, A., & Singh, R. (2021). Advanced security model for multimedia data sharing in internet of things. *Transactions on Emerging Telecommunications Technologies*, *4621*. Advance online publication. doi:10.1002/ett.4621

Dittmann, G., & Jelitto, J. (2019). A blockchain proxy for lightweight IoT DEVICES. *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 82-85. doi:10.1109/CVCBT.2019.00015

Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation Research Part E, Logistics and Transportation Review*, *142*, 102067. doi:10.1016/j.tre.2020.102067 PMID:33013183

Fakhri, D., & Mutijarsa, K. (2018). Secure IoT communication using blockchain technology. *2018 International Symposium on Electronics and Smart Devices (ISESD)*, 1-6. doi:10.1109/ISESD.2018.8605485

Fang, Z., Wang, J., Ren, Y., Han, Z., Poor, H. V., & Hanzo, L. (2022). Age of information in energy harvesting aided massive multiple access networks. *IEEE Journal on Selected Areas in Communications*, *40*(5), 1441–1456. doi:10.1109/JSAC.2022.3143252

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*, *51*, 102029. doi:10.1016/j.ijinfomgt.2019.10.014

Furneaux, N. (2018). Understanding the Blockchain. In I. N. Furneaux (Ed.), *Investigating cryptocurrencies: Understanding, extracting, and analyzing blockchain evidence* (pp. 39–65). Wiley. doi:10.1002/9781119549314.ch3

Garg, K., Saraswat, P., Bisht, S., Aggarwal, S. K., Kothuri, S. K., & Gupta, S. (2019). A comparitive analysis on e-voting system using blockchain. *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 1-4. doi:10.1109/IoT-SIU.2019.8777471

Gasimov, V. A., & Aliyeva, S. K. (2021). Using blockchain technology to ensure security in the cloud and IoT environment. *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 1-5. doi:10.1109/HORA52670.2021.9461397

Geetha, V., & Balakrishnan, B. (2021). A user authentication and access control scheme for IoT-based healthcare using blockchain. *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1-7. doi:10.1109/ICCCNT51525.2021.9579992

Gong-Guo, Z., & Wan, Z. (2021). Blockchain-based IoT security authentication system. *2021 International Conference on Computer, Blockchain and Financial Development (CBFD),* 415-418. doi:10.1109/CBFD52659.2021.00090

Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020). Evaluation and demonstration of blockchain applicability framework. *IEEE Transactions on Engineering Management*, *67*(4), 1142–1156. doi:10.1109/TEM.2019.2928280

Gunanidhi, G. S., & Krishnaveni, R. (2022). Improved security blockchain for iot based healthcare monitoring system. *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, 1244-1247. doi:10.1109/ICAIS53314.2022.9742777

Guo, X., Guo, Q., Liu, M., Wang, Y., Ma, Y., & Yang, B. (2020). A certificateless consortium blockchain for IoTs. *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, 496-506. doi:10.1109/ICDCS47774.2020.00054

Gupta, P., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2021). Towards a blockchain powered IoT data marketplace. *2021 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, 366-368. doi:10.1109/COMSNETS51098.2021.9352865

Hao, X., Yeoh, P. L., Wu, T., Yu, Y., Li, Y., & Vucetic, B. (2021). Scalable double blockchain architecture for IoT information and reputation management. *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, 171-176. doi:10.1109/WF-IoT51360.2021.9595791

Hewa, T., Ylianttila, M., & Liyanage, M. (2020). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, *117*, 102857. doi:10.1016/j.jnca.2020.102857

Holbrook, J. (2020). Introduction to Blockchain Technologies. In J. Jolbrook (Ed.), *Architecting enterprise blockchain solutions* (pp. 1–28). Wiley. doi:10.1002/9781119557722.ch1

Iqbal, M., & Matulevičius, R. (2021). Exploring sybil and double-spending risks in blockchain systems. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 76153–76177. doi:10.1109/ACCESS.2021.3081998

Islam, M. A., & Madria, S. (2019). A permissioned blockchain based access control system for IoT. *2019 IEEE International Conference on Blockchain (Blockchain)*, 469-476. doi:10.1109/Blockchain.2019.00071

Ismail, S., Dawoud, D., & Reza, H. (2022). Towards a lightweight identity management and secure authentication for IoT using blockchain. *2022 IEEE World AI IoT Congress (AIIoT)*, 77-83. doi:10.1109/AIIoT54504.2022.9817349

Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., & Irani, Z. (2020). A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International Journal of Information Management*, *50*, 302–309. doi:10.1016/j.ijinfomgt.2019.08.012

Khan, M. A., & Salah, K. (2017). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. doi:10.1016/j.future.2017.11.022

