Journal Pre-proof

Blockchain Adoption for Authentication: A Survey

Hoang-Anh Pham, Cong T. Nguyen and Thuong C. Lam

PII: S2096-7209(25)00110-1
DOI: https://doi.org/10.1016/j.bcra.2025.100383
Reference: BCRA 100383

To appear in: *Blockchain: Research and Applications*

Received date: 19 February 2024
Revised date: 8 December 2024
Accepted date: 14 May 2025

Please cite this article as: H.-A. Pham, C.T. Nguyen and T.C. Lam, Blockchain Adoption for Authentication: A Survey, *Blockchain: Research and Applications*, 100383, doi: https://doi.org/10.1016/j.bcra.2025.100383.

Blockchain Adoption for Authentication: A Survey

Hoang-Anh Pham[a,b], Cong T. Nguyen[a,b], Thuong C. Lam[c]

[a]*Ho Chi Minh City University of Technology (HCMUT), Ho Chi Minh City, 72506, Vietnam*
[b]*Vietnam National University Ho Chi Minh City (VNU-HCM), Ho Chi Minh City, 71308, Vietnam*
[c]*HUTECH University, Ho Chi Minh City, 700000, VietNam*

Abstract

In network security, authentication is the crucial process to validate the identification of network participants, acting as the first defense mechanism to protect the networks from potential attacks. However, the conventional authentication approaches face many challenges, such as the reliance on a centralized entity, single point of failure, and the limited capacity and heterogeneity of devices in various types of networks. To address these problems, blockchain has recently emerged to be a promising solution, offering a secure and decentralized framework for authentication management. This article aims to provide a comprehensive survey on the applications of blockchain for authentication in diverse network environments. Particularly, we first provide an overview of blockchain, its related cryptography techniques, and common attacks on authentication processes. We then discuss diverse blockchain-based approaches proposed to address emerging issues in authentication in different types of networks including vehicular, IoT, healthcare, distributed computing, and other emerging application areas. Finally, we highlight important challenges, open issues, and future research directions of blockchain for future authentication systems.

Keywords:
Blockchain, Authentication, Vehicular Networks, IoT, Healthcare, Distributed Computing, Wireless Networking, Identity Management, UAV

1. Introduction

In network security, authentication is the process of validating the identification of users or entities connecting to systems [1]. This process is essential as the first defense mechanism to protect sensitive data from unauthorized access, thereby protecting systems from potential attacks including impersonation, data theft, and unauthorized system changes. Moreover, authentication has become more crucial because of the ever-growing use of distributed systems [2]. However, in the current stage of the internet when billions of devices are connected in various areas (e.g., IoT, healthcare, education, commerce), multiple authentication-related challenges arise.

Particularly, conventional authentication relies on a centralized entity to store identification data, such as a web server storing usernames and passwords in a relational database table. This centralized entity represents a single point of failure, which could be targeted by multiple attacks. For instance, protocols such as OAuth 2.0 [3], SAML [4], and Kerberos [5], which are the most widely used state-of-the-art methods for authentication, might face this centralization challenge. Particularly, the unavailability or compromise of critical servers, such as the authorization server in OAuth 2.0, the authentication server in Kerberos, or identity provider in SAML, can severely disrupt authentication services. Moreover, an insider with harmful intentions can exploit the lack of inherent data immutability of conventional systems, enabling attacks such as XML Signature Wrapping that manipulate the XML structure in SAML messages [6]. Besides, authentication in large-scale heterogeneous networks, such as IoT and edge computing, is another challenge. Because the devices in these networks are typically limited in computing resources, it is difficult to implement advanced security solutions on them. While the OAuth 2.0-based ACE-OAuth standard [7] can be implemented on these resource-constraint systems, it also raises privacy concerns as the Authorization Server may access sensitive client information. With the wireless nature of these networks, these devices are also more vulnerable to attacks including leakage of confidential information, identity spoofing, and message eavesdropping [1, 2].

To address these challenges, blockchain-based authentication is emerging as an effective solution. Particularly, a blockchain is a distributed database shared among multiple nodes in a network. Data is stored in a sequence of blocks linked via cryptography. Moreover, the nodes must follow a consensus mechanism to add data to a blockchain, thereby enhancing the security of the networks [8] [9]. As a result, blockchain-based approaches bring multiple advantages compared to conventional authentication, which can be summarized as follows.

- Decentralization: with blockchain-based authentication, the identification data is stored in multiple entities of networks instead of a centralized entity. Therefore, the single point of failure is removed, making systems more resistant to attacks.

- Tamper-proof: data stored on blockchains cannot be altered by any single entity, which makes blockchain-based

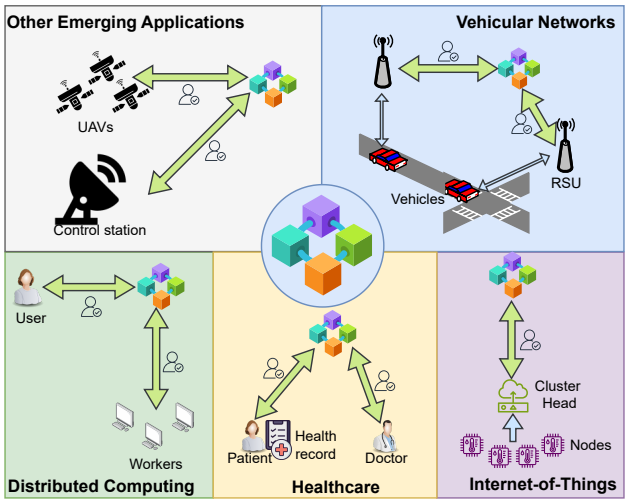

Figure 1: Application scenarios of blockchain-based authentication systems.

authentication systems more secure against data tampering [10] attempts from both outside attackers and malicious insiders.

- Transparency and Auditability: adding data to blockchain is transparent and auditable, enhancing the accountability of authentication [11], and providing traceability for changes.

- Anonymity and Privacy: leveraging cryptography enables anonymous blockchain-based authentication systems, thereby enhancing the privacy of users. This is an important feature when storing sensitive information, such as the medical conditions of patients in healthcare. Moreover, blockchain's inherent characteristics such as decentralization and smart contracts can be utilized to build self-sovereign identity platforms, enabling entities to have ownership and control over their digital identities [12].

With the aforementioned advantages, various approaches that utilize blockchain technology for authentication have been proposed in recent years. This paper aims to provide a comprehensive survey of these approaches. Particularly, we first provide an overview of blockchain-based authentication, including fundamentals of blockchains, authentication, and cryptography techniques. As illustrated in Fig. 1, we present a survey on applications of blockchain-based authentication in multiple areas including vehicular networks, IoT, healthcare, distributed computing, and other emerging application areas. For these applications, we provide detailed reviews and analyses on how blockchain-based authentication is leveraged to overcome the challenges of conventional authentication. Finally, we discuss the current challenges and open issues of blockchain-based authentication and introduce potential research directions for this technique in the future.

There are a few surveys with different focuses. For example, [13], [14], and [15] discuss authentication process in IoT. Moreover, [16], [17], and [18] discuss authentication in vehicular, healthcare, and distributed computing, respectively. Alternatively, there are surveys [19], [20], and [21] that investigate authentication approaches with broader focuses. Particularly, [19] focuses on multi-factor authentication, [20] focuses on attacks and defense mechanisms, and [21] focuses on biometric-based authentication. To the best of our knowledge, there is no survey in the literature that focuses on the application of blockchain technology for authentication. Given the significant advantages that blockchain technology can bring, this paper aims to fill the gap in the literature and contribute to the future development of blockchain-based authentication systems.

The rest of this paper is organized as follows. Section 2 provides the fundamental background of key concepts, including blockchain technology, cryptographic mechanisms, and attacks on authentication processes. Then, applications of blockchain-based authentication in vehicular networks, IoT, healthcare, and distributed computing are presented from Sections 3 to 7. Section 8 discusses challenges, open issues, and future research directions of blockchain-based authentication. Finally, Section 9 concludes this article.

2. Fundamental Background

In this section, we provide fundamental background on key concepts, techniques, and attacks that are frequently used in blockchain-based authentication systems.

2.1. Blockchain Technology

2.1.1. Overview

Blockchain introduces a novel method for managing data in a decentralized way. A blockchain is a distributed database or ledger where records are shared among nodes in a peer-to-peer network. Blockchain employs cryptographic hashes, digital signatures, and distributed consensus methods to guarantee that records cannot be altered once added to the blockchain without the agreement of other network participants. Therefore, data stored on the blockchain can be verified without a central entity.

2.1.2. Transactions

Transactions are the basic data structures that record transfers of tokens between users or other entities, i.e., smart contracts on a blockchain. A transaction specifies the identities of the sender and receiver, and the amount of tokens to be debited from or credited to their accounts. Two main cryptographic techniques are used to protect the authenticity of transactions:

- Hash functions: Hash functions randomly map any input to a unique fixed-length output in a one-way manner, preventing recovery of the input by pure computational infeasibility. Additionally, the probability of a strongly secured hash function such as SHA-256 to generate the same output for two different inputs is extremely small.

- Asymmetric Key: Each node generates a pair of keys: one public, one private. The private key is used to sign input

messages, creating a fixed-length signature. This signature can be verified by other entities using the public key: they employ a verification function to confirm that the signature originates from the corresponding private key. For identity purposes, nodes use the hash of their public key as a pseudonymous, permanent blockchain address. In transactions, inputs are signed with the sender's private key. The nodes in the network can then verify these transactions by checking if the signature matches the public address, thereby validating the input's authenticity.

As illustrated in Fig. 2, when a sender wants to send money to a recipient, first they create a transaction, which contains their address, the amount of money, the recipient's address, and their digital signature. Then they broadcast this transaction to the network. When a miner, i.e., a consensus participant, receives this transaction, they validate it using the sender's digital signature. The miner then includes multiple valid transactions into a block. If the block is mined successfully, the miner broadcasts the block to other nodes in the network to verify. If the block is verified successfully as the first block mined after the last block in the chain, these nodes integrate it as the latest block in the chain [9].

2.1.3. Blocks

A block, created by a node participating in the consensus process, contains transaction records. In the block's data structure, a hash pointer is kept. This data field is used to ensure the integrity of the transaction records, and that the adjacent blocks are organized in the correct order. Additionally, the Merkle tree data structure can be leveraged to generate the tamper evident digest in the transaction set of a block while requiring less on-chain storage. A hash pointer to a block is the hashcode of its concatenated data fields, stored as its header. A block stores the hashcodes of the reference blocks, indicating that it recognizes that the transactions in the reference blocks are created earlier than the new block's transactions. A set of transactions can form a Merkle tree with each leaf labeled with the hashcode of a transaction and each non-leaf node labeled with the hashcode of the concatenated labels of its two children. The root of a Merkle tree is called the Merkle digest/root. A block in lightweight form stores only the Merkle root of the selected transactions, which is sufficient for validation and synchronization. A node storing lightweight blocks must query its peer to retrieve the complete transaction records in the blocks [8, 22].

Apart from the Merkle digest, the block header and the hash pointers, a block may contain additional data fields, based on specifications of consensus schemes. In a blockchain, blocks are organized based on the hash pointers to their references/predecessors. The first block in every blockchain, namely the genesis block, has no reference and is the common ancestor block of all valid blocks. Depending on the number of references a block has, blocks can be organized in different forms, such as a linear linked list, as a tree of blocks, or as a Directed Acyclic Graph (DAG) [23]. Without specification, most of our discussion on blockchains is limited to the linear linked list case, where the order of the blocks is guaranteed.

2.1.4. Consensus Mechanisms

In a blockchain network, faulty nodes can behave maliciously or arbitrarily. Moreover, nodes can process misinformation due to connection latency, i.e., Byzantine failures. Therefore, the consensus mechanism is a core component to achieve distributed agreement of nodes about the state of the network. Moreover, the consensus mechanism governs other network's operations, such as transaction adding and incentive mechanisms. An example of a consensus mechanism is Proof of Work (PoW) which is used in public blockchain networks, most noticeably Bitcoin [24]. Particularly, PoW requires miners i.e., nodes participating in the consensus process, to solve cryptographic puzzles if they want to create new blocks. Because the puzzles take substantial processing power to solve, block creation is difficult, thereby deferring malicious manipulation of the blockchain. Another consensus mechanism is Proof of Stake (PoS), which is used in the current implementation of the public blockchain network Ethereum (Ethereum used PoW in its early stage) [25]. In particular, PoS chooses block creators based on nodes' monetary stake i.e., the ownership of cryptocurrency tokens. The block creators are chosen randomly, with higher odds assigned to nodes with larger stakes. PoS networks can be secured with incentive mechanisms, including rewarding honest nodes with newly minted tokens, while nodes' malicious behaviors can lead to the loss of their stakes.

2.2. Cryptography Mechanisms

2.2.1. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC), proposed in 1985 by Neal Koblitz and Victor Miller, is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. In ECC, a key pair is a set of two points on an elliptic curve defined over a finite field. In particular, the private key is randomly selected and multiplied with a generator point on the curve to compute the public key [26].

The security of ECC relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is more difficult to solve than the integer factorization problem used in traditional cryptosystems such as Rivest–Shamir–Adleman (RSA). Moreover, in ECC, smaller key sizes provide equivalent security compared to that of RSA or Diffie-Hellman. Additionally, no known subexponential-time algorithms solve the ECDLP on suitably chosen curves. Therefore, ECC cryptosystems are more secure and efficient for a given key size, and more practical for embedded devices and blockchains [26].

2.2.2. Elliptic Curve Digital Signature Algorithm

Proposed in 1992 as a variant of the Digital Signature Algorithm (DSA), the Elliptic Curve Digital Signature Algorithm (ECDSA) is a cryptographic algorithm used to create a digital signature scheme optimized specifically for ECC implementations [27]. Leveraging the aforementioned advantages of ECC, ECDSA can reduce the signature and key sizes by roughly 20 times compared to those of RSA while maintaining the same security strength [28]. Therefore, ECDSA-ECC systems can significantly reduce bandwidth, computing power,

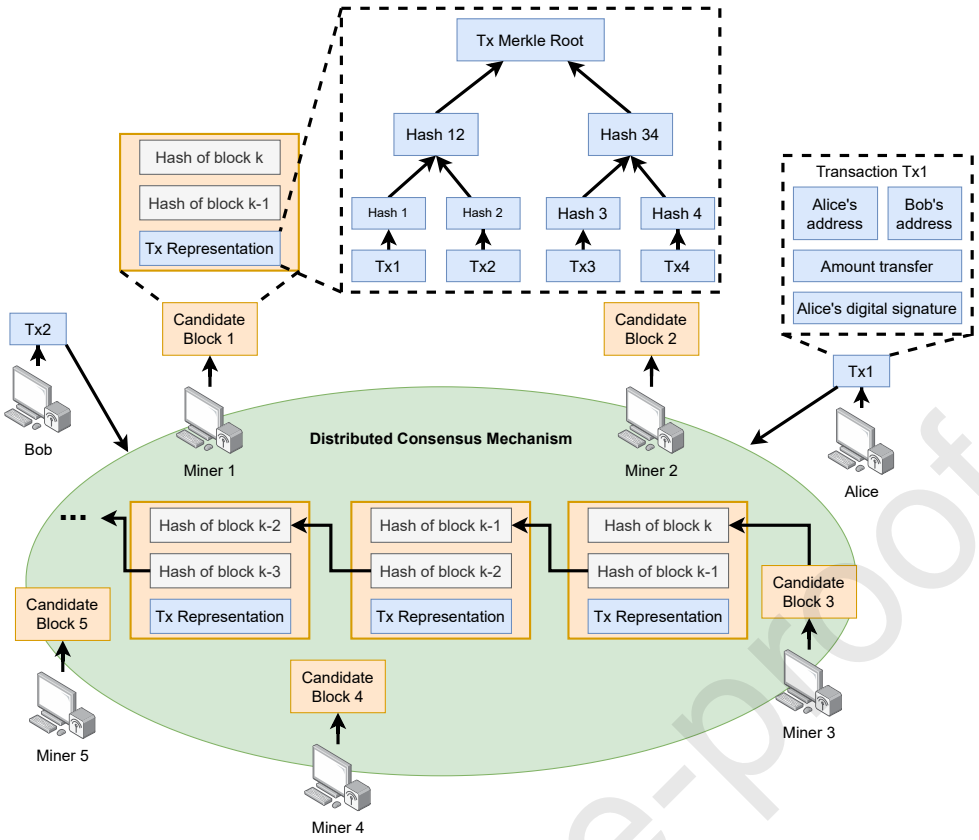

Figure 2: An illustration of a blockchain network.

and required storage compared to other approaches. As a result, the invention of ECDSA vastly expanded the adoption of ECC across multiple applications ranging from web browsers to blockchains [29].

2.2.3. Zero-Knowledge Proof

A zero-knowledge proof is a cryptographic method that allows one party (the prover) to validate knowledge of a piece of information to another party (the verifier) without revealing that piece of information [30]. Particularly, the verifier issues a random cryptographic challenge, to which the prover must respond with a solution that convinces the verifier of their knowledge. Moreover, the challenge space is large enough to prevent fraud. Zero-knowledge proofs enable authentication and identity validation without compromising privacy, making them applicable for blockchain consensus, voting, authentication systems, and other domains requiring validation with anonymity.

2.2.4. Secure Hash Algorithms

Secure Hash Algorithms (SHAs) are a family of cryptographic hash functions published by the National Institute of Standards and Technology. Particularly, SHAs are designed to provide one-way hash functions for creating unique fixed-length hash digests of electronic data as input [31]. Moreover, these digests cannot be regenerated without access to the input, thereby ensuring that the data has not been tampered with [32]. Therefore, SHAs are essential to detect unauthorized changes.

2.3. Attacks on Authentication Processes

2.3.1. Man-in-the-Middle Attacks

A Man-in-the-Middle (MITM) attack is a type of cyberattack where a malicious third party secretly takes control communication channel between two or more nodes in a network. In particular, the attacker can intercept, modify, or replace victims' communication traffic, often to steal credential information, spy on victims, or corrupt data [33]. For instance, an attacker can set up a public Wi-Fi network with a similar name to a legitimate network. Then, unaware users can connect to it, allowing the attacker to monitor all information they send. Some methods to prevent MITM attacks include using strong encryption or a Virtual Private Network (VPN) to ensure that the attacker cannot decipher the transmitted messages [34].

2.3.2. Replay Attacks

A replay attack is an attack on a security protocol when a malicious party replays messages from a different context into the intended context, thereby making honest participants think that the protocol is working as expected [35]. Particularly, an attacker can copy an entity's authentication message and use it to carry out authentication with another entity, regardless of whether the message is encrypted or not. Replay attacks can be effective to gain unauthorized access to sensitive data or to misdirect the participants. For example, in VANETs, an attacker can replay traffic-related messages that were exchanged by neighboring vehicles, causing confusion or misinformation.

Moreover, in this case, replaying a message about a clear road when there is a hazard can lead to accidents [36]. To defend against replay attacks, it is effective to include a timestamp in the transmitted data by ensuring that the data is only valid within a period of time. Moreover, a random number, namely nonce, can be generated each time the authentication takes place to act as a mark if the messages are replayed [34].

2.3.3. Impersonation Attacks

An impersonation attack happens when an attacker impersonates a legitimate node in a network [37]. For example, in IoT networks where devices can be compromised easily because of their limited computing resources, an attacker can impersonate other devices, thereby stealing data and spreading malware. To prevent impersonation attacks, authentication messages are required to include the identity of the sender. However, several forms of Impersonation Attacks target humans rather than protocols, making them difficult to defend against [34].

2.3.4. Non-repudiation Attacks

A non-repudiation attack happens when a node in a network illegitimately denies its action. For instance, in VANETs, a malicious vehicular node can deny receiving or sending a message to disrupt the flow of information in the network. Moreover, a node can launch an attack and deny its action, thereby avoiding detection and punishment. Using digital signature as proof of identity is an effective way to prevent non-repudiation attacks [34].

2.3.5. Insider Attacks

An insider attack occurs when an insider compromises the confidentiality, integrity, or availability of a network by taking advantage of their authorized access. The insider can be an employee or a contractor with granted access to the network. For instance, an IoT device in a smart home can be compromised to leak sensitive data to an attacker [22], or a malicious node could disrupt the communication between vehicles in vehicular networks, leading to safety risks [38]. Against insider attacks, potential defense mechanisms include classifying levels of access for insiders, analyzing behaviors to detect anomalies, and monitoring.

2.3.6. Modification Attacks

A modification attack is a type of cyberattack where an unauthorized entity gains access to and tampers with data [39]. The entity can modify messages in the network, change stored data, or reconfigure system hardware or network topologies. For example, if an attacker can change the patients' medical data at a hospital, it can lead to wrong diagnoses and treatment for their conditions. To defend against Modification Attacks, it is necessary to detect any modification to data, regardless of whether the modification is authorized or not, by mechanisms such as using one-way hash functions [34], storing the last modified timestamp with data, etc. Besides, modification attacks can be prevented by making confidential data immutable, i.e., unable to be modified.

2.3.7. Eavesdropping Attacks

An eavesdropping attack is a type of cyberattack where a malicious third party can listen to messages exchanged between two or more nodes in a network. Because the attacker does not modify the communication channel, it is difficult for nodes to detect that the attacker is eavesdropping on their messages. With this attack, unencrypted sensitive data is visible to the attackers. Strong encryption techniques are effective against eavesdropping attacks [34] by preventing the attackers from deciphering the messages.

3. Applications of Blockchain-based Authentication for Vehicular Networks

A vehicular network is a specialized communication system that enables vehicles to exchange information with each other and with roadside infrastructure, enhancing road safety, traffic management, and providing information services. It significantly improves transportation efficiency and driver convenience by enabling real-time traffic updates, automated toll payments, and enhanced navigation systems [40]. However, vehicular networks face distinct challenges in authentication, primarily due to the high mobility of vehicles, the need for rapid and secure communication, and the vulnerability to various cyberattacks. These challenges include ensuring the integrity and confidentiality of data exchanged, managing the dynamic and large-scale nature of vehicular networks, and safeguarding against impersonation and replay attacks. Moreover, the decentralized nature of these networks demands robust mechanisms to validate and authenticate vehicles without compromising user privacy or system efficiency [16, 40]. To address these problems, blockchain has emerged to be an effective solution: it enables decentralized management of identities to achieve privacy-preserving authentication, leverages cryptographic techniques to ensure data integrity and confidentiality, and provides a transparent and tamper-proof system for secure, real-time communication in vehicular networks.

3.1. Vehicular Ad-hoc Networks

Vehicular Ad-hoc Networks (VANETs) are a type of vehicular network specifically designed for vehicle-to-vehicle and vehicle-to-infrastructure communication. They are essential for intelligent transportation, enhancing road safety, and managing traffic by enabling real-time communication between vehicles and infrastructure. However, their dynamic nature, with high-speed vehicles and changing network topologies, presents significant challenges. These include ensuring rapid and secure authentication for reliable communication, maintaining driver and vehicle privacy, and protecting against security threats such as spoofing and message tampering. Additionally, the scalability of VANETs demands authentication mechanisms that can efficiently manage the large volume of vehicles without causing network delays or congestion [16]. Blockchain technology has recently emerged as a promising solution for these challenges. For example, in [41], the authors introduce a Blockchain-Assisted Coded Caching Certificate Revocation

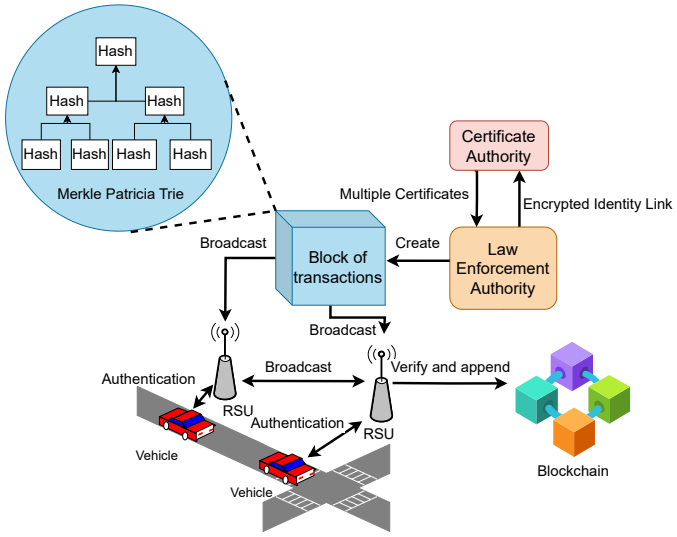

Figure 3: Blockchain-based authentication framework for VANETs employing Law Enforcement Authority [43].

List (BAC-CRL) for authentication in VANETs. The proposed framework combines blockchain technology with a multi-layer coded caching strategy to enhance certificate revocation processes. Particularly, blockchain is employed to create a network that connects regional Certificate Authorities (CAs) and Road-Side Units (RSUs). The blockchain network is responsible for managing and storing multipart Certificate Revocation Lists (CRL). This prevents On-Board Units, which have limited resources, from being overloaded with extensive revoking information. When a vehicle requests authentication, the system first checks the current CRL to make sure that the vehicle's credentials have not been revoked. Then the proposed framework employs the Efficient Anonymous Authentication Protocol (EAAP) [42] to facilitate anonymous authentication of the vehicle. Additionally, to reduce communication overhead and processing time, a multi-layer coded caching strategy is introduced to efficiently distribute the minimum required bits of CRLs. Security analysis demonstrates that the proposed system meets the needs of privacy-preserving authentication and retains data integrity. Moreover, simulation results show that the proposed framework achieves an average processing time of 3.13 milliseconds, which is at least 2 times better than the compared proposals.

Apart from distributed CRLs, another approach to decentralized authentication is by employing Law Enforcement Authority (LEA), as proposed in [43]. As illustrated in Fig. 3, the proposed framework utilizes two separate authentication mechanisms. In the first mechanism, the TA issues multiple certificates to a vehicle, each containing a public key, an expiration time, and an encrypted identity link that can only be decrypted by the LEA. These multiple certificates are hashed, and the hash value is stored on the blockchain in a Merkle Patricia Tree (MPT) data structure. This data structure allows the receiver of each message to verify the sender's authenticity using the Merkle proof. Thanks to the use of multiple certificates, only the LEA can access and decrypt the identity link of the vehicles, thus enabling anonymous authentication. These multiple certificates are combined together to form a block of transactions, which is broadcasted to the RSUs for verification by employing the second authentication mechanism. In this mechanism, ECDSA [27] is employed to facilitate digital signature generation and verification. After successfully verified, the block of transactions is appended to the blockchain by the RSUs. Additionally, the RSUs are employed to facilitate communications between vehicles, RSUs, and the LEA and form a cohesive network. Experiment results show that the proposed framework can achieve a certificate issuance or revocation throughput of over 180 transactions per second, an average latency of around 1.5 seconds, and distributed authentication by individual vehicles within 1 millisecond. Moreover, for 10 million certificates, the average authentication communication overhead is only 8.17KB.

In [44], the authors introduce an anonymous authentication protocol for VANET using Simulation-Extractable Zero-Knowledge Succinct Non-interactive Arguments of Knowledge (SE zk-SNARKs) combined with blockchain technology. The authentication process starts with the initialization phase, where the LEA generates essential parameters that are made available to all entities in the system. Simultaneously, Regional Certificate Authorities (RCAs) establish their unique keys, consisting of secret and corresponding public keys. These RCA keys are important for the system's integrity, as they are used for issuing and validating certificates for vehicles and RSUs. In the registration phase, RSUs and vehicles are registered with their respective RCAs and are issued credentials which are securely stored on the blockchain. In the authentication phase, these RCA-issued certificates are used to generate proofs for vehicle messages via SE zk-SNARKs. This process involves dividing the proof statement into two distinct components: a static part, which is computed once and securely stored on the blockchain, ensuring immutability and reuse for future proofs; and a dynamic part, uniquely generated for each authentication instance using fresh random elements, thereby ensuring that each message or transaction is authenticated with a specific and current proof. Security analysis demonstrates that the proposed approach satisfies authentication, anonymity, privacy preservation, and can mitigate MITM attacks. Additionally, performance evaluation shows that the proposed scheme introduces only 224 bytes communication overhead per authentication and takes 0.73 milliseconds for proof generation. Moreover, the impact of vehicle's speed and density on authentication delay is marginal, with the packet loss ratio being less than 0.09%.

To enable cross-domain authentication, in [45] the authors propose a blockchain-based framework for VANETs. This approach, namely BCGS, integrates blockchain technology and an efficient group signature scheme to provide anonymous and traceable cross-domain authentication. In particular, a modified secure group signature scheme based on the work in [46] is proposed to enable authentication in a single domain and register a temporary public key. This public key, verified by miners on the blockchain network, is then stored for device authentication by utilizing lightweight smart contracts. Additionally, to enhance efficiency, all smart contracts are designed to contain

only two atomic operations, i.e., read and write. Security analysis shows that the framework can resist various attacks such as replay, MITM, birthday collisions, and hijacking attacks. Simulation results show that the proposed system can achieve a latency of 0.03 seconds when processing 400 authentication queries across four domains. Moreover, it takes around 65 milliseconds for the framework to sign a message and 200 milliseconds to verify a message, which is comparable to the state-of-the-art approaches. Similarly, another cross-domain authentication framework is proposed in [47], where the authors propose an identity authentication architecture for VANETs based on blockchain technology. It employs the InterPlanetary File System (IPFS) [48] and smart contracts to enhance the management of certificates. Particularly, identity information submitted by the vehicle is verified by the TA, which then issues a Verifiable Credential (VC) stored on the IPFS network. The address of this VC file on the IPFS network and its hash are stored on the blockchain. When a vehicle requests authentication, a verifier, e.g., an RSU or another vehicle, retrieves the user's public key from the IPFS address and uses it to verify the digital signature on the VC. Additionally, the verifier checks the VC's integrity and authenticity by validating it against the information stored on the blockchain. Security analyses confirm the framework's resilience against replay, MITM, and privacy attacks. Moreover, experiment results show that the total authentication time is approximately 45.2 milliseconds.

In [49], the authors propose a novel blockchain-based mutual authentication and session key agreement protocol, namely B-HAS, to enable secure communication in VANETs. In particular, a hierarchical blockchain architecture is introduced, with auxiliary blockchains maintained by edge RSUs and a parent blockchain maintained by base RSUs and Registration Authority (RA), facilitating multi-vehicular domain authentication. The proposed protocol employs ECC and one-way hash functions to achieve authentication between vehicles and RSUs within the same region (intra-regional) as well as across regions (inter-regional). During intra-regional communication, the vehicle and edge RSU mutually authenticate each other by verifying message hashes before negotiating a session key. For inter-regional handovers, edge RSUs communicate to share vehicle authentication information over an authenticated channel. Performance evaluation clearly shows the efficiency of the proposed protocol via its low communication and computation overheads, i.e., 2144 bits and 106.44 ms for intra-vehicular, and 3616 bits and 211.92 for inter-vehicular. Another framework that utilizes multiple blockchains is proposed in [50]. Particularly, the authors propose a dual blockchain architecture for secure vehicle authentication and communication in VANET, namely D-BLAC. D-BLAC utilizes two blockchains: a Registration Blockchain (RBC) for decentralized vehicle registration using Proof-of-Authority consensus, and a Message Blockchain (MBC) for efficient transmission of emergency messages using Proof-of-Position consensus. Upon registration, vehicles receive a unique public-private key pair, which is stored on the RBC. The RBC employs the Proof-of-Authority consensus mechanism that utilizes RSUs as authority nodes to validate and add vehicle registration to the RBC. In the MBC, an algorithm is proposed for the storage and transmission of messages, in which only critical emergency data is permanently retained while other data is removed over time. This dual blockchain structure enhances efficiency and security by separating authentication and communication functions. Security analysis proves that the proposed framework can resist various attacks including replay, non-repudiation, modification, and impersonation. Performance evaluation shows that compared to existing approaches, the proposed framework improves the computational cost, throughput, transmission delay, and vehicle verification rate by at least 12.9%, 33.9%, 35%, and 18.7%, respectively.

In [51], the authors propose a novel authentication scheme for VANETs using blockchain technology to address issues such as the lack of transparency and vulnerabilities to attacks in conventional VANETs authentication mechanisms. The framework consists of three entities: vehicles, TAs, and RSUs. The vehicles first register to the network by encrypting their data using a combination of ECC and Advanced Encryption Standard (AES) [52]. This encrypted data is hashed using the Secure Hash Algorithm-256 (SHA-256) [53], and then appended to the blockchain by utilizing a special smart contracts function. When a vehicle requests authentication and sends its encrypted data, the TA verifies by generating the SHA-256 hash for the received data and comparing it to the data stored on the blockchain. The TA then issues digitally signed certificates for authenticated vehicles by employing the Elliptic Curve Digital Signature Algorithm (ECDSA) [27], and stores them on the blockchain. The role of the RSUs is to facilitate communication by relaying authentication data between the TA and the vehicles. Security analysis demonstrates the framework's resilience against insider, impersonation, and repudiation attacks.

3.2. Other Types of Vehicular Networks

Besides VANETs, blockchain technology has also been leveraged for authentication in other types of vehicular networks such as Vehicle-to-Grid (V2G), vehicular networks with roaming services, and smart transportation systems. For example, in [54], the authors propose an efficient blockchain-based authentication framework for energy trading applications in V2G networks. In particular, a blockchain-based three-phase process, which includes registration, searching, and authentication, was proposed for secure and anonymous transactions between electric vehicles (EVs), charging stations (CSs), and utility centers (UCs) in V2G networks. Additionally, to minimize communication and computation overheads on resource-constrained EVs, the lightweight Merkle Root Hash is employed in the mutual authentication mechanism. Moreover, security analysis demonstrates the framework's ability to mitigate impersonation, replay, and eavesdropping attacks, while also highlighting effective privacy preservation. Experimental results show that the proposed system outperforms existing approaches by at least 2.36 times in terms of computation and communication costs. Similarly, a blockchain-based framework is proposed in [55] for V2G networks. As illustrated in Fig. 4, The proposed framework features an energy trading scheme that leverages blockchain's distributed ledger to validate transactions, thus reducing intermediaries and enhancing

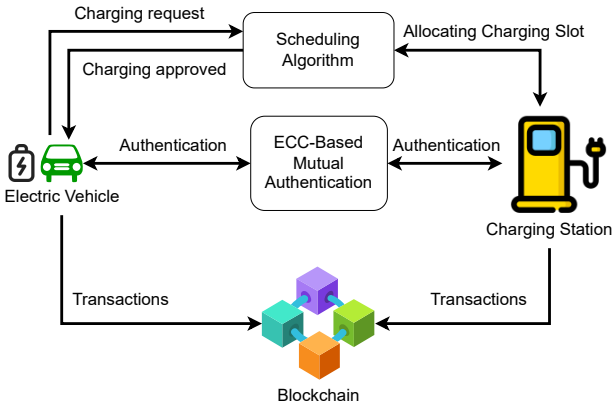

Figure 4: Vehicle-to-Grid network with ECC-based authentication and scheduling algorithm [55].

privacy and transparency. Particularly, EVs and CSs are mutually authenticated in the network via the lightweight ECC. Moreover, the framework utilized a CS scheduling algorithm that selects the optimal station by minimizing EVs' expected waiting times, taking into account multiple factors such as driving distance, charging rates, energy cost, and real-time availability slots at nearby stations. Experimental results show that, compared to state-of-the-art approaches, the proposed framework can reduce the communication and computation overheads by at least 20.7% and 16.5%, respectively.

In [56], a novel decentralized authentication scheme for roaming services in mobile vehicular networks based on blockchain's smart contracts is proposed. Specifically, the authors employ smart contracts to build a distributed roaming protocol to facilitate user and access point registration, authentication, and revocation. Additionally, a space-efficient probabilistic data structure, namely Bloom filter [57], is leveraged to implement storage-limited smart contracts, thereby supporting the efficient and secure revocation required for large-scale 5G mobile networks. Moreover, a billing scheme utilizing a sequence of hash values as proof of service provision is proposed to prevent operators from conducting malicious actions. A detailed security analysis shows the system's resilience to modification, replay, and MITM attacks. Experimental results show that the total authentication delay is roughly 460ms, the revocation space is approximately 200 KB for 50000 revoked entities, and the roaming system's failure probability is negligible even when the node's failure probability reaches approximately 90%. Another blockchain-based framework is proposed in [58], which utilizes a certificated-based authentication scheme for accident detection and notification in smart transportation systems. The proposed framework employs blockchain technology to allow each vehicle in the network to securely send accident-related transactions to the nearby Cluster Head, which relays the transactions to the RSUs. Subsequently, these RSUs transfer the transactions to the Edge Servers (ES), which are responsible for combining and forwarding these transactions to the Cloud Server for a complete block creation and addition to the blockchain. Moreover, a formal security assessment using the AVISPA tool [59] shows that the system is resilient against replay and MITM attacks. Experiment results show that the proposed framework can reduce the computation and communication costs compared to those of state-of-the-art approaches by at least 19% and 10%, respectively.