Kim, M., Lee, S., Park, C., Lee, J., & Saad, W. (2022). Ensuring data freshness for blockchain-enabled monitoring networks. *IEEE Internet of Things Journal*, *9*(12), 9775–9788. doi:10.1109/JIOT.2022.3149781

Kinai, A., Otieno, F., Bore, N., & Weldemariam, K. (2020). Multi-factor authentication for users of non-internet based applications of blockchain-based platforms. *2020 IEEE International Conference on Blockchain (Blockchain),* 525-531. doi:10.1109/Blockchain50366.2020.00076

Kleinknecht, L. (2021). Can Blockchain capabilities contribute to sustainable supply-chain governance? *IEEE Engineering Management Review*, *49*(4), 150–154. doi:10.1109/EMR.2021.3123205

Kshetri, N., & Voas, J. (2018). Blockchain in developing countries. *IT Professional*, *20*(2), 11–14. doi:10.1109/MITP.2018.021921645

Liang, W., Zhang, D., Lei, X., Tang, M., Li, K.-C., & Zomaya, A. Y. (2021). Circuit copyright blockchain: Blockchain-based homomorphic encryption for IP circuit protection. *IEEE Transactions on Emerging Topics in Computing*, *9*(3), 1410–1420. doi:10.1109/TETC.2020.2993032

Liu, G., Wu, J., & Wang, T. (2021). Blockchain-enabled fog resource access and granting. *Intelligent and Converged Networks*, *2*(2), 108–114. doi:10.23919/ICN.2021.0009

López Peña, M. A., & Muñoz Fernández, I. (2019). SAT-IoT: An architectural model for a high-performance fog/edge/cloud IoT platform. *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 633-638. doi:10.1109/WF-IoT.2019.8767282

Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications*, *125*, 251–279. doi:10.1016/j.jnca.2018.10.019

Malik, S., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2019). TrustChain: Trust management in blockchain and IoT supported supply chains. *2019 IEEE International Conference on Blockchain (Blockchain)*, 184-193. doi:10.1109/Blockchain.2019.00032

McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in Healthcare Applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, *135*, 62–75. doi:10.1016/j.jnca.2019.02.027

Meng, T., Zhao, Y., Wolter, K., & Xu, C.-Z. (2021). On consortium blockchain consistency: A queueing network model approach. *IEEE Transactions on Parallel and Distributed Systems*, *32*(6), 1369–1382. doi:10.1109/TPDS.2021.3049915

Nikhitha, T. R., & Kumara, A. H. S. (2020). Implementation of secure data storage in blockchain with near-field communication authentication. *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, 768-773. doi:10.1109/ICIRCA48905.2020.9182976

Niya, S. R., Schiller, E., Cepilov, I., Maddaloni, F., Aydinli, K., Surbeck, T., Bocek, T., & Stiller, B. (2019). Adaptation of proof-of-stake-based blockchains for IoT data streams. *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 15-16. doi:10.1109/BLOC.2019.8751260

Noh, S., & Rhee, K.-H. (2020). Implicit authentication in neural key exchange based on the randomization of the public blockchain. *2020 IEEE International Conference on Blockchain (Blockchain)*, 545-549. doi:10.1109/Blockchain50366.2020.00079

Patel, S., Sahoo, A., Mohanta, B. K., Panda, S. S., & Jena, D. (2019). DAuth: A decentralized web authentication system using Ethereum based blockchain. In *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*, 1-5. doi:10.1109/ViTECoN.2019.8899393

Qu, Y., Pokhrel, S. R., Garg, S., Gao, L., & Xiang, Y. (2021). A blockchained federated learning framework for cognitive computing in industry 4.0 networks. *IEEE Transactions on Industrial Informatics*, *17*(4), 2964–2973. doi:10.1109/TII.2020.3007817

Ray, P. P., Dash, D., Salah, K., & Kumar, N. (2021). Blockchain for IoT-based healthcare: Background, consensus, platforms, and use cases. *IEEE Systems Journal*, *15*(1), 85–94. doi:10.1109/JSYST.2020.2963840

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its Integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173–190. doi:10.1016/j.future.2018.05.046

Rubio, D. M., Berg-Weger, M., Tebb, S. S., Lee, E. S., & Rauch, S. (2003). Objectifying content validity: Conducting a content validity study in social work research. *Social Work Research*, *27*(2), 94–104. doi:10.1093/swr/27.2.94

Sadek, I. M. M. A., & Ilyas, M. (2021). Securing IoT devices using blockchain concept. *2021 International Conference on Engineering and Emerging Technologies (ICEET)*, 1-6. doi:10.1109/ICEET53442.2021.9659792