3.3. Summary

In this section, we discuss various blockchain-based approaches to authentication in different types of vehicular networks. As summarized in Table 1, most of the surveyed frameworks aim to provide secure authentication for vehicular networks, with a strong focus on improving the authentication process' efficiency. To this end, the proposed approaches utilize blockchain for decentralized and tamper-resistant authentication. Moreover, cryptographic methods such as ECC, ECDSA, AES, and SHA-256 are leveraged for secure data handling. Furthermore, new consensus mechanisms, authentication protocols, and hierarchical blockchain architectures are proposed to reduce the authentication process' communication and computation overheads. While the discussed works demonstrate the effectiveness of blockchain technology in addressing the challenges of authentication in vehicular networks, there are still some open issues. For example, blockchain's inherent scalability issue coupled with the limited resources of vehicles and infrastructure still poses a significant challenge in managing a large volume of vehicles and transactions. However, most of the discussed works do not implement experiments on a large scale to evaluate the scalability of the proposed frameworks. This is also an issue in evaluating the robustness of the proposed approaches against the dynamic of vehicular networks where vehicles frequently leave and join the networks.

4. Applications of Blockchain-based Authentication for Internet of Things

The Internet-of-Things (IoT) refers to the interconnected networks of billions of physical devices, ranging from computers and smartphones to home appliances and sensors, enabling these objects to connect and exchange data. With its huge scale and distributed nature, providing effective authentication and access control for IoT devices remains a significant challenge. Particularly, the diverse nature and vast number of IoT devices make traditional centralized authentication systems vulnerable to single point of failure and scalability issues. Additionally, IoT environments face privacy concerns, as centralized systems often require the collection and storage of sensitive data, making them attractive targets for attacks. Moreover, the heterogeneity of IoT devices, with varying capabilities and standards, complicates the implementation of a unified authentication protocol, leading to potential security gaps and interoperability challenges [60, 15, 14]. To address these problems, blockchain has emerged as an effective solution, offering a decentralized approach that eliminates the need for a central authority, thereby reducing the risk of a single point of failure. Additionally, blockchain technology enables decentralized management of identities, facilitating privacy-preserving

Table 1: Summary of Blockchain-based Authentication Applications in Vehicular Networks

Ref.	Application areas	Objectives	Approaches
[41]	VANETs	- Enhance certificate revocation processes	- Use blockchain to store CRL - Utilize EAAP to facilitate anonymous authentication - Employ coded caching to distribute minimum required bits of CRLs
[43]		- Enable decentralized authentication	- Utilize MPT structure to store certificates - Employ ECDSA to facilitate digital signature generation and verification
[44]		- Provide decentralized authentication	- Leverage SE zk-SNARKs to generate proofs for messages - Use blockchain to store issued credientials
[45]		- Enable anonymous cross-domain authentication	- Utilize group signature scheme for single domain authentication - Use blockchain for cross-domain authentication
[47]		- Enable cross-domain authentication - Enhance certificates management and storage	- Utilize IPFS to store verifiable credentials - Use blockchain for cross-domain authentication - Employ blockchain to store verifiable credentials' IPFS addresses
[49]		- Provide mutual authentication	- Use ECC for intra-regional and inter-regional authentication
[50]		- Provide decentralized authentication - Enable effective emergency communication	- Propose Proof-of-Authentication RBC for authentication - Propose Proof-of-Position MBC for emergency communication
[51]		- Provide transparent and secured authentication	- Utilize ECC and AES for authentication - Leverage SHA-256 for enhanced security - Employ ECDSA for certificate generation - Use blockchain to store encrypted vehicle information
[54]	Vehicle-to-Grid	- Provide mutual authentication - Allow secure and anonymous transactions between vehicles and the grid	- Use Merkle Root Hash to facilitate mutual authentication - Leverage blockchain to enable anonymous transactions
[55]		- Provide lightweight authentication - Enable charging station scheduling	- Employ ECC for lightweight authentication mechanism - Develop a novel charging station scheduling algorithm - Use blockchain to store and validate transactions
[56]	Roaming service in mobile vehicular network	- Provide distributed roaming protocol - Enhance storage efficiency	- Leverage smart contract to facilitate roaming protocol - Use space-efficient Bloom filter data structure
[58]	Smart transportation	- Enable accident detection and notification	- Use blockchain to facilitate secured accident-related transactions in the network

authentication by allowing devices or trusted entities to verify one's identity without revealing sensitive information. This approach enhances security, maintains user privacy, and ensures better scalability, adapting efficiently to the ever-growing and evolving landscape of IoT devices [60, 10].

4.1. Industrial Internet of Things

With the emergence of IoT in various consumer and business sectors, there has been an increasing demand to apply the connectivity and data-driven insights of this technology to industrial applications such as manufacturing and logistics. This leads to the development of Industrial Internet-of-Things (IIoT), which aims to revolutionize these sectors through enhanced efficiency, predictive maintenance, and real-time operational decision-making [61]. However, establishing a reliable and secure authentication framework for IIoT is challenging due to scalability needs in managing a vast array of devices, the diversity of device capabilities, network security vulnerabilities, and physical security risks [61]. Blockchain technology, with its decentralized, scalable, and tamper-proof nature, offers a promising solution to these problems. For example, a secure authentication and privacy-preserving blockchain framework for IIoT is proposed in [62], which employs cryptography for secure user authentication and machine learning for optimal blockchain node selection. As illustrated in Fig. 5, a Transient key congruential generator-based ECC mechanism is developed to enable efficient user information encryption. Additionally, blockchain nodes leverage ZKP to verify users before allowing access to the blockchain network. After granting network access, the Approximation Fully Homomorphic Encryption Neural Network (AFHENN) is developed to recognize known malicious behavior patterns of miner nodes via direct training on encrypted data. Experiment results show that the proposed framework achieves a packet delivery ratio of 88.98% with an execution time of 7.509 milliseconds and a latency of 43.38 seconds. Another framework that utilized ZKP is proposed in [63], namely BP-AKAA, where blockchain plays a key role in enabling cross-domain authentication and key agreement for IIoT device-to-device (D2D) communications. Particularly, the framework utilizes non-interactive ZKP to protect device identity privacy and leverages permissioned blockchain's distribution and tamper-resistance to solve inter-domain trust issues. Specifically, BP-AKAA utilizes two discrete-logarithm-based NIZKP protocols for identity key generation and privacy-preserving authentication. It also incorporates an attribute-based encryption scheme to realize fine-grained access control. The proposed BP-AKAA scheme supports multiple critical functions, including cross-domain, privacy-preserving, mutual authentication, attribute-based threshold access control, and session key agreement, which are necessary for secure IIoT

D2D data sharing. Security analysis proves that it can resist various attacks such as MITM, RS corruption, and user-server attacks. Moreover, simulation results show that the proposed framework can significantly reduce computation, communication, and storage overheads compared to state-of-the-art approaches.

Apart from ZKP, Machine Learning (ML) techniques have also been leveraged to develop blockchain-based authentication frameworks. Particularly, in [64], the authors develop a novel authentication scheme based on Transfer Learning (TL) and blockchain technology for IIoT applications. Specifically, the proposed scheme employs a region-based dual blockchain architecture. It features an inner blockchain for authenticating local users within each region and an outer blockchain for cross-region authentication. Additionally, to enhance authentication accuracy, region-specific user credits are introduced. Each user is allocated two types of credits, i.e., local and cross-region, based on their historical behavioral records. These credits are then integrated into the Guiding Deep Deterministic Policy Gradient (G-DDPG), a high-accuracy deep reinforcement learning algorithm, to train the local authentication model. Furthermore, to reduce the training time, authentication models can be transferred locally or cross-regionally via TL. Experiment results show that the system throughput can reach up to 133 TPS, and the maximum latency is no more than 8s. Similarly, in [65], the authors present two innovative blockchain-based authentication schemes designed for IIoT devices, integrating Machine Learning (ML) and Physical Unclonable Functions (PUFs)[66] as key components. PUFs, in this context, leverage manufacturing variations in hardware to derive unique digital signatures for each device. The first scheme leverages Static Random Access Memory (SRAM) PUFs, known for their lightweight nature and compatibility with various devices, enabling decentralized authentication for IIoT devices. In this approach, each device locally stores its SRAM PUF Challenge-Response Pairs (CRPs), while network nodes hold a subset of CRP addresses. Through nodes verifying hashed responses, device authentication is achieved without the need for centralized storage of CRPs. The second scheme employs Arbiter PUFs in conjunction with ML techniques to construct authentication models. A certificate authority collects CRPs from devices to train machine learning models, which are then distributed to nodes. Devices generate challenges from the blockchain, and nodes produce predicted responses. Successful authentication occurs if the Hamming distance between device and node responses falls below a predefined threshold. The authors formally prove the security of these schemes against cloned device attacks, and experimental results demonstrate an accuracy of over 99.9% in predicting 64-bit Arbiter PUF responses for authentication.

4.2. Wireless Sensor Networks

Wireless Sensor Network (WSN) has emerged to address the need for real-time data collection and monitoring in diverse and often inaccessible environments. They are networks of distributed and autonomous sensor devices that wirelessly communicate to collect and transmit their data to a central location for analysis and monitoring. Although by leveraging wireless communication technology WSN can effectively collect and monitor data from distributed and remote areas, this approach also poses significant challenges such as limited resources of sensor nodes, data security and privacy concerns, signal interference, and the need for robust and scalable authentication framework to handle large amount of nodes efficiently [67]. To address these challenges, blockchain technology can be leveraged to build authentication frameworks for WSN, offering enhanced security and privacy. For example, in [68] the authors propose a hybrid blockchain-based identity authentication scheme for WSNs. In this scheme, nodes in the WSN are divided based on their capability into base stations, cluster heads, and ordinary nodes to form a hierarchical network, as illustrated in Fig. 6. A hybrid blockchain model comprised of local blockchains and a public blockchain is developed to facilitate authentication. For intra-cluster communication, a local blockchain is employed to record nodes' identity data after they are verified by the cluster head. For inter-cluster and inter-WSN communication, a public blockchain is employed. Additionally, ECDSA is utilized to facilitate digital signature generation and verification. Security analysis demonstrates the system's resilience against multiple attacks such as Sybil, spoofing, message substitution, replay, MITM, and denial of service. However, the performance of the system is not evaluated.

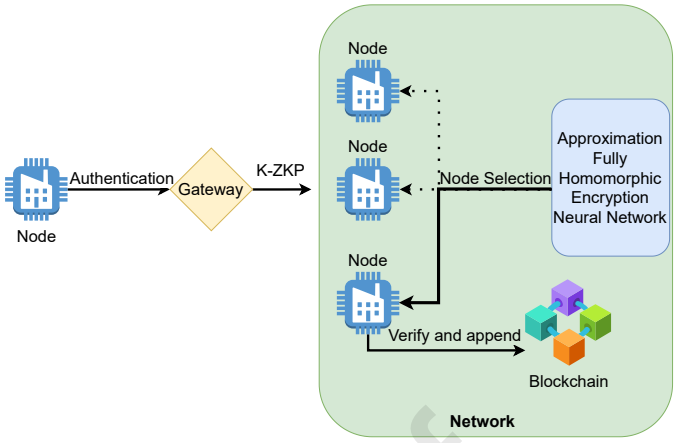

Figure 5: Blockchain-enabled authentication scheme for IIoT [62].

In [69] the authors introduce a decentralized authentication protocol leveraging blockchain technology to validate sensor nodes without a trusted third party. Particularly, the proposed protocol stores sensor data in IPFS instead of centralized cloud servers. Additionally, a blockchain-enabled public data auditing mechanism is proposed to eliminate the dependence on third-party auditors. Moreover, smart contracts facilitate automatic verification and accountability tracing sensor nodes' activities, ensuring data integrity. Experimental results show that the proposed protocol can reduce communication and computation overheads by roughly 12.5% and 15.8%, respectively, compared to those of baseline approaches. Another framework that utilizes IPFS is introduced in [70], which is a blockchain-based mutual authentication and session key agreement proto-

col for large-scale WSNs with multiple base stations. The protocol, namely BSAPM, utilizes smart contracts to register sensor nodes and users and stores records on private blockchain networks. It employs the IPFS protocol to distribute sensor data storage. Moreover, BSAPM allows a user registered at one base station to efficiently access data from any node registered at other stations. Security analyses using Scyther tool [71] and Real-or-Random model demonstrate that BSAPM can resist various attacks including impersonation, MITM, replay, and insider attacks. Compared to state-of-the-art approaches, BSAPM can reduce computation and communication costs by up to 3.5 and 2 times, respectively.

In contrast to traditional blockchain structure, in [72] the authors propose a blockchain-empowered authentication scheme that utilizes the DAG structure [23] to address security challenges in WSN. Specifically, WSNs are vulnerable to attacks where nodes can be physically interfered with and compromised. To address this, the proposed framework, namely BAS, leverages blockchain technology to securely store and manage node identity information, facilitating trusted device authentication. Specifically, BAS introduces a Trust Relationship Graph (TR-Graph) data structure to represent relationships between valid sensor nodes. Sink nodes manage local TR-Graphs and validate nodes in their network domain. Meanwhile, a DAG-based blockchain connects all sink nodes, enabling consensus-based sharing and maintenance of global identity data. Additionally, the framework aims to prevent worm attacks [73] through robust access control and rapid detection-triggered isolation of infections. Experiment results show that the proposed protocol effectively contains outbreaks, limiting infections to only 20% of nodes, as opposed to 80% in other WSNs.

4.3. Smart Home Networks

Smart home networks have become increasingly significant in modernizing residential environments by utilizing IoT technology for interconnected home automation systems. These networks typically consist of various smart devices including thermostats, lighting, security systems, and appliances, all communicating wirelessly to create an automated and user-responsive environment. While this technological integration offers enhanced convenience, energy efficiency, and security, it also introduces challenges such as the need for secure and seamless connectivity and authentication among diverse devices, protection of personal data privacy, and vulnerability to cyber-attacks [74]. To address these issues, a novel blockchain-based framework is presented in [75], where the authors develop a novel blockchain-based mutual authentication system for smart homes to provide traceability and privacy protection of access control policy. Particularly, the proposed framework utilizes Practical Byzantine Fault Tolerance (PBFT) [76] as the consensus algorithm for the blockchain network. Additionally, smart contracts are used to record authentication requests from users and manage a revocation list. This revocation list is then used in a lightweight group signature scheme [77] to anonymously authenticate group members. Moreover, all the transactions in the system are encrypted using an elliptic curve integrated encryption scheme [78]. Experiment results show that

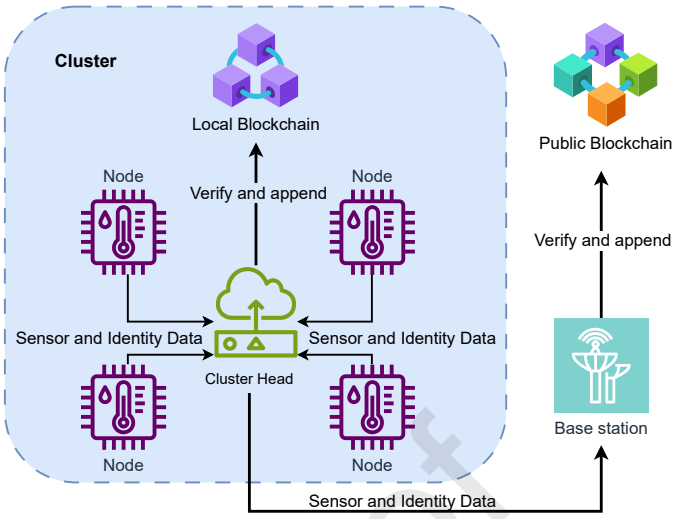

Figure 6: Hybrid blockchain-based authentication framework for WSNs [68].

the proposed approach can significantly reduce the computation and communication costs compared to those of a baseline method. Another framework that employs smart contracts is presented in [79], where the authors propose a decentralized authentication scheme for smart homes based on private blockchain technology and fog computing, aiming to address security threats such as impersonation attacks and the reliance on trusted third parties. To this end, the proposed framework utilizes a private blockchain's tamper-proof and decentralized structure to improve security, whereas fog nodes are leveraged to provide localized computing services for efficiency and scalability. Particularly, the framework involves registering fog nodes and devices on the blockchain, with devices assigned to fog nodes. Users can then trigger smart contracts to obtain access credentials on-chain and authenticate with fog nodes off-chain via exchanged signed messages. Security analysis shows that the proposed approach can ensure confidentiality and integrity, while being able to mitigate various attacks including MITM, replay, and DoS attacks. Experiment results show that the proposed approach can reduce the communication cost by up to 3 times and the computation cost by up to 5 times compared to most state-of-the-art approaches.

4.4. Smart Grid

Smart grids are electrical grids that utilize various devices and sensors to dynamically react to changes across the grid. However, the usage of those devices and sensors also brings forth cybersecurity risks regarding the authentication of connected devices and users [80]. To address those authentication risks, a blockchain-based authentication scheme is proposed in [81]. The proposed scheme employs technologies such as ECC, PUFs, and hash functions to enable mutual authentication between smart meters and service providers. Particularly, the scheme stores all smart grid data securely in a private blockchain, with service providers responsible for verifying and adding new blocks through the PBFT consensus algorithm. Moreover, an experimental testbed is developed to evaluate the

proposed scheme. Detailed security analysis shows the scheme is resilient against various attacks such as replay, MITM, impersonation, and physical capture attacks. Formal verification using the Scyther tool [71] confirms security against replay and MITM attacks. Performance evaluation shows that the scheme has significantly lower computational and communication overheads compared to related schemes, while providing additional security features and functionality. Similarly, in [82], the authors propose an authentication protocol for securing communication in a heterogeneous blockchain-based smart grid environment. Particularly, AP-HBSG allows entities with certificateless public key cryptography (CL-PKC) and public key infrastructure (PKI) to mutually authenticate and establish session keys. It eliminates single point of failure via a decentralized blockchain architecture, where nodes reach the consensus to access smart meter data. Additionally, a blind signature technique enables nodes to verify the source of messages. Moreover, AP-HBSG implements ECC to align with smart meters' limited computing capability. Security analysis shows that the proposed protocol can mitigate modification attacks and achieves perfect forward secrecy. Experiment results show that compared to related schemes, AP-HBSG reduces authentication computation cost by up to 76.5% and communication overhead by up to 67.9%.

4.5. Heterogeneous IoT

Heterogeneous IoT represents a complex and multifaceted ecosystem within the broader Internet-of-Things landscape, characterized by a diverse array of devices, sensors, and systems with varying capabilities and specifications. This ecosystem includes a wide range of technologies, from simple temperature sensors to advanced computing devices, all interconnected through various communication protocols and networks. A critical challenge in this heterogeneous environment is ensuring effective and secure authentication of each device within the network. The heterogeneity of devices leads to varied security requirements and vulnerabilities, making standardized authentication protocols challenging to implement. Additionally, the sheer volume of devices necessitates a scalable authentication solution that can accommodate rapid expansions and modifications in the network [83]. To address these challenges, multiple blockchain-enabled frameworks have been proposed. For example, in [84], a hybrid centralized and decentralized authentication architecture for heterogeneous IoT systems is proposed. As illustrated in Fig. 7, to address the scalability issues, the authors implement a dual-layered authentication structure, combining an edge-based scheme, where edge servers store encrypted device information, with a blockchain network that validates communications across multiple edge networks. To improve network efficiency and responsiveness, lightweight symmetric and asymmetric encryption techniques are utilized with the SPECK algorithm [85] and ECC, respectively. Experiment results show that the proposed framework outperforms the centralized and decentralized approaches in terms of average processing times by 19.6% and 20.5%, respectively. Moreover, the proposed framework's throughput is 27.6% and 27.4% higher,

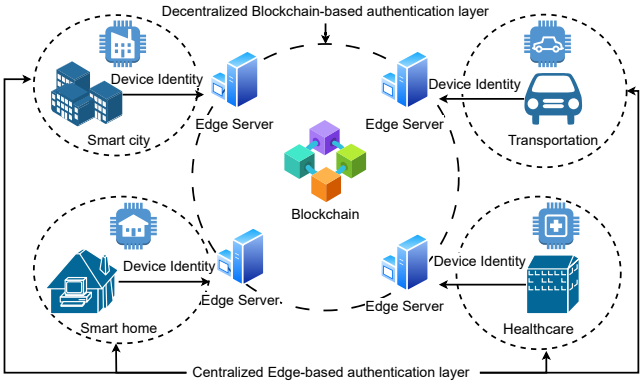

Figure 7: Blockchain-based authentication framework for heterogeneous IoT framework [84].

while consuming 22% and 28% less energy compared to those of the centralized and decentralized approaches, respectively.

Similarly, in [60] the authors develop a blockchain-based authentication scheme to address the security vulnerabilities of complicated heterogeneity IoT systems. The proposed scheme combines blockchain technology and Modular Square Root technique [86] is proposed. In the proposed scheme, the Modular Square Root technique [86] is utilized to ensure the security and efficiency of the authentication process, whereas blockchain technology is used to enhance the security and scalability of the system. Simulation results show that the proposed framework has a computation time of 1.766 ms and a computation cost of 1888 bits, significantly lower than those of state-of-the-art approaches.

4.6. Other IoT Networks

In [87], the authors develop a novel smart contract-based authenticated key agreement scheme for IoT-based agriculture applications. The proposed framework aims to support both D2D and device-to-gateway (D2G) mutual authentication in a hybrid blockchain network. In particular, all communication information such as trading transactions, chemicals, and fertilizers quality are encapsulated in blocks of encrypted and unencrypted data. Using smart contracts, these blocks are then added to the blockchain which utilizes the PBFT consensus algorithm [88]. Additionally, a detailed security analysis is conducted using the AVISPA [59] tool. Simulation results show that the proposed framework can achieve lower communication overhead compared to baseline approaches.

In [89], the authors propose a hybrid blockchain-based identity authentication scheme for Mobile Crowd Sensing (MCS). The framework, namely HBIA, utilizes a hybrid blockchain model combining public and private chains to establish a balance between the transparency needs of blockchains and the privacy requirements of MCS participants. Particularly, the authentication process employs a hierarchical approach using smart contracts: cluster head nodes undergo authentication on the public chain, while participating nodes within each cluster are authenticated on the private chains. To improve efficiency, the ZKP algorithm is employed to enable privacy-preserving

off-chain computations of authentication-related tasks. Additionally, the framework employs Zero-Knowledge Succinct Non-interactive Arguments of Knowledge (ZK-SNARK) [90], which generates cryptographic proofs for computations conducted off-chain and send them back to the private chains, thereby enabling smart contract-based on-chain verification. Simulation results show that the proposed approach achieves a 33% faster verification time compared to that of other approaches.

4.7. Summary

In this section, we discuss blockchain-based authentication frameworks for different types of IoT networks. As summarized in Table 2, most of the surveyed frameworks aim to enhance the security, privacy, and scalability of the authentication processes. To this end, the proposed approaches utilize blockchain's iherent characteristics to enhance the security and transparency of the authentication processes. Moreover, mechanisms such as ZKP, smart contracts, and ML are leveraged to improve privacy and automate various processes. While the proposed frameworks can significantly improve the authentication process in IoT environments, as shown by the simulation and experiment results, there are still some challenges that need to be addressed. First, blockchain technology is still facing serious scalability issues, which might be exacerbated by the vast number of IoT devices. Moreover, interoperability might become an issue for authentication as different IoT networks (based on different blockchain networks) need to communicate with each other. In addition, IoT devices often have limited computational capacity, which is not suitable for compute-intensive blockchain consensus mechanisms such as PoW.

5. Applications of Blockchain-based Authentication for Healthcare Systems

In recent years, the healthcare sector has been evolving rapidly, integrating technology to improve patient care and operational efficiency. These technological advancements have transformed several key areas in healthcare. First, patient identification has become more streamlined and accurate, using technologies including biometrics and smart ID cards. Second, healthcare information management and administration have been revolutionized with Electronic Health Records (EHR) and advanced data sharing and analysis. Third, the provision of healthcare services has seen significant changes with the adoption of telehealth, remote monitoring, and personalized medicine based on genetic information. However, with the adoption of these technologies comes heightened concerns. For example, ensuring the integrity and privacy of patient data has become a significant challenge, as digital systems are more susceptible to cyberattacks and unauthorized access. Additionally, establishing a reliable authentication framework for both patients and healthcare personnel is crucial to maintaining the trust and security of the healthcare system [17, 91, 92]. Blockchain technology, with its inherent decentralized nature, cryptographic mechanisms, and immutable ledgers, offers promising solutions to avoid single point of failure, prevent tampering and unauthorized access, and facilitate efficient medical record sharing in healthcare data management systems.

5.1. Patient Identification and Authentication

Patient identification and authentication have become critical in the modern healthcare sector, aiming to ensure accuracy and security across various healthcare systems. These systems are developed to accurately identify patients and authenticate their information, using technologies including biometrics, smart ID cards, and EHR. While these technologies facilitate efficient and precise patient identification and authentication, they also present significant challenges such as maintaining the confidentiality and integrity of patient data, protecting against unauthorized access, and creating a scalable and reliable framework for handling large volumes of patient information [17, 91]. To overcome these challenges, in [93] the authors introduce a novel blockchain-based privacy-preserving biometric authentication framework for healthcare applications. It enables anonymous yet auditable patient authentication by storing encrypted biometric templates in a Merkle tree off-chain, with only a commitment to the Merkle root published on-chain. Moreover, two specialized protocols are proposed for biometric matching without expensive bilinear pairings. Particularly, using additive ElGamal encryption [94] and ZKP, one protocol is developed for set difference metrics on unordered feature sets, e.g., fingerprint, and the other is proposed for Euclidean distance metrics on ordered feature vectors such as face biometrics. By transforming the features into random elements in ZKP, brute force attacks can be prevented. In the formal security analysis, the proposed protocol is proven to resist password guessing, key compromise impersonation, and replay attacks. Simulation results show that the proposed approach can significantly reduce the computation costs for users and servers compared to a baseline method.

Another framework that utilizes biometric data is introduced in [95], where a novel patient authentication framework between an access point device and a database node using finger vein (FV). Particularly, the framework consists of two stages. First, a hybrid biometric pattern model is proposed, combining radio frequency identification and finger vein features for increased randomization and security. Then, a combination of encryption, blockchain, and steganography techniques is implemented to secure the hybrid pattern model during transmission. Blockchain technology is then leveraged to transmit this encrypted hybrid pattern, using hashing and chaining of data blocks for integrity and availability. Steganography based on a particle swarm optimization method is also proposed to conceal the encrypted pattern in images for added confidentiality. Security analysis shows that the framework is highly secure against spoofing and brute force attacks. Performance evaluation on 106 samples shows that the proposed approach can achieve 97.9% accuracy.

Instead of relying solely on patient biometrics data, in [96] the authors propose a multi-factor authentication management protocol for Internet-of-Medical-Things applications us-

Table 2: Summary of Blockchain-based Authentication Applications in IoT Networks

Ref.	Application areas	Objectives	Approaches
[62]	Industrial IoT	- Enable efficient user information encryption - Provide secure authentication - Allow optimal blockchain node selection	- Use Transient key congruential generator-based ECC for information encryption - Leverage ZKP for authentication - Develop AFHENN for node selection
[63]		- Enable cross-domain authentication - Facilitate secured data sharing	- Leverage permissioned blockchain and NIZKP protocols for authentication - Incorporate attribute-based encryption scheme for access control in data sharing
[64]		- Enable cross-domain authentication - Enhance authentication accuracy	- Employ dual blockchains to facilitate intra-regional and inter-regional authentication - Use G-DDPG to improve authentication accuracy - Leverage transfer learning to reduce training time
[65]		- Generate unique digital signatures - Facilitate authentication	- Employ PUFs and manufacturing variation to generate unique digital signatures - Combine blockchain and machine learning for authentication
[68]	Wireless Sensor Networks	- Provide intra-cluster and inter-cluster authentication - Facilitate digital signature management	- Leverage hierarchical blockchain architecture for intra-cluster and inter-cluster authentication - Employ ECDSA to facilitate digital signature generation and verification
[69]		- Enable decentralized sensor data storage - Provide data auditing mechanism - Facilitate authentication	- Utilize IPFS for distributed sensor storage - Propose blockchain-based data auditing mechanism - Employ smart contracts for authentication and data verification
[70]		- Provide distributed sensor data storage - Facilitate mutual authentication	- Employ IPFS for distributed sensor storage - Leverage private blockchain for mutual authentication
[72]		- Enable secured authentication - Prevent worm attacks	- Leverage DAG and TR-Graph data structure to facilitate authentication - Utilize robust access control and rapid detection-triggered isolation of infections
[75]	Smart Home Networks	- Facilitate mutual authentication - Provide traceability and privacy protection access control	- Employ group signature scheme for anonymous authentication - Leverage PBFT-based blockchain's smart contract to record authentication requests - Utilize elliptic curve integrated encryption scheme to enable data privacy protection
[79]		- Enable decentralized authentication	- Employ blockchain's smart contract to facilitate authentication
[81]	Smart Grid	- Provide mutual authentication between smart meters and service providers	- Utilize PBFT-based blockchain to facilitate mutual authentication
[82]		- Facilitate mutual authentication in smart grid environment - Enhance efficiency for smart meters with limited computing capacity	- Leverage CL-PKC and PKI for mutual authentication - Utilize ECC for efficient encryption
[84]	Heterogeneous IoT	- Enable scalable authentication - Improve network efficiency and responsiveness	- Develop a dual-layered authentication structure with edge servers and blockchain network - Employ lightweight SPECK algorithm and ECC to enhance efficiency and responsiveness
[60]		- Provide secured, scalable and efficient authentication	- Utilize blockchain and Modular Square Root to facilitate authentication
[87]	Agriculture IoT Network	- Enable authenticated mutual key agreement scheme	- Employ PBFT-based blockchain's smart contract for authentication
[89]	Mobile Crowd Sensing	- Allow privacy preserving and transparent authentication for MCS participants	- Utilize dual blockchain for intra-cluster and inter-cluster authentication - Employ ZK-SNARK to generate proofs for off-chain computation

ing blockchain technology. As illustrated in Fig. 8, the protocol adopts a three-factor authentication method, comprising password, biometrics, and smart card factors, to ensure secure user login. It introduces a blockchain to decentralize identity storage and message verification. The protocol also leverages Chebyshev chaotic maps [97] to protect the authentication process and negotiation of session keys. Additionally, the framework employs a TA to register nodes in the network, as well as to verify and append identity information to the blockchain. Moreover, a gateway node is utilized to handle authentication between entities and facilitate data forwarding and management. Through formal security analysis, the protocol is proven to achieve user anonymity and resistance against various attacks such as impersonation, MITM, and session key disclosure. Performance evaluation shows that compared to baseline approaches, the protocol can reduce computation, communication, and storage overheads by up to 28.5%, 48.4%, and 46.4%, respectively.

In [98] the authors propose a blockchain-based framework for patient referrals in healthcare networks. Specifically, the proposed scheme enables a Primary Health Center to mutually authenticate a patient to a referred hospital without requiring the patient to register with multiple providers. More-

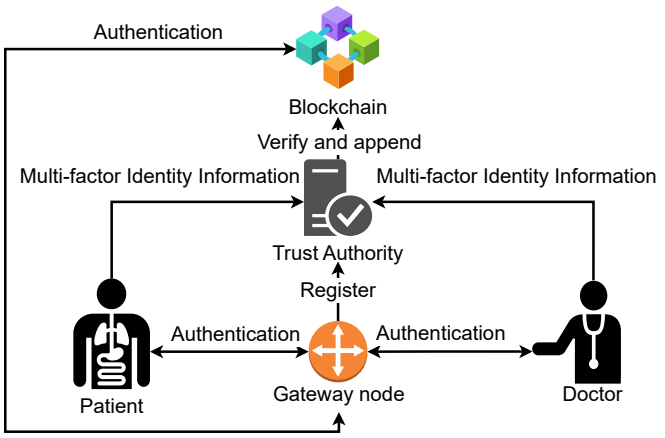

Figure 8: Blockchain-based authentication framework healthcare patient identification system [96].

over, ECC is utilized to achieve quick credential verification, patient anonymity, secure secret key management, and session key agreement with perfect forward secrecy. Security analysis shows that the proposed framework meets all specified requirements including mutual authentication, patient anonymity, secure secret key management, and prevention of insider and replay attacks. Moreover, performance analysis shows that the proposed framework has lower computation costs than most other multi-party authentication schemes, with an estimated authentication execution time of 0.58 milliseconds. Another framework that employs ECC is presented in [99], where the authors utilize blockchain technology to develop a scalable and lightweight group authentication framework for a fog-based Internet of Medical Things (IoMT) system, aiming at providing remote monitoring service for patients. Particularly, this framework employs a global blockchain for node identification and registration, complemented by multiple local blockchains dedicated to authenticating devices within their respective fog areas. Additionally, to reduce communication and computation overhead, ECC and Shamir's secret sharing algorithm [100] are integrated. Security analysis using the AVISPA tool [59] confirms the framework's resilience against various authentication-related attacks. Simulation results show that the framework can process on average 400 transactions per second with 0.5 second latency.

Besides remote monitoring of patients, blockchain technology can also be leveraged for authentication in telehealth services. For example, in [101] the authors propose a blockchain-based distributed architecture and mutual authentication scheme, namely BIoMTAKE, for telehealth services provision. The proposed architecture utilizes Hyperledger Fabric to establish a decentralized blockchain network across hospitals and employs fog servers as blockchain peers. This eliminates dependency on a single trusted authority by distributing access control and data storage. Additionally, BIoMTAKE also enables mutual authentication between IoMT devices and data collector nodes using lightweight cryptographic techniques including ECC and hashing algorithms. Moreover, it establishes a common secret session key for secure communication. The scheme aims to prevent security attacks such as impersonation, MITM attacks, and replay attacks by dynamically generating authentication parameters and validating message freshness. Formal security analysis proves that BIoMTAKE can prevent session key compromise. Performance evaluation shows that compared to baseline approaches, BIoMTAKE can reduce the computational and communication overheads by at least 14.8% and 43.5%, respectively.

The authors in [102] take a different approach by utilizing bioacoustics finger signal to propose a novel framework that employs blockchain technology to build a decentralized authentication system for user authentication in telemedicine information systems. Particularly, a light-weighted cryptography algorithm is developed to extract and secure unique finger features. The bioacoustics finger signal is then acquired and pre-processed to extract distinguishable features such as velocity, and acceleration. Next, the algorithm generates cryptographic keys to encrypt these features and uses an asymmetric verification process for resolving user identities. It also employs a caching technique to improve authentication speed. Experiment results show that the proposed algorithm can significantly reduce the decryption speed compared to that of other approaches.

5.2. Healthcare Information Management

Healthcare information management has evolved to meet the complex demands of modern healthcare delivery, focusing on the efficient and accurate handling of vast amounts of health-related data. This field encompasses the collection, storage, retrieval, and use of healthcare information, facilitated by technologies such as EHR, data analytics, and cloud computing. While these advancements have significantly improved the management and accessibility of health data, they also introduce challenges such as ensuring data security and privacy, protecting against unauthorized access, and maintaining data integrity across multiple platforms and systems [17, 91, 92]. To address these issues, the authors in [103] utilize blockchain technology to develop a secure EHR management system, integrating data sanitization and polynomial interpolation techniques for encryption. In particular, the framework employs a blockchain structure to securely share patient health data with high verifiability. Two key mechanisms are then proposed for privacy preservation. First, an algorithm based on Penguins Search Optimization Algorithm [104] is developed to generate optimal keys for data sanitization. Second, polynomial interpolation with a Merkle tree blockchain is implemented for additional cryptographic security. Experiment results show that the proposed framework can reduce authentication time by 57.25% and memory usage by 42.85% compared to existing techniques.

In [105], the authors propose a blockchain architecture to enable patient tokenization for secure and decentralized health information exchange. It employs non-fungible tokens (NFTs) as unique patient identifiers, linking records across healthcare sites while preserving privacy. Moreover, self-sovereign identity mechanisms allow patients to control NFT access permissions. The system has four key components: NFT creation and biometric linkage; connecting patient IDs to NFTs across sites;

patient authentication for NFT access control; and HIE processes utilizing NFT verification. Additionally, it implements encryption, hashing, and ZKP to enhance the system's security. Experiments with 3 million transactions demonstrate the framework's feasibility, with average validation times of 1.17s.