Saif, A. N. M., & Islam, M. A. (2022). Blockchain in human resource management: A systematic review and bibliometric analysis. *Technology Analysis and Strategic Management*, 1–16. doi:10.1080/09537325.2022.2049226

Sanka, A. I., Irfan, M., Huang, I., & Cheung, R. C. (2021). A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Computer Communications*, *169*, 179–201. Advance online publication. doi:10.1016/j.comcom.2020.12.028

Solomon Doss, J. K., & Kamalakkannan, S. (2020). IoT system accomplishment using BlockChain in validating and data security with cloud. *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 60-64. doi:10.1109/I-SMAC49090.2020.9243412

Srivastava, G., Crichigno, J., & Dhar, S. (2019). A light and secure healthcare blockchain for IoT medical devices. *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, 1-5. doi:10.1109/CCECE.2019.8861593

Sun, Y., Zhang, L., Klaine, P., Cao, B., & Imran, M. A. (2022). Performance analysis on wireless blockchain IoT system. In M. A. Imran, B. Cao, L. Zhang, & M. Peng (Eds.), *Wireless blockchain: Principles, technologies and applications* (pp. 179–199). IEEE. doi:10.1002/9781119790839.ch8

Toufaily, E., Zalan, T., & Dhaou, S. B. (2021). A framework of blockchain technology adoption: An investigation of challenges and expected value. *Information & Management*, *58*(3), 103444. doi:10.1016/j.im.2021.103444

Urien, P. (2021). *A new IoT trust model based on TLS-SE and TLS-IM secure elements: A blockchain use case. In 2021 IEEE 18th Annual Consumer Communications & Networking Conference*. CCNC. doi:10.1109/CCNC49032.2021.9369485

Wamba, S. F., Jean Robert, K. K., Ransome, E. B., & John, G. K. (2019). Bitcoin, Blockchain and Fintech: A systematic review and case studies in the supply chain. *Production Planning and Control*, *31*(2-3), 115–142. doi:10.1080/09537287.2019.1631460

Wang, G., Shi, Z., Nixon, M., & Han, S. (2019). ChainSplitter: Towards Blockchain-Based Industrial IoT Architecture for Supporting Hierarchical Storage. *2019 IEEE International Conference on Blockchain (Blockchain)*, 166-175. doi:10.1109/Blockchain.2019.00030

Wang, X., Gao, F., Zhang, J., Feng, X., & Hu, X. (2020). Cross-domain authentication mechanism for power terminals based on blockchain and credibility evaluation. *2020 5th International Conference on Computer and Communication Systems (ICCCS)*, 936-940. doi:10.1109/ICCCS49078.2020.9118421

Wang, X., Garg, S., Lin, H., Piran, M. J., Hu, J., & Hossain, M. S. (2021). Enabling secure authentication in industrial IoT with transfer learning empowered blockchain. *IEEE Transactions on Industrial Informatics*, *17*(11), 7725–7733. doi:10.1109/TII.2021.3049405

Wolfond, G. (2017). A blockchain ecosystem for digital identity: Improving service delivery in canada's public and private sectors. *Technology Innovation Management Review*, *7*(10), 35–40. doi:10.22215/timreview/1112

Xu, S., Sun, A., Cai, X., Ren, Z., Zhao, Y., & Zhou, J. (2021). Post-quantum user authentication and key exchange based on consortium blockchain. *2021 IEEE 27th International Conference on Parallel and Distributed Systems (ICPADS),* 667-674. doi:10.1109/ICPADS53394.2021.00089

Xue, K., Luo, X., Ma, Y., Li, J., Liu, J., & Wei, D. S. L. (2022a). A distributed authentication scheme based on smart contract for roaming service in mobile vehicular networks. *IEEE Transactions on Vehicular Technology*, *71*(5), 5284–5297. doi:10.1109/TVT.2022.3148303

Xue, K., Luo, X., Tian, H., Hong, J., Wei, D. S. L., & Li, J. (2022b). A blockchain based user subscription data management and access control scheme in mobile communication networks. *IEEE Transactions on Vehicular Technology*, *71*(3), 3108–3120. doi:10.1109/TVT.2021.3138203

Zheng, W., Zheng, Z., Chen, X., Dai, K., Li, P., & Chen, R. (2019). NutBaaS: A blockchain-as-a-service platform. *IEEE Access : Practical Innovations, Open Solutions*, *7*, 134422–134433. doi:10.1109/ACCESS.2019.2941905

Sara Jeza Alotaibi is Deputy General Manager for Business Development and Partnerships and General Supervisor of the Gender Balance Center in the Institute of Public Administration in Saudi Arabia. She has authored a wealth of published papers and three books in the IT, and public administration arena, and is a driven, motivated young woman focused on education, self-development, professionalism and, above all, making a difference whilst teaching others how to do the same.