5.3. Summary

In this section, we discuss the key role of blockchain in the authentication processes of various types of networks in the healthcare sector. As summarized in Table 3, for patient identification and authentication, blockchain offers a solution to enhance security and privacy in biometric authentication by storing sensitive biometric data off-chain and linking them with on-chain hash pointers. For healthcare information management, blockchain is employed to improve EHR management system's security, whereas blockchain tokens can be utilized for health information exchange. In healthcare service provision, blockchain is leveraged to achieve mutual authentication, patient anonymity, and secure data management. Although the effectiveness of the proposed frameworks is clearly demonstrated, there are still several challenges. First, blockchain's limited interoperability might become a serious issue in the healthcare sector, as different hospitals might employ blockchain networks with different architectures and protocols. Consequently, the exchange of information, e.g., patient data, might be difficult and inefficient. Moreover, blockchain's inherent transparency might expose patients' sensitive data, causing serious privacy concerns. Although off-chain storage can partially circumvent this issue, these storage sites might become targets for attacks, which necessitate additional defense mechanisms.

6. Applications of Blockchain-based Authentication for Distributed Computing Systems

Distributed computing, where computing tasks are divided across multiple nodes rather than confined to a single system, significantly enhances computational efficiency and enables complex scalable problem-solving. This decentralized approach, while facilitating greater flexibility and resilience, inherently introduces issues such as ensuring security and maintaining consistent system-wide protocols. Additionally, there is also the challenge of reliable and privacy-preserving authentication, since such a dispersed and dynamic environment is vulnerable to unauthorized access and cyberattacks [106, 107]. Blockchain technology can address these challenges by leveraging its decentralized ledger, providing a secure and transparent mechanism for maintaining data consistency, enhancing network security, and ensuring reliable authentication.

6.1. Cloud Computing

Cloud computing has dramatically transformed digital resource management by leveraging remote, internet-based data centers to offer scalable and on-demand computing services. However, the shift to cloud computing also introduces challenges such as ensuring optimal network latency for good user experience in off-premise setups and maintaining robust system security in a multi-tenant environment. In particular, the problem of managing digital identities and access controls in large-scale systems requires a reliable authentication framework [108]. Many frameworks have employed blockchain technology as a solution to these challenges. For example, in [109] the authors introduce a novel protocol that integrates blockchain technology with advanced cryptographic mechanisms to enhance user authentication in cloud services. Particularly, traditional anonymous authentication solutions often compromise either user privacy or incur significant overhead. The proposed protocol is designed to overcome these limitations by utilizing blockchain technology. It employs bilinear pairing, partial authentication factors, dynamic credits, and fake public keys to facilitate anonymous mutual authentication between users and cloud service providers. Additionally, it integrates ring signatures with blockchain to ensure two-level accountability, while preserving user privacy. Simulation results show that the proposed protocol achieves lower communication and computation costs compared to several baseline approaches. Similarly, in [110], the authors present a novel framework to manage access control and protect sensitive data in cloud computing environments. The central idea revolves around overcoming the vulnerabilities of centralized access control mechanisms, which are susceptible to tampering and data leaks by attackers or internal cloud managers. Particularly, the proposed framework utilizes account addresses of blockchain nodes as the identity. Moreover, access control, authorization, and authorization revocation processes are carefully designed to ensure that permissions are encrypted and securely stored on the blockchain. Simulation results show that the proposed approach can significantly reduce access control latency compared to traditional access control approaches.

Different from [110] and [109], the authors in [111] and [112] focus on mobile cloud computing environments. Particularly, a novel framework to enhance the security and trustworthiness of mobile cloud computing resources is proposed in [111]. The framework is specifically designed to address the limitations of mobile devices, such as limited computing power and storage capacity, by leveraging mobile resource management without a cloud server. To this end, the framework employs blockchain technology to establish trust in the resource information of participating mobile devices. Particularly, the blockchain is constructed using mobile resource information, with the master node initially creating the first block. When a new client node attempts to connect, it generates a block, shares it with connected devices, and undergoes authentication. If the authentication by 51% or more connected devices is successful, the new block is appended to the blockchain. This process is repeated for each new client added to the system. Simulation results show that the proposed framework can mitigate MITM attacks. However, there is no performance comparison with related approaches. In [112], the authors propose a blockchain-based unified authentication and hierarchical access control scheme for the mobile cloud computing environment to address privacy concerns related to users' access permissions and identities. Particularly, it employs the Pedersen commit-

Table 3: Summary of Blockchain-based Authentication Applications in Healthcare

Ref.	Application areas	Objectives	Approaches
[93]	Patient identification and authentication	- Enable auditable biometric authentication	- Utilize ElGamal encryption and ZKP for biometric matching - Employ blockchain for storing a commitment of Merkle root
[95]		- Provide biometric patient authentication	- Propose a hybrid biometric pattern comprised of radio frequency and finger vein features - Utilize blockchain for biometric pattern transmission and storage - Propose steganography based on particle swarm optimization for pattern concealment
[96]		- Facilitate multi-factor authentication	- Employ blockchain for identity storage and message verification - Leverage Chebyshev chaotic maps for authentication process protection and session keys negotiation
[98]		- Provide authentication for patient referrals	- Leverage ECC for quick and secure authentication
[99]		- Facilitate group authentication for fog-based IoMT system - Enhance system efficiency	- Use blockchain for node identification and registration - Employ ECC and Shamir to reduce communication and computation overhead
[101]		- Allow decentralized mutual authentication	- Utilize ECC and hashing algorithms for authentication - Leverage blockchain to build a decentralized network across multiple hospitals
[102]		- Facilitate decentralized authentication	- Develop a lightweight cryptography algorithm to extract and secure unique finger features - Employ caching technique to improve authentication speed
[103]	Healthcare information	- Develop secure EHR management system	- Use blockchain for patient data sharing - Employ Penguins Search Optimization Algorithm for data sanitization - Implement polynomial interpolation with a Merkle tree blockchain for additional security
[105]		- Enable secured decentralized health information exchange	- Employ NFT as patient identifiers - Utilize ZKP to enhance security

ments scheme [113] to conceal specific access permissions on the public ledger, achieving privacy protection while still supporting auditability for service providers. Additionally, the proposed scheme enables single registration for accessing multiple services with different permissions using one credential stored on the blockchain. Simulation results show that the proposed scheme outperforms related approaches in terms of communication cost by up to 2.7 times and computation overhead by up to 2.3 times.

6.2. Edge Computing

In contrast to cloud computing, which relies on more centralized data processing, edge computing positions data processing closer to the data source. While this proximity effectively reduces network latency, it also brings forth challenges such as managing heterogeneity of edge devices, maintaining network security, and ensuring users privacy as well as data integrity in a complex environment of a vast amount of physical entities. Specifically, developing a reliable authentication framework for both edge devices and end-users is critical in implementing edge computing at large scale [106, 107]. Multiple blockchain frameworks have been utilized to address these issues, such as the proposed group-authentication framework for Vehicular Edge Computing (VEC) applications in [114]. Particularly, the framework employs secret sharing and a dynamic proxy mechanism for decentralized identification. Sub-authentication results are combined through a blockchain-based trust management system, facilitating collaborative authentication among vehicles. Additionally, vehicles with a high reputation (achieved through contributions to the authentication processes) can be elected as miners to create new blocks. Security analysis shows that the framework is secure against replay, MITM, tamper, and collusion attacks. Moreover, simulation results show that the proposed framework's execution time scales linearly with the increasing number of involved vehicles. However, the performance is not compared with related approaches.

Apart from secret sharing schemes, ECC has been employed to implement blockchain-empowered authentication frameworks. For example, in [106] the authors propose a distributed and trusted authentication system combining edge computing and blockchain to achieve efficient authentication and information sharing among different IoT platforms. Particularly, the system consists of three layers: the physical network layer with IoT devices, the blockchain edge layer with resolution and cache nodes providing edge authentication services, and the blockchain network layer storing authentication logs. An optimized PBFT consensus algorithm is designed for the blockchain to ensure data integrity and traceability. Moreover, a distributed authentication mechanism leveraging dynamic name resolution and ECC is introduced, which preserves identity confidentiality and communication security. Furthermore, a caching strategy based on the Belief Propagation algorithm [115] is designed to minimize content download latency by over 6% to 12% compared to traditional caching approaches. The system guarantees trusted authentication and conditional privacy while achieving efficient edge services and storage. Simulation results demonstrate the feasibility of the authentication mechanism with an average latency of 50ms and 14%

higher hit ratio performance compared to a baseline method. Similarly, in [116] the authors propose a trusted blockchain system for securing edge-based 5G networks. To enable efficient identification, authentication, and addressing of edge devices, the framework utilizes a permissioned blockchain with validator nodes, edge devices, and distributed ledgers. Particularly, Validator nodes distribute unique public-private key pairs to all edge devices during registration. When a device sends a message, it uses its private key to sign the message using the ECDSA [27]. Then, validator nodes verify the sender's identity using the corresponding public key and the ECDSA. This ensures that every message is authenticated and its integrity is maintained. Additionally, all transactions and key pairs are securely recorded on the blockchain's distributed ledgers, providing a traceable and secure communication environment. Security demonstrates the network's resilience against MITM, side-channel, and key search attacks. Performance analysis shows that for a network of 150 nodes and 500 nodes, the average authentication time is 14 milliseconds and 265 milliseconds, respectively. Another framework that utilized ECC is presented in [117], where the authors propose a blockchain-based mutual authentication scheme between IoT devices and edge servers in a collaborative edge computing environment. It integrates certificateless cryptography, ECC, and pseudonym-based cryptography to provide anonymity and confidentiality while authenticating devices and servers. Specifically, it considers both static and dynamic conditions for IoT devices, designing authentication protocols for intra-edge and inter-edge scenarios to ensure continuity of service. Additionally, a key generation scheme is presented, with the cloud's key generation center producing partial private keys for edge servers and IoT devices generating their own key pairs. In addition, a session key negotiation mechanism based on ECC is proposed. Security analysis shows that the proposed scheme can mitigate various attacks including Sybil, replay, and MITM. Moreover, performance evaluation demonstrates linear scalability in registration and authentication operations as the number of devices increases.

To improve authentication efficiency, a modified ECC without the computationally intensive bilinear pairings technique can be employed. For example, in [118] the authors introduce a blockchain-based conditional privacy-preserving authentication scheme for edge computing services to enable secure communications between mobile users and edge servers. Particularly, the proposed scheme leverages blockchain technology to store and manage user dynamic pseudonyms and public keys through smart contracts, facilitating flexible user revocation and authentication. Dynamic pseudonyms are assigned to the users in the registering phase and updated periodically to ensure user privacy on the network. Additionally, by leveraging dynamic pseudonyms, conditional traceability is achieved, allowing the authority to decrypt the user's encrypted real identity stored on the blockchain to track misbehaving users. To further enhance the efficiency of the system, a modified ECC without bilinear pairings is employed to encrypt user pseudonyms and public keys stored on the blockchain. Furthermore, multiple authentication factors, namely passwords, biometrics, and smart cards, are all used to encrypt the user's private key, which can only be decrypted with all factors presented. Security analysis shows that the proposed protocol can prevent common attacks such as password guessing, key compromise impersonation, and replay attack. Experiment results show that the proposed approach outperforms related schemes by at least 5.5% in terms of communication costs.

To enhance security, a multi-factor authentication framework is introduced in [119]. Particularly, the authors propose a blockchain-based decentralized authentication scheme for edge and IoT environments to address security and reliability issues with traditional centralized authentication approaches. The proposed scheme leverages edge devices to form blockchain network nodes. These nodes participate in an improved PBFT protocol that requires agreement from at least 10 nodes to reach the consensus. The scheme supports various authentication methods including password, certificate, biometric, and token-based. Key objectives are to avoid single point of failure, prevent attacks on central authorities, and enable collaborative authentication across decentralized nodes. Performance evaluation shows average authentication times of 2.24s, 2.31s, and 2.40s for 4, 6, and 8 peers respectively.

6.3. Distributed Machine Learning

Distributed machine learning has become increasingly prominent, enabling complex AI tasks to be processed efficiently across multiple machines or nodes. By leveraging the combined computational power of the whole network, this approach not only accelerates the learning process but also handles larger datasets more effectively than traditional centralized machine learning models. However, one of the main challenges in distributed machine learning is ensuring data consistency and model synchronization across different nodes. With the heightened risk of cyberattacks and data tampering in distributed environments, establishing a reliable authentication framework is essential for the security and integrity of the distributed machine learning process [120]. Blockchain-based authentication schemes can provide solutions for these challenges. For example, in [121] the authors introduce a secure and efficient authentication framework for distributed learning systems. The proposed framework employs certificateless cryptography to address security challenges such as impersonation and data privacy breaches in distributed environments. It ensures mutual authentication and secure session key agreement while maintaining user anonymity and untraceability. Moreover, the framework utilizes ECC to enhance computational efficiency and make it suitable for resource-constrained systems. Security analysis shows that the scheme can mitigate replay and impersonation attacks, as well as ephemeral key leakage. Experiment results show that the proposed scheme can significantly reduce the authentication execution time compared to various baseline approaches.

In [122], the authors develop a lightweight authentication scheme for a blockchain-enabled federated learning system. Particularly, the proposed framework utilizes consensus committee groups based on contributions as the consensus algorithm. These committee groups subsequently employ the ZKP protocol to authenticate the participating nodes. Furthermore,

to prevent data leakage, a local training method based on differential privacy is developed. Additionally, a novel adaptive model aggregation algorithm, which considers both model quality and node contribution, is introduced to improve the accuracy of the global model. Experiment results demonstrate the classification accuracy of the proposed approach. Nevertheless, the efficiency of the authentication process is not evaluated. Another blockchain-based federated learning framework is presented in [123], where the authors present a framework that combines blockchain technology with federated learning for the Internet-of-Health Things (IoHT) networks. This framework leverages a blockchain network for secure, transparent management of IoHT devices, ensuring data integrity and provenance. Moreover, by integrating federated learning, the framework enables collaborative model training across distributed IoHT devices without sharing sensitive health data, thus preserving patient confidentiality. Additionally, the framework incorporates advanced security protocols, such as differential privacy and homomorphic encryption, to enhance data protection during model training. While simulation results demonstrate the effectiveness of federated learning, the authentication process is not evaluated.

Another approach for secure authentication in federated learning systems is by utilizing blockchain's smart contracts. Particularly, in [124] the authors introduce a novel framework combining blockchain technology with federated learning to enhance the security and accountability in distributed learning systems. The proposed framework employs smart contracts to create a verifiable and auditable environment for federated learning processes. Specifically, the framework employs multiple entities including participants, workers, a blockchain-based committee, and users. Participants contribute local data training and receive contribution-based rewards, while workers process transactions related to model updates for verification and audit. The blockchain-based committee oversees model aggregation operations using the learning smart contract, and the recording of verification proofs in the blockchain using the verifying smart contract. Moreover, the users can publish model requests and receive the well-trained model utilizing a trading contract. Additionally, an effective committee selection scheme and a novel authenticated data structure are employed to ensure the integrity and transparency of model training across a distributed network. Simulation results show that the authentication execution time scales linearly with the increasing number of participants. Similarly, in [125] the authors present a blockchain-based framework to enhance the security, verifiability, and efficiency of federated learning systems. Particularly, the proposed framework combines bilinear mapping and blockchain technology for federated learning among UAVs from different domains. Key Generation Centers are introduced to generate public-private key pairs for each domain, and domains negotiate and deploy authentication and updating contracts on the blockchain before collaborative learning. The process involves local and global registration, local model updates, authentication, and global model updates. UAVs participate by registering, updating local models, undergoing authentication, and contributing to global model updates. The framework authenticates UAVs through blockchain transactions, authentication contracts, and collaborative model updates. Security analysis shows that the proposed framework can mitigate various attacks including DDoS, poisoning, membership inference, and reconstruction attacks. Simulation results show that the proposed approach can reduce the communication cost by up to 2.5 times compared to state-of-the-art approaches.

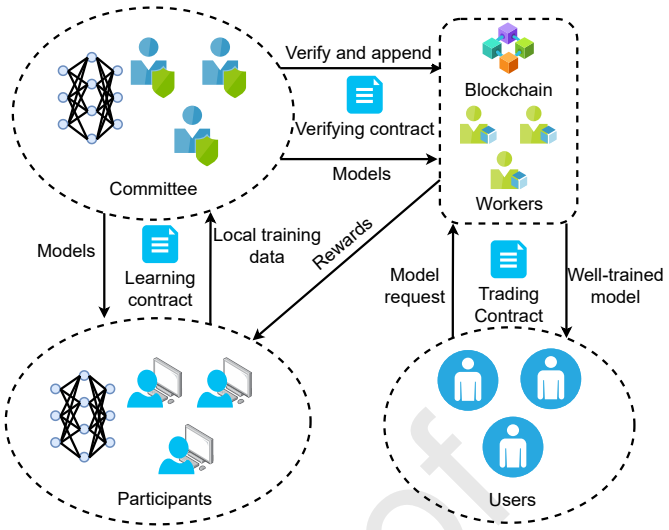

Figure 9: Blockchain-based authentication framework for distributed machine learning [124].

6.4. Summary

In this section, we discuss the key role of blockchain in the authentication processes in several distributed computing systems including cloud computing, edge computing, and distributed learning. As summarized in Table 4, blockchain is utilized in cloud computing to enhance security by managing digital identities and access controls in a transparent and secure manner. Moreover, it is utilized to improve user authentication in cloud services, introducing protocols that ensure anonymity and confidentiality. Similarly, in edge computing, blockchain technology ensures trust in resource information of participating devices, preventing data tampering. For distributed machine learning, blockchain plays a key role in ensuring data consistency, model synchronization, and accountability across multiple nodes, thereby addressing cybersecurity concerns and enhancing the reliability of the distributed learning processes. Nevertheless, similar to other areas, there are some open issues of blockchain-based authentication in distributed computing environments. First, employing blockchain as an additional layer of security further burdens the distributed computing systems, which already have high overheads and limited spare resources from the computing processes. Second, these systems often consist of many different types of devices, which aggravates blockchain's interoperability issues.

Table 4: Summary of Blockchain-based Authentication Applications in Distributed Computing Systems

Ref.	Application areas	Objectives	Approaches
[109]	Cloud computing	- Enhance user authentication in cloud services	- Employ bilinear pairing and fake public keys to facilitate anonymous mutual authentication - Integrate ring signature with blockchain to ensure two-level accountability
[110]		- Manage access control in cloud computing environments - Protect sensitive data	- Leverage blockchain account addresses as identity - Employ blockchain for secured permissions storage
[111]		- Enable decentralized authentication in mobile cloud computing	- Use blockchain to construct a decentralized authentication protocol
[112]		- Facilitate authentication and hierarchical access control in mobile cloud computing	- Leverage Pedersen commitments scheme to conceal specific access permissions - Employ blockchain for credentials torage
[114]	Edge computing	- Allow decentralized group authentication	- Employ secret sharing and dynamic proxy mechanism for identification - Use blockchain technology to build a trust management system
[106]		- Provide efficient authentication and information sharing	- Utilize PBFT-based blockchain for storing authentication logs - Leverage ECC and dynamic name resolution to develop distributed authentication mechanism - Employ Belief Propagation algorithm to minimize content download latency
[116]		- Enable authentication and identification of edge devices	- Use a permissioned blockchain for transactions and key pairs record - Utilize ECDSA for message signing and authentication
[117]		- Facilitate mutual authentication in collaborative edge computing	- Integrate certificateless cryptography and pseudonym-based cryptography for authentication - Introduce a key generation scheme to generate key pairs - Employ ECC for session key negotiation
[118]		- Allow conditional privacy-preserving authentication	- Leverage blockchain and smart contract to store and manage user dynamic pseudonyms and public keys - Employ ECC without bilinear pairing to encrypt user pseudonyms - Use multiple authentication factors to enhance security
[119]		- Provide multi-factor decentralized authentication	- Employ PBFT-based blockchain for multi-factor authentication
[121]	Distributed machine learning	- Enable secure and efficient authentication	- Leverage certificateless cryptography to address security challenges - Employ ECC to enhance computational efficiency
[122]		- Facilitate lightweight authentication for federated learning	- Utilize ZKP for nodes authentication - Employ differential privacy to develop a local training method - Propose a adaptive model aggregation algorithm
[123]		- Enhance data privacy and integrity in federated learning - Facilitate secure data management	- Leverage differential privacy and homomorphic encryption to enhance data protection - Use blockchain for secure and transparent data management
[124]		- Enhance security and accountability in federated learning	- Employ multiple smart contracts to create verifiable and auditable federated learning environment - Utilize blockchain for transactions and models storage - Propose a committee selection scheme to ensure security in the network
[125]		- Improve security and verifiability in federated learning - Facilitate decentralized authentication	- Employ bilinear mapping and introduce Key Generation Centers to generate key pairs - Utilize blockchain for authentication and transaction recording

7. Other Emerging Application Areas

7.1. Wireless Networking

Authentication challenges in wireless networks, incorporating advanced technologies such as 5G, 6G, and satellite communication, stem from the need for robust security protocols to protect against unauthorized access, ensure data integrity, and establish trust in a dynamic and heterogeneous network environment. To address those challenges, blockchain can be an effective solution. In [126], the authors propose a blockchain-based group authentication scheme for secure handovers in 6G heterogeneous networks. The system includes user equipment (UE), access points, servers, and a blockchain network. For handover scenarios, the scheme performs mutual authentication and key agreement between UE and target access points, using aggregated signatures and D-H key exchange to achieve confidentiality. Moreover, group user batch verification is enabled by blockchain consensus to reduce individual checking. The scheme realizes global, seamless handovers without added complexity, handles group handovers efficiently via aggregated signatures, and accelerates one-by-one checking using shared randomness. Security analysis via the AVISPA tool shows that the scheme can prevent replay, framing, masquerade, and MITM attacks. Performance evaluation shows that the scheme minimizes overhead versus related protocols, while significantly cutting group authentication delays by 89.8%. Similarly, in [127], the authors propose a privacy-preserving authentication protocol for 5G networks to address security and privacy challenges. To this end, the proposed scheme leverages

blockchain and pseudonyms to enable anonymous mutual authentication between a UE and a serving network (SN). Particularly, the UE computes fresh authentication parameters using random numbers and its private key to initiate the protocol. After verification, the SN assigns a temporary identity to the UE to preserve anonymity. A new session key is established using a random number chosen by the SN for every authentication, ensuring forward/backward secrecy even if a key is compromised. Then, the SN adds a block to the blockchain after each successful authentication. Security analysis proves that the protocol can mitigate various attacks including impersonation, MITM, replay, and tracking attacks. Performance evaluation shows that the proposed scheme requires fewer message exchanges and lower data transmission compared to existing protocols.

In [128], the authors propose Mobile-Chain, a novel blockchain-based mutual authentication framework for secure roaming services in global mobility networks. The decentralized architecture aims to address vulnerabilities in existing protocols and provide robust security features including authentication, anonymity, confidentiality, and untraceability. To this end, the framework leverages blockchain advantages of immutability, transparency, and elimination of single point failure to strengthen security. A key derivation protocol is then utilized to simplify roaming handovers. Moreover, smart contracts are leveraged to facilitate entity authentication and manage session keys. Security analysis demonstrates Mobile-Chain's resilience against common attacks in mobile networks. Performance evaluation shows that the proposed framework can reduce communication costs by up to 1.7 times compared to other baseline approaches. In [129], the authors propose a novel blockchain-based authentication framework for Low Earth Orbit satellites. Particularly, the proposed scheme utilizes a consortium blockchain to record registration data to maintain a decentralized certificate library of each device within the network. In this network, the MPTdata structure is employed to form a distributed certificate management which replaces the computationally intensive certificate revocation list. Additionally, a lightweight certificateless cryptography scheme is proposed to calculate the cryptographic key pairs for devices in the network. This not only reduces the computation time but also ensures the system's privacy preservation since the data are encrypted by the public key of the device before transmitting through the satellite network. Security analysis shows that the framework is resistant to data tampering, eavesdropping, and MITM attacks. Performance analysis shows that compared to other existing approaches, the proposed framework's total transmission time is up to 2 times shorter.

7.2. Identity Management

Compared to authentication, identity management is a broader concept that encompasses the entire lifecycle of digital identities, addressing processes such as provisioning, access management, and governance across multiple systems. Conventional identity management approaches, such as centralized and federated systems, provide structured frameworks for managing users' credentials but face significant challenges. Centralized systems, such as the Lightweight Directory Access Protocol (LDAP) [130], offer centralized control but create a single point of failure, making them susceptible to data breaches and service disruption. Federated systems including SAML enable cross-domain authentication through trusted partnerships, but they may encounter issues such as trust delegation and dependence on intermediaries for consensus [131]. Additionally, these approaches might compromise user privacy and autonomy due to the centralized control of identity data. In [132], the authors propose a blockchain-enabled decentralized cross-domain identity management system, namely BIdM, to address the security and scalability issues of traditional centralized systems. The proposed framework introduces a consortium blockchain to avoid single point of failure and uses decentralized identifiers for naming and managing identities. To enable efficient identity validation, the framework leverages a one-way accumulator data structure that reduces the time complexity. Identities are accumulated in the blockchain while credentials are stored off-chain. Consensus among domains enables cross-domain authentication without needing the original identity provider. Simulation results show that the proposed system can reduce the latency by up to 6 times compared to that of a baseline approach. Similarly, in [133], the authors propose a novel blockchain-based biometric authentication framework. The framework utilizes a permissioned blockchain to record authentication activities and employs a decentralized mechanism for managing and validating biometric data. Specifically, it splits biometric data into fragments that are distributed across different clients in the network. This distributed storage mechanism enhances security against data leakage while eliminating single point of failure. Additionally, a smart contract is developed to locate the fragments for each authentication request. Moreover, security analysis shows that the framework can guarantee availability despite multiple client failures, unlike centralized alternatives. Performance evaluation demonstrates that the proposed scheme can reduce the authentication process delay by up to 2.8 times compared to that of conventional systems. In [134], the authors present a privacy-aware authentication framework for multi-server environments. In particular, the proposed scheme utilizes multiple permission servers acting as consensus nodes in the Ouroboros consensus mechanism [135] to ensure the consistency of users' access by smart cards or mobile devices. Additionally, the proposed framework utilizes the ECDSA to create and verify signatures. The digital signature is then included in every transaction, along with the identity, the public key, and the revocation status of the user. Security analysis shows that the proposed scheme is secured against multiple attacks such as impersonation, server spoofing, replay, and MITM attacks. Performance analysis demonstrates that the proposed framework can reduce communication costs by up to 3.2 times compared to baseline approaches.

7.3. Unmanned Aerial Vehicles Networks

In Unmanned Aerial Vehicles (UAVs) networks, it is crucial to ensure secure and reliable verification of the identity and legitimacy of unmanned aerial vehicles, mitigate risks associated with unauthorized access, and protect sensitive data during

communication and collaboration. To this end, a blockchain-enabled privacy-preserving and lightweight authentication protocol is developed in [136] to achieve secure and efficient communication between UAVs and ground control stations. The protocol combines ECC, hash functions, and digital signatures to enable mutual authentication and prevent various attacks while minimizing computation and communication costs. Particularly, the framework utilizes blockchain for UAV identity and credential management to mitigate security risks associated with device tampering and credential theft. The protocol comprises registration, authentication, password update, and revocation phases to securely register UAVs and facilitate access control. Security analysis using the AVISPA tool [59] demonstrates the framework's resilience against common attacks such as DDoS and MITM. Performance evaluation shows that the protocol reduces computation overhead by 10.45% and communication cost by nearly 60% compared to existing schemes. Similarly, in [137], the authors propose a novel authentication protocol integrating cloud computing and blockchain technology to improve security and efficiency for UAVs in flying ad-hoc networks. Particularly, blockchain is utilized to provide decentralized access control via distributed ledger transactions validated through the PBFT consensus protocol between ground station servers. Moreover, the framework employs metadata, which contains only the addresses of actual data. After being uploaded to the blockchain, UAV actual data undergoes encryption and secure cloud storage for future retrieval. Security analysis using the AVISPA tool shows strong session key security along with resilience to MITM attacks. Experiment results demonstrate that the framework can reduce computational overheads by 2.13 times compared to related schemes.

7.4. Summary

In this section, we discuss blockchain-based authentication approaches in emerging application areas including wireless networking, identity management, and UAV networks. As summarized in Table 5, Blockchain plays a crucial role in wireless networking by providing secure authentication, ensuring data integrity, and establishing trust in dynamic and heterogeneous environments, addressing challenges in technologies including 5G, 6G, and satellite communication. Utilizing mechanisms such as group authentication schemes and privacy-preserving protocols, the proposed framework can enhance security, reduce complexity, and improve efficiency in wireless communication networks. For identity management, the proposed approaches utilize blockchain's consensus mechanism, smart contract, and related cryptography mechanisms to enhance privacy, efficiency, and reliability throughout the entire lifecycle of digital identities. In UAV networks, mechanisms such as ECC, hash functions, and digital signatures are utilized to authenticate UAVs, mitigate unauthorized access, and provide a decentralized platform for managing UAV operations. A common open issue in the areas discussed in this Section includes scalability issues due to the limited available resources. Moreover, energy efficiency is a serious concern in UAV networks as it directly impacts UAV operations.

8. Challenges, Open Issues, and Future Direction

8.1. Challenges and Open Issues

8.1.1. Scalability

Scalability poses a significant challenge as blockchain-based authentication frameworks are developed for various types of networks, often with thousands or millions of devices such as IoT or cloud/edge networks. Handling the sheer volume of identity verifications and access validations generated by large user bases is difficult for blockchain technology, which is already facing scalability issues by itself. Particularly, the underlying consensus and encryption mechanisms that secure blockchains also constrain transaction processing speeds, latency, and storage, which are all crucial performance factors for authentication processes. Particularly, in traditional blockchains such as PoW-based networks, there are several approaches including increasing block size and reducing block generation time. However, these approaches have negative impacts on the security of the blockchain, as they significantly increase the risk of forks [9]. Therefore, developing intelligent approaches that can increase the processing capabilities of blockchain without compromising security is a key challenge in improving blockchain-based authentication systems.

8.1.2. Interoperability

The heterogeneity of environments such as IoT, cloud/edge, and healthcare networks causes significant interoperability issues even outside the realm of blockchain. Coupled with the inherent interoperability of blockchain networks, this poses significant challenges for blockchain-based frameworks that need to authenticate devices from various platforms and standards. Particularly, blockchain networks often employ different consensus mechanisms and protocols. However, the cryptography, consensus rules, transaction formats, and block storage differ vastly between blockchains of different consensus protocols. Consequently, transactions and data from one consensus mechanism or protocol are not recognized by others in traditional blockchain systems[138]. Additionally, it is not possible to make different service providers, e.g., hospitals, operate using the same blockchain network or use the same protocol. Therefore, interoperability remains a major obstacle that hinders the effectiveness of blockchain-enabled authentication approaches.

8.1.3. Key Management Challenges

In blockchain-based authentication systems, key management poses several challenges. First, revoking compromised credentials and distributing new keys in decentralized networks such as blockchain is difficult. The decentralized nature of blockchain data means that there is no centralized authority for revocation. Moreover, since the data stored in the blockchain is immutable, it is difficult to revoke issued keys. Second, implementing key recovery mechanisms poses a persistent challenge. In conventional blockchain, once a private key is lost, the user will lose access to the account, and there is no on-chain way to recover the lost key. Third, the limited local storage capacity of devices, such as IoT sensors and vehicles, makes key storage

Table 5: Summary of Blockchain-based Authentication Applications in Emerging Application Areas.

Ref.	Application areas	Objectives	Approaches
[126]	Wireless networking	- Enable group authentication for secure hangovers in 6G networks	- Employ aggregated signatures and D-H key exchange for authentication - Use blockchain for group user batch verification
[127]		- Provide anonymous mutual authentication in 5G networks	- Leverage blockchain and pseudonyms to enable authentication
[128]		- Facilitate authentication for secure roaming services	- Use smart contracts for authentication and session keys management - Propose a key derivation protocol to simplify roaming handovers
[129]		- Allow decentralized authentication in Low Earth Orbit satellite network	- Utilize consortium blockchain and MPT data structure to record and manage devices' data - Propose a lightweight certificateless cryptography scheme to calculate and verify key pairs
[132]	Identity management	- Enable cross-domain identity management	- Use consortium blockchain to enable cross-domain authentication - Leverage a one-way accumulator data structure to reduce time complexity
[133]		- Provide biometric decentralized authentication	- Employ permissioned blockchain to record authentication activities - Propose a decentralized data-splitting mechanism to enhance security in identity data storage
[134]		- Facilitate privacy-aware authentication in multi-server environment	- Utilize Ouroboros-based blockchain to store and manage authentication transactions - Employ ECDSA to generate and verify digital signatures
[136]	UAV Networks	- Allow lightweight anonymous authentication	- Leverage ECC for digital signature generation and verification - Use blockchain for credential management
[137]		- Provide decentralized access control	- Employ PBFT-based blockchain to validate and authorize transactions

complex over extended periods. Fourth, the mobility of vehicles, UAVs, and mobile devices creates difficulties in real-time coordination with authentication infrastructure, hindering the smooth handover of verified keys and potentially introducing windows for identity spoofing during offline periods.

8.2. Future Research Directions

8.2.1. Shardings for Blockchain-based Authentication Systems

To address the scalability issues in blockchain-based authentication systems, sharding can be a promising solution. Sharding is an approach that partitions a blockchain network into multiple sub-networks (shards) for parallel processing of transactions, thereby significantly improving the transaction processing speed [139]. In the context of authentication systems, for example, the blockchain can be divided into multiple shards, each with a number of TAs to issue authentication certificates. When the authentication demands are higher, more shards with more TAs can be added to the network. As a result, authentication certificates can be issued multiple times faster compared to the traditional non-shard approach. For example, in [140], a multi-layer sharding blockchain architecture is proposed to manage decentralized identities (DIDs) in Web 3.0. In the proposed architecture, leader shards are employed to establish trust, while multiple regular shards are utilized for DIDs management, e.g., DIDs registration, authentication, and deletion. As a result, the scalability issue can be mitigated by introducing more shards to the system. However, this also brings forth some challenges. First, in dynamic environments such as mobile computing and vehicular networks, the shards need to be frequently configured according to the number of devices in each shard. Moreover, the division of blockchain into shards weakens the blockchain security. For example, in a blockchain with 5 shards, a 51% attack might only need 11% of network participants to succeed, as opposed to 51% participants in a blockchain with no shard. Therefore, it is crucial to optimize the number of shards while taking into account the security of the blockchain [141].

8.2.2. Sidechains for Blockchain-based Authentication Systems

Sidechain technology is a promising solution to address blockchain's interoperability issues, especially in networks such as healthcare, IoT, and distributed computing. Particularly, sidechain technology enables blockchain networks to employ different protocols to communicate with each other. To this end, cross-chain transfer protocols can be employed, where a set of validators are responsible for validating transactions in and among different blockchain networks (sidechains) [142]. As a result, authentication data from a blockchain can be validated by participants in another blockchain, e.g., when a vehicle moves to a different region. Moreover, authentication data might also be transferred directly, e.g., patient transfers between hospitals. For example, to address the interoperability issues in blockchain-based authentication systems, the authors of [143] introduce a sidechain-enabled system for device authentication in smart communities. Particularly, the approach leverages private side blockchains for managing local registration and authentication processes, while a local main blockchain facilitates information sharing across systems. The optimized two-way peg protocol ensures secure information exchange by dynamically assessing the trustworthiness of smart devices, based on factors such as authentication method, previous authentication information sharing history, and local authentication results. Nevertheless, the use of cross-chain validators also creates a new attack surface where these validators

can be targeted. Moreover, once a blockchain is overwhelmed by attackers, any sidechain that is connected to that blockchain is also at risk [138]. Therefore, the security of sidechain ecosystems needs to be thoroughly analyzed.

8.2.3. Quantum-resistant Blockchain-based Authentication

Quantum computers have the potential to break widely-used cryptographic schemes, such as RSA and ECC, which form the basis for many authentication mechanisms discussed in this paper [144]. If these cryptographic mechanisms are broken, the authentication process, even the blockchain itself, will become easy targets for attackers. Therefore, it is crucial to develop cryptographic mechanisms that are resistant to quantum-based approaches. A promising approach is used in several frameworks [145, 146, 147], which leverage lattice-based cryptography such as Kyber algorithm [148] to mitigate quantum attacks. Particularly, the security of the widely employed cryptographic mechanisms such as RSA and ECC relies on the difficulty of factoring large numbers or solving discrete logarithm problems. Unfortunately, these types of problems might be solved efficiently by quantum algorithms such as Shor's algorithm. On the other hand, lattice-based cryptography is built on mathematical structures called lattices. The security of these systems depends on solving problems such as Shortest Vector Problem and Learning With Errors, which currently cannot be solved efficiently by quantum algorithms.

8.2.4. Quantum Key Distribution

Quantum key distribution (QKD) leverages unique properties of quantum mechanics to enable two remote parties to generate shared random secret keys while detecting any eavesdropping attempt. To this end, key bit values are encoded on individual photons and transmitted over a quantum channel. The receiver then measures each photon to extract an identical key. Any interception and measurement by an attacker will alter the quantum state of photons, and thus eavesdropping attempts can be detected [149]. As a result, QKD provides a powerful mechanism for blockchain authentication against many types of attacks. For example, in [150], a secure and efficient authentication scheme for blockchain-enabled Internet-of-Vehicle systems is developed, which leverages QKD for authentication and key generation. Nevertheless, practical implementation of QKD is challenging due to specific hardware and environment requirements. Therefore, this is still a very potential research direction.

9. Conclusion

Blockchain is an effective solution to address various challenges that conventional authentication systems are facing. In this article, we have presented a comprehensive survey on blockchain applications for authentication in various types of networks. Particularly, we have first provided a tutorial on blockchain technology and the fundamental background of various cryptography techniques and authentication-related attacks. Then, we have discussed the applications of blockchain for authentication in various types of networks including vehicular, IoT, healthcare, and distributed computing. For these applications, we have provided detailed discussions and analyses on how blockchain can be leveraged to facilitate the authentication process. Finally, we have presented the current challenges and open issues and introduced some potential research directions of blockchain for future authentication systems.

Acknowledgement

This research is funded by Vietnam National University Ho Chi Minh City (VNU-HCM) under grant number DS2022-20-07. The authors also acknowledge Ho Chi Minh City University of Technology (HCMUT), VNU-HCM for supporting this study.

References

[1] A. Al Abdulwahid, N. Clarke, S. Furnell, I. Stengel, C. Reich, The Current Use of Authentication Technologies: An Investigative Review, in: Proceedings of 2015 International Conference on Cloud Computing (ICCC), 2015, pp. 1–8. doi:10.1109/CLOUDCOMP.2015.7149658.

[2] M. Papathanasaki, L. Maglaras, N. Ayres, Modern Authentication Methods: A Comprehensive Survey, AI, Computer Science and Robotics Technology (2022). doi:10.5772/acrt.08.

[3] M. Jones, D. Hardt, The oauth 2.0 authorization framework: Bearer token usage, Standard (2012).

[4] M. Schwartz, M. Machulak, M. Schwartz, M. Machulak, Saml, Securing the Perimeter: Deploying Identity and Access Management with Free Open Source Software (2018) 59–103.

[5] I. Authentication, Service for computer networks, IEEE Communications Magazine 163 (6804/94) (1994).

[6] J. Somorovsky, A. Mayer, J. Schwenk, M. Kampmann, M. Jensen, On breaking {SAML}: Be whoever you want to be, in: 21st USENIX Security Symposium (USENIX Security 12), 2012, pp. 397–412.

[7] S. Ludwig, S. Göran, W. Erik, E. Samuel, T. Hannes, Authentication and authorization for constrained environments using the oauth 2.0 framework (ace-oauth), Standard (2012).

[8] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, D. I. Kim, A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks, IEEE Access 7 (2019) 22328–22370. doi:10.1109/ACCESS.2019.2896108.

[9] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, E. Dutkiewicz, Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities, IEEE Access 7 (2019) 85727–85745. doi:10.1109/ACCESS.2019.2925010.

[10] D. Li, W. Peng, W. Deng, F. Gai, A blockchain-based authentication and security mechanism for IoT, in: Proceedings of 2018 27th International Conference on Computer Communication and Networks (ICCCN), IEEE, 2018, pp. 1–6. doi:10.1109/ICCCN.2018.8487449.

[11] P. Sharma, R. Jindal, M. D. Borah, A Review of Blockchain-Based Applications and Challenges, Wireless Personal Communications 123 (2) (2022) 1201–1243. doi:10.1007/s11277-021-09176-7.

[12] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda, S. Islam, Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey, IEEE Access 10 (2022) 113436–113481. doi:10.1109/ACCESS.2022.3216643.

[13] M. Saadeh, A. Sleit, M. Qatawneh, W. Almobaideen, Authentication Techniques for the Internet of Things: A Survey, in: Proceedings of 2016 Cybersecurity and Cyberforensics Conference (CCC), 2016, pp. 28–34. doi:10.1109/CCC.2016.22.

[14] A. Albalawi, A. Almrshed, A. Badhib, S. Alshehri, A Survey on Authentication Techniques for the Internet of Things, in: Proceedings of 2019 International Conference on Computer and Information Sciences (ICCIS), 2019, pp. 1–5. doi:10.1109/ICCISci.2019.8716401.

[15] M. El-hajj, A. Fadlallah, M. Chamoun, A. Serhrouchni, A Survey of Internet of Things (IoT) Authentication Schemes, Sensors 19 (5) (2019). doi:10.3390/s19051141.

[16] F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban, R. C. Bansal, A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network, IEEE Access 9 (2021) 31309–31321. doi:10.1109/ACCESS.2021.3060046.

[17] A. H. Sodhro, A. I. Awad, J. van de Beek, G. Nikolakopoulos, Intelligent authentication of 5G healthcare devices: A survey, Internet of Things 20 (2022) 100610. doi:10.1016/j.iot.2022.100610.

[18] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun, K. Sakurai, Authentication in mobile cloud computing: A survey, Journal of Network and Computer Applications 61 (2016) 59–80. doi:10.1016/j.jnca.2015.10.005.

[19] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, Y. Koucheryavy, Multi-Factor Authentication: A Survey, Cryptography 2 (1) (2018). doi:10.3390/cryptography2010001.

[20] X. Wang, Z. Yan, R. Zhang, P. Zhang, Attacks and defenses in user authentication systems: A survey, Journal of Network and Computer Applications 188 (2021) 103080. doi:10.1016/j.jnca.2021.103080.

[21] Z. Rui, Z. Yan, A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification, IEEE Access 7 (2019) 5994–6009. doi:10.1109/ACCESS.2018.2889996.

[22] A. Y. Khan, R. Latif, S. Latif, S. Tahir, G. Batool, T. Saba, Malicious Insider Attack Detection in IoTs Using Data Analytics, IEEE Access 8 (2020) 11743–11753. doi:10.1109/ACCESS.2019.2959047.

[23] F. M. Benčić, I. P. Žarko, Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph, in: Proceedings of IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018, pp. 1569–1570. doi:10.1109/ICDCS.2018.00171.

[24] S. Nakamoto, Bitcoin: A Peer-to-Peer electronic cash system, Decentralized Business Review (2008) 21260doi:10.2139/ssrn.3440802.

[25] V. Buterin, Ethereum white paper (2014).
URL `https://ethereum.org/en/whitepaper`

[26] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, E. Wustrow, Elliptic Curve Cryptography in Practice, in: N. Christin, R. Safavi-Naini (Eds.), Financial Cryptography and Data Security, Springer, Berlin, Heidelberg, 2014, pp. 157–175. doi:10.1007/978-3-662-45472-5_11.

[27] D. Johnson, A. Menezes, S. Vanstone, The Elliptic Curve Digital Signature Algorithm (ECDSA), International journal of information security 1 (2001) 36–63. doi:10.1007/s102070100002.

[28] S. SECG, 1: Elliptic Curve Cryptography, Standards for Efficient Cryptography Group (1999).

[29] I. Blake, G. Seroussi, N. Smart, Elliptic Curves in Cryptography, Vol. 265 of London Mathematical Society Lecture Note Series, Cambridge University Press, 1999. doi:10.1017/CBO9781107360211.

[30] S. Goldwasser, S. Micali, C. Rackoff, The knowledge complexity of interactive proof-systems, Association for Computing Machinery, New York, NY, USA, 2019, p. 203–225. doi:10.1145/3335741.3335750.

[31] National Institute of Standards and Technology (NIST), Secure Hash Standard (SHS) (FIPS 180-4), Tech. rep., NIST (2022). doi:10.6028/NIST.FIPS.180-4.

[32] P. Rogaway, T. Shrimpton, Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance, in: B. Roy, W. Meier (Eds.), Fast Software Encryption, Springer Berlin Heidelberg, 2004, pp. 371–388. doi:10.1007/978-3-540-25937-4_24.

[33] M. Conti, N. Dragoni, V. Lesyk, A Survey of Man In The Middle Attacks, IEEE Communications Surveys & Tutorials 18 (3) (2016) 2027–2051. doi:10.1109/COMST.2016.2548426.

[34] S. Boonkrong, Authentication and access control: practical cryptography methods and tools, Springer, 2021.

[35] S. Malladi, J. Alves-Foss, R. B. Heckendorn, On preventing replay attacks on security protocols, in: Proceedings of International Conference on Security and Management, Vol. 6, 2002.

[36] M. A. Al-shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, N. Abdullah, M. M. Hamdi, Review of prevention schemes for replay attack in Vehicular Ad hoc Networks (VANETs), in: Proceedings of IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP), IEEE, 2020, pp. 394–398. doi:10.1109/ICICSP50920.2020.9232047.

[37] D. D. N. Nguyen, K. Sood, Y. Xiang, L. Gao, L. Chi, Impersonation Attack Detection in IoT Networks, in: Proceedings of IEEE Global Communications Conference (GLOBECOM), 2022, pp. 6061–6066. doi:10.1109/GLOBECOM48099.2022.10001392.

[38] A. Kim, J. Oh, J. Ryu, K. Lee, A Review of Insider Threat Detection Approaches With IoT Perspective, IEEE Access 8 (2020) 78847–78867. doi:10.1109/ACCESS.2020.2990195.

[39] J. Andress, The basics of information security: understanding the fundamentals of InfoSec in theory and practice, Syngress, 2014.

[40] Z. Lu, G. Qu, Z. Liu, A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy, IEEE Transactions on Intelligent Transportation Systems 20 (2) (2019) 760–776. doi:10.1109/TITS.2018.2818888.

[41] J. Liang, M. Sadiq, G. Yang, D. Cheng, BAC-CRL: Blockchain-Assisted Coded Caching Certificate Revocation List for Authentication in VANETs, Journal of Network and Computer Applications 218 (2023) 103716. doi:10.1016/j.jnca.2023.103716.

[42] M. Azees, P. Vijayakumar, L. J. Deboarh, EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad hoc Networks, IEEE Transactions on Intelligent Transportation Systems 18 (9) (2017) 2467–2476. doi:10.1109/TITS.2016.2634623.

[43] Z. Lu, Q. Wang, G. Qu, H. Zhang, Z. Liu, A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs, IEEE Transactions on Very Large Scale Integration (VLSI) Systems 27 (12) (2019) 2792–2801. doi:10.1109/TVLSI.2019.2929420.

[44] J. K. Shahrouz, M. Analoui, An anonymous authentication scheme with conditional privacy-preserving for Vehicular Ad hoc Networks based on Zero-Knowledge Proof and Blockchain, Ad Hoc Networks 154 (2024) 103349. doi:10.1016/j.adhoc.2023.103349.

[45] B. Chen, Z. Wang, T. Xiang, J. Yang, D. He, K.-K. R. Choo, BCGS: Blockchain-assisted privacy-preserving cross-domain authentication for VANETs, Vehicular Communications 41 (2023) 100602. doi:10.1016/j.vehcom.2023.100602.

[46] M. Buser, J. K. Liu, R. Steinfeld, A. Sakzad, S.-F. Sun, DGM: A Dynamic and Revocable Group Merkle Signature, in: K. Sako, S. Schneider, P. Y. A. Ryan (Eds.), Computer Security (ESORICS 2019), Springer, 2019, pp. 194–214. doi:10.1007/978-3-030-29959-0_10.

[47] H. Zhang, F. Zhao, Cross-domain identity authentication scheme based on blockchain and PKI system, High-Confidence Computing 3 (1) (2023) 100096. doi:10.1016/j.hcc.2022.100096.

[48] J. Benet, IPFS-content addressed, versioned, P2P file system, arXiv preprint arXiv:1407.3561 (2014). doi:10.48550/arXiv.1407.3561.

[49] S. K. Dwivedi, R. Amin, S. Vollala, M. K. Khan, B-HAS: Blockchain-Assisted Efficient Handover Authentication and Secure Communication Protocol in VANETs, IEEE Transactions on Network Science and Engineering 10 (6) (2023) 3491–3504. doi:10.1109/TNSE.2023.3264829.

[50] R. Tandon, A. Verma, P. Gupta, D-BLAC: A dual blockchain-based decentralized architecture for authentication and communication in VANET, Expert Systems with Applications 237 (2024) 121461. doi:10.1016/j.eswa.2023.121461.

[51] K. Parmar, S. Patil, D. Patel, V. Patel, B. Parikh, P. Padaria, Privacy-preserving Authentication Scheme for VANETs using Blockchain Technology, Procedia Computer Science 220 (2023) 40–47. doi:10.1016/j.procs.2023.03.008.

[52] V. Kapoor, V. S. Abraham, R. Singh, Elliptic Curve Cryptography, Ubiquity (2008). doi:10.1145/1386853.1378356.

[53] H. Gilbert, H. Handschuh, Security Analysis of SHA-256 and Sisters, in: M. Matsui, R. J. Zuccherato (Eds.), Selected Areas in Cryptography, Springer Berlin Heidelberg, 2004, pp. 175–193. doi:10.1007/978-3-540-24654-1_13.

[54] S. Aggarwal, N. Kumar, P. Gope, An Efficient Blockchain-Based Authentication Scheme for Energy-Trading in V2G Networks, IEEE Transactions on Industrial Informatics 17 (10) (2021) 6971–6980. doi:10.1109/TII.2020.3030949.

[55] G. Sharma, A. M. Joshi, S. P. Mohanty, sTrade: Blockchain based secure energy trading using Vehicle-to-Grid mutual authentication in smart transportation, Sustainable Energy Technologies and Assessments 57 (2023) 103296. doi:10.1016/j.seta.2023.103296.

[56] K. Xue, X. Luo, Y. Ma, J. Li, J. Liu, D. S. L. Wei, A Distributed Authentication Scheme Based on Smart Contract for Roaming Service in

Mobile Vehicular Networks, IEEE Transactions on Vehicular Technology 71 (5) (2022) 5284–5297. doi:10.1109/TVT.2022.3148303.

[57] S. Tarkoma, C. E. Rothenberg, E. Lagerspetz, Theory and Practice of Bloom Filters for Distributed Systems, IEEE Communications Surveys & Tutorials 14 (1) (2012) 131–155. doi:10.1109/SURV.2011.031611.00024.

[58] A. Vangala, B. Bera, S. Saha, A. K. Das, N. Kumar, Y. Park, Blockchain-Enabled Certificate-Based Authentication for Vehicle Accident Detection and Notification in Intelligent Transportation Systems, IEEE Sensors Journal 21 (14) (2021) 15824–15838. doi:10.1109/JSEN.2020.3009382.

[59] T. AVISPA, Automated Validation of Internet Security Protocols and Applications, EB/OL (2015).

[60] X. Yang, X. Yang, X. Yi, I. Khalil, X. Zhou, D. He, X. Huang, S. Nepal, Blockchain-based Secure and Lightweight Authentication for Internet of Things, IEEE Internet of Things Journal 9 (5) (2021) 3321–3332. doi:10.1109/JIOT.2021.3098007.

[61] K. Tange, M. De Donno, X. Fafoutis, N. Dragoni, A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities, IEEE Communications Surveys & Tutorials 22 (4) (2020) 2489–2520. doi:10.1109/COMST.2020.3011208.

[62] P. C. Sharma, M. R. Mahmood, H. Raja, N. S. Yadav, B. B. Gupta, V. Arya, Secure authentication and privacy-preserving blockchain for Industrial Internet of Things, Computers and Electrical Engineering 108 (2023) 108703. doi:10.1016/j.compeleceng.2023.108703.

[63] S. Liu, L. Chen, H. Yu, S. Gao, H. Fang, BP-AKAA: Blockchain-enforced Privacy-preserving Authentication and Key Agreement and Access Control for IIoT, Journal of Information Security and Applications 73 (2023) 103443. doi:10.1016/j.jisa.2023.103443.

[64] X. Wang, S. Garg, H. Lin, M. J. Piran, J. Hu, M. S. Hossain, Enabling Secure Authentication in Industrial IoT With Transfer Learning Empowered Blockchain, IEEE Transactions on Industrial Informatics 17 (11) (2021) 7725–7733. doi:10.1109/TII.2021.3049405.

[65] D. Li, R. Chen, D. Liu, Y. Song, Y. Ren, Z. Guan, Y. Sun, J. Liu, Blockchain-based Authentication for IIoT Devices with PUF, Journal of Systems Architecture 130 (2022) 102638. doi:10.1016/j.sysarc.2022.102638.

[66] Y. Gao, S. F. Al-Sarawi, D. Abbott, Physical Unclonable Functions, Nature Electronics 3 (2) (2020) 81–91. doi:10.1038/s41928-020-0372-5.

[67] S. Kumari, M. K. Khan, M. Atiquzzaman, User authentication schemes for Wireless Sensor Networks: A review, Ad Hoc Networks 27 (2015) 159–194. doi:10.1016/j.adhoc.2014.11.018.

[68] Z. Cui, F. XUE, S. Zhang, X. Cai, Y. Cao, W. Zhang, J. Chen, A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN, IEEE Transactions on Services Computing 13 (2) (2020) 241–251. doi:10.1109/TSC.2020.2964537.

[69] S. K. Dwivedi, R. Amin, S. Vollala, Design of secured blockchain based decentralized authentication protocol for sensor networks with auditing and accountability, Computer Communications 197 (2023) 124–140. doi:10.1016/j.comcom.2022.10.016.

[70] M. Abdussami, R. Amin, P. Saravanan, S. Vollala, BSAPM: BlockChain based secured authentication protocol for large scale WSN with FPGA implementation, Computer Communications 209 (2023) 63–77. doi:10.1016/j.comcom.2023.06.011.

[71] C. J. F. Cremers, The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols, in: A. Gupta, S. Malik (Eds.), Computer Aided Verification, Springer Berlin Heidelberg, 2008, pp. 414–418. doi:10.1007/978-3-540-70545-1_38.

[72] Y. Chen, X. Yang, T. Li, Y. Ren, Y. Long, A blockchain-empowered authentication scheme for worm detection in Wireless Sensor Network, Digital Communications and Networks (2022). doi:10.1016/j.dcan.2022.04.007.

[73] O. A. Toutonji, S.-M. Yoo, M. Park, Stability analysis of VEISV propagation modeling for network worm attack, Applied Mathematical Modelling 36 (6) (2012) 2751–2761. doi:10.1016/j.apm.2011.09.058.

[74] S. AlJanah, N. Zhang, S. W. Tay, A Survey on Smart Home Authentication: Toward Secure, Multi-Level and Interaction-Based Identification, IEEE Access 9 (2021) 130914–130927. doi:10.1109/ACCESS.2021.3114152.

[75] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, K.-K. R. Choo, HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes, IEEE Internet of Things Journal 7 (2) (2020) 818–829. doi:10.1109/JIOT.2019.2944400.

[76] M. Castro, B. Liskov, Practical Byzantine Fault Tolerance, in: Proceedings of 3rd Symposium on Operating Systems Design and Implementation (OSDI), USENIX Association, New Orleans, LA, 1999.

[77] D. Chaum, E. van Heyst, Group Signatures, in: D. W. Davies (Ed.), Advances in Cryptology (EUROCRYPT '91), Springer Berlin Heidelberg, 1991, pp. 257–265. doi:10.1007/3-540-46416-6_22.

[78] D. Hankerson, S. Vanstone, A. Menezes, Elliptic Curve Arithmetic (2004) 75–152doi:10.1007/0-387-21846-7_3.

[79] X. Xu, Y. Guo, Y. Guo, Fog-enabled private blockchain-based identity authentication scheme for smart home, Computer Communications 205 (2023) 58–68. doi:10.1016/j.comcom.2023.04.005.

[80] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, H. E. Ghazi, Cyber-security in smart grid: Survey and challenges, Computers & Electrical Engineering 67 (2018) 469–482. doi:10.1016/j.compeleceng.2018.01.015.

[81] A. Badshah, M. Waqas, G. Abbas, F. Muhammad, Z. H. Abbas, S. Vimal, M. Bilal, LAKE-BSG: Lightweight authenticated key exchange scheme for blockchain-enabled smart grids, Sustainable Energy Technologies and Assessments 52 (2022) 102248. doi:10.1016/j.seta.2022.102248.

[82] E. Nkurunziza, T. Lawrence, E. Issameldeen, G. Mwitende, AP-HBSG: Authentication protocol for heterogeneous blockchain-based smart grid environment, Computer Communications 212 (2023) 212–226. doi:10.1016/j.comcom.2023.09.034.

[83] K. Sood, S. Yu, D. D. N. Nguyen, Y. Xiang, B. Feng, X. Zhang, A Tutorial on Next Generation Heterogeneous IoT Networks and Node Authentication, IEEE Internet of Things Magazine 4 (4) (2021) 120–126. doi:10.1109/IOTM.001.2100115.

[84] O. A. Khashan, N. M. Khafajah, Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems, Journal of King Saud University - Computer and Information Sciences 35 (2) (2023) 726–739. doi:10.1016/j.jksuci.2023.01.011.

[85] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers, The SIMON and SPECK lightweight block ciphers, in: Proceedings of the 52nd Annual Design Automation Conference (DAC), Association for Computing Machinery, New York, NY, USA, 2015. doi:10.1145/2744769.2747946.

[86] M. O. Rabin, Digitalized signatures and public-key functions as intractable as factorization (1979).

[87] A. Vangala, A. K. Sutrala, A. K. Das, M. Jo, Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming, IEEE Internet of Things Journal 8 (13) (2021) 10792–10806. doi:10.1109/JIOT.2021.3050676.

[88] M. Castro, B. Liskov, Practical byzantine fault tolerance and proactive recovery, ACM Trans. Comput. Syst. 20 (4) (2002) 398–461. doi:10.1145/571637.571640.

[89] T. Wang, H. Shen, J. Chen, F. Chen, Q. Wu, D. Xie, A hybrid blockchain-based identity authentication scheme for Mobile Crowd Sensing, Future Generation Computer Systems 143 (2023) 40–50. doi:10.1016/j.future.2023.01.013.

[90] J. Groth, M. Maller, Snarky signatures: Minimal signatures of knowledge from simulation-extractable SNARKs, in: J. Katz, H. Shacham (Eds.), Advances in Cryptology (CRYPTO 2017), Springer, 2017, pp. 581–612. doi:10.1007/978-3-319-63715-0_20.

[91] Y. Sun, F. P.-W. Lo, B. Lo, Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey, IEEE Access 7 (2019) 183339–183355. doi:10.1109/ACCESS.2019.2960617.

[92] M. K. Khan, S. Kumari, An Authentication Scheme for Secure Access to Healthcare Services, Journal of Medical Systems 37 (4) (2013) 9954. doi:10.1007/s10916-013-9954-3.

[93] N. D. Sarier, Privacy Preserving Biometric Authentication on the Blockchain for Smart Healthcare, Pervasive and Mobile Computing 86 (2022) 101683. doi:10.1016/j.pmcj.2022.101683.

[94] J. Yuan, Q. Ye, H. Wang, J. Pieprzyk, Secure Computation of the Vector Dominance Problem, in: L. Chen, Y. Mu, W. Susilo (Eds.), Information Security Practice and Experience, Springer Berlin Heidelberg, 2008, pp. 319–333. doi:10.1007/978-3-540-79104-1_23.

[95] A. Mohsin, A. Zaidan, B. Zaidan, O. Albahri, A. Albahri, M. Alsalem, K. Mohammed, Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient

authentication, Computer Standards & Interfaces 66 (2019) 103343. doi:10.1016/j.csi.2019.04.002.

[96] J. Miao, Z. Wang, Z. Wu, X. Ning, P. Tiwari, A Blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things, Expert Systems with Applications 237 (2024) 121329. doi:10.1016/j.eswa.2023.121329.

[97] J. Ryu, D. Kang, D. Won, Improved secure and efficient Chebyshev chaotic map-based user authentication scheme, IEEE Access 10 (2022) 15891–15910. doi:10.1109/ACCESS.2022.3149315.

[98] M. Hegde, R. R. Rao, B. M. Nikhil, DDMIA: Distributed Dynamic Mutual Identity Authentication for Referrals in Blockchain-Based Health Care Networks, IEEE Access 10 (2022) 78557–78575. doi:10.1109/ACCESS.2022.3193238.

[99] N. Alsaeed, F. Nadeem, F. Albalwy, A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing, Future Generation Computer Systems 151 (2024) 162–181. doi:10.1016/j.future.2023.09.032.

[100] E. Dawson, D. Donovan, The breadth of Shamir's secret-sharing scheme, Computers & Security 13 (1) (1994) 69–78. doi:10.1016/0167-4048(94)90097-3.

[101] A. Tomar, N. Gupta, D. Rani, S. Tripathi, Blockchain-assisted authenticated key agreement scheme for IoT-based healthcare system, Internet of Things 23 (2023) 100849. doi:10.1016/j.iot.2023.100849.

[102] Z. H. Mohammed, K. Chankaew, R. R. Vallabhuni, V. R. Sonawane, S. Ambala, M. S, Blockchain-enabled bioacoustics signal authentication for cloud-based electronic medical records, Measurement: Sensors 26 (2023) 100706. doi:10.1016/j.measen.2023.100706.

[103] M. Lakshmanan, G. Anandha Mala, K. Anandkumar, Highly secured EHR management system based on blockchain technology with digitally signed authentication using data sanitization and polynomial interpolation, Biomedical Signal Processing and Control 87 (2024) 105412. doi:10.1016/j.bspc.2023.105412.

[104] Y. Gheraibia, A. Moussaoui, Penguins Search Optimization Algorithm (PeSOA), in: M. Ali, T. Bosse, K. V. Hindriks, M. Hoogendoorn, C. M. Jonker, J. Treur (Eds.), Recent Trends in Applied Artificial Intelligence, Springer Berlin Heidelberg, 2013, pp. 222–231. doi:10.1007/978-3-642-38577-3_23.

[105] Y. Zhuang, C.-R. Shyu, S. Hong, P. Li, L. Zhang, Self-sovereign identity empowered non-fungible patient tokenization for health information exchange using blockchain technology, Computers in Biology and Medicine 157 (2023) 106778. doi:10.1016/j.compbiomed.2023.106778.

[106] S. Guo, X. Hu, S. Guo, X. Qiu, F. Qi, Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System, IEEE Transactions on Industrial Informatics 16 (3) (2020) 1972–1983. doi:10.1109/TII.2019.2938001.

[107] T. R. Gadekallu, Q.-V. Pham, D. C. Nguyen, P. K. R. Maddikunta, N. Deepa, B. Prabadevi, P. N. Pathirana, J. Zhao, W.-J. Hwang, Blockchain for Edge of Things: Applications, Opportunities, and Challenges, IEEE Internet of Things Journal 9 (2) (2022) 964–988. doi:10.1109/JIOT.2021.3119639.

[108] J. H. Park, J. H. Park, Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions, Symmetry 9 (8) (2017). doi:10.3390/sym9080164.

[109] Q. Lyu, H. Li, Z. Deng, J. Wang, Y. Ren, N. Zheng, J. Liu, H. Liu, K.-K. R. Choo, A2UA: An Auditable Anonymous User Authentication Protocol Based on Blockchain for Cloud Services, IEEE Transactions on Cloud Computing 11 (3) (2023) 2546–2561. doi:10.1109/TCC.2022.3216580.

[110] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, K. Yu, AuthPrivacyChain: A Blockchain-Based Access Control Framework With Privacy Protection in Cloud, IEEE Access 8 (2020) 70604–70615. doi:10.1109/ACCESS.2020.2985762.

[111] H.-W. Kim, Y.-S. Jeong, Secure Authentication-Management human-centric Scheme for trusting personal resource information on mobile cloud computing with blockchain, Human-centric Computing and Information Sciences 8 (1) (2018) 11. doi:10.1186/s13673-018-0136-7.

[112] Y. Zhang, L. Xiong, F. Li, X. Niu, H. Wu, A blockchain-based privacy-preserving auditable authentication scheme with hierarchical access control for mobile cloud computing, Journal of Systems Architecture 142 (2023) 102949. doi:10.1016/j.sysarc.2023.102949.

[113] R. Metere, C. Dong, Automated Cryptographic Analysis of the Pedersen Commitment Scheme, in: J. Rak, J. Bay, I. Kotenko, L. Popyack, V. Skormin, K. Szczypiorski (Eds.), Computer Network Security, Springer International Publishing, 2017, pp. 275–287. doi:10.1007/978-3-319-65127-9_22.

[114] H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan, Y. Zhang, Blockchain Empowered Cooperative Authentication With Data Traceability in Vehicular Edge Computing, IEEE Transactions on Vehicular Technology 69 (4) (2020) 4221–4232. doi:10.1109/TVT.2020.2969722.

[115] J. S. Yedidia, W. Freeman, Y. Weiss, Generalized Belief Propagation, in: T. Leen, T. Dietterich, V. Tresp (Eds.), Advances in Neural Information Processing Systems, Vol. 13, MIT Press, 2000, pp. 1–7.

[116] E. S. Babu, A. Barthwal, R. Kaluri, Sec-edge: Trusted blockchain system for enabling the identification and authentication of edge based 5G networks, Computer Communications 199 (2023) 10–29. doi:10.1016/j.comcom.2022.12.001.

[117] G. Cheng, Y. Chen, S. Deng, H. Gao, J. Yin, A Blockchain-Based Mutual Authentication Scheme for Collaborative Edge Computing, IEEE Transactions on Computational Social Systems 9 (1) (2022) 146–158. doi:10.1109/TCSS.2021.3056540.

[118] Y. Wang, X. Jia, Y. Xia, M. K. Khan, D. He, A blockchain-based conditional privacy-preserving authentication scheme for edge computing services, Journal of Information Security and Applications 70 (2022) 103334. doi:10.1016/j.jisa.2022.103334.

[119] M. Zhaofeng, M. Jialin, W. Jihui, S. Zhiguang, Blockchain-Based Decentralized Authentication Modeling Scheme in Edge and IoT Environment, IEEE Internet of Things Journal 8 (4) (2021) 2116–2123. doi:10.1109/JIOT.2020.3037733.

[120] C. Ma, J. Li, K. Wei, B. Liu, M. Ding, L. Yuan, Z. Han, H. Vincent Poor, Trusted AI in Multiagent Systems: An Overview of Privacy and Security for Distributed Learning, Proceedings of the IEEE 111 (9) (2023) 1097–1132. doi:10.1109/JPROC.2023.3306773.

[121] Y. Ma, Q. Cheng, X. Luo, 2PCLA: Provable Secure and Privacy Preserving Enhanced Certificateless Authentication Scheme for Distributed Learning, IEEE Transactions on Information Forensics and Security 18 (2023) 5876–5889. doi:10.1109/TIFS.2023.3318952.

[122] S. Ji, J. Zhang, Y. Zhang, Z. Han, C. Ma, LAFED: A lightweight authentication mechanism for blockchain-enabled federated learning system, Future Generation Computer Systems 145 (2023) 56–67. doi:10.1016/j.future.2023.03.014.

[123] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, G. Muhammad, Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach, IEEE Access 8 (2020) 205071–205087. doi:10.1109/ACCESS.2020.3037474.

[124] Z. Peng, J. Xu, X. Chu, S. Gao, Y. Yao, R. Gu, Y. Tang, VFChain: Enabling Verifiable and Auditable Federated Learning via Blockchain Systems, IEEE Transactions on Network Science and Engineering 9 (1) (2022) 173–186. doi:10.1109/TNSE.2021.3050781.

[125] C. Feng, B. Liu, K. Yu, S. K. Goudos, S. Wan, Blockchain-Empowered Decentralized Horizontal Federated Learning for 5G-Enabled UAVs, IEEE Transactions on Industrial Informatics 18 (5) (2022) 3582–3592. doi:10.1109/TII.2021.3116132.

[126] M. Soni, D. K. Singh, Blockchain-based group authentication scheme for 6G communication network, Physical Communication 57 (2023) 102005. doi:10.1016/j.phycom.2023.102005.

[127] Z. Haddad, Blockchain-enabled anonymous mutual authentication and location privacy-preserving scheme for 5G networks, Journal of King Saud University - Computer and Information Sciences 35 (6) (2023) 101458. doi:10.1016/j.jksuci.2022.11.018.

[128] I. M., M. Raj, V. K. Mishra, S. R., A. K. Das, V. B. K., Mobile-Chain: Secure blockchain based decentralized authentication system for global roaming in mobility networks, Computer Communications 200 (2023) 1–16. doi:10.1016/j.comcom.2022.12.026.

[129] B. Wang, Z. Chang, S. Li, T. Hämäläinen, An Efficient and Privacy-Preserving Blockchain-Based Authentication Scheme for Low Earth Orbit Satellite-Assisted Internet of Things, IEEE Transactions on Aerospace and Electronic Systems 58 (6) (2022) 5153–5164. doi:10.1109/TAES.2022.3187389.

[130] G. Carter, LDAP System Administration: Putting Directories to Work, " O'Reilly Media, Inc.", 2003.

[131] D. Pöhn, W. Hommel, An overview of limitations and approaches in

identity management, in: Proceedings of the 15th International Conference on Availability, Reliability and Security, 2020, pp. 1–10.
[132] R. Chen, F. Shu, S. Huang, L. Huang, H. Liu, J. Liu, K. Lei, BIdM: A Blockchain-Enabled Cross-Domain Identity Management System, Journal of Communications and Information Networks 6 (1) (2021) 44–58. doi:10.23919/JCIN.2021.9387704.
[133] Y. K. Lee, J. Jeong, Securing biometric authentication system using blockchain, ICT Express 7 (3) (2021) 322–326. doi:10.1016/j.icte.2021.08.003.
[134] L. Xiong, F. Li, S. Zeng, T. Peng, Z. Liu, A Blockchain-Based Privacy-Awareness Authentication Scheme With Efficient Revocation for Multi-Server Architectures, IEEE Access 7 (2019) 125840–125853. doi:10.1109/ACCESS.2019.2939368.
[135] A. Kiayias, A. Russell, B. David, R. Oliynykov, Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol, in: J. Katz, H. Shacham (Eds.), Advances in Cryptology (CRYPTO 2017), Springer International Publishing, 2017, pp. 357–388. doi:10.1007/978-3-319-63688-7_12.
[136] M. A. Akram, H. Ahmad, A. N. Mian, A. D. Jurcut, S. Kumari, Blockchain-based privacy-preserving authentication protocol for UAV networks, Computer Networks 224 (2023) 109638. doi:10.1016/j.comnet.2023.109638.
[137] S. Yu, J. Lee, A. K. Sutrala, A. K. Das, Y. Park, LAKA-UAV: Lightweight authentication and key agreement scheme for cloud-assisted Unmanned Aerial Vehicle using blockchain in flying ad-hoc networks, Computer Networks 224 (2023) 109612. doi:10.1016/j.comnet.2023.109612.
[138] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, Y. Xiao, H.-A. Pham, E. Dutkiewicz, N. H. Tuong, FedChain: Secure Proof-of-Stake-Based Framework for Federated-Blockchain Systems, IEEE Transactions on Services Computing 16 (4) (2023) 2642–2656. doi:10.1109/TSC.2023.3240235.
[139] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, R. P. Liu, Survey: Sharding in Blockchains, IEEE Access 8 (2020) 14155–14181. doi:10.1109/ACCESS.2020.2965147.
[140] Y. Liu, B. Zhao, Z. Zhao, J. Liu, X. Lin, Q. Wu, W. Susilo, Ss-did: A secure and scalable web3 decentralized identity utilizing multi-layer sharding blockchain, IEEE Internet of Things Journal (2024).
[141] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, Y. Xiao, D. Niyato, E. Dutkiewicz, Metashard: A novel sharding blockchain platform for metaverse applications, IEEE Transactions on Mobile Computing (2023) 1–14doi:10.1109/TMC.2023.3290955.
[142] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, K.-K. R. Choo, Sidechain technologies in blockchain networks: An examination and state-of-the-art review, Journal of Network and Computer Applications 149 (2020) 102471. doi:10.1016/j.jnca.2019.102471.
[143] M. Li, H. Tang, A. R. Hussein, X. Wang, A sidechain-based decentralized authentication scheme via optimized two-way peg protocol for smart community, IEEE Open Journal of the Communications Society 1 (2020) 282–292.
[144] M. Allende, et al., Quantum-resistance in blockchain networks, Scientific Reports 13 (1) (2023) 5664. doi:10.1038/s41598-023-32701-6.
[145] H. Shekhawat, D. S. Gupta, Quantum-resistance blockchain-assisted certificateless data authentication and key exchange scheme for the smart grid metering infrastructure, Pervasive and Mobile Computing 100 (2024) 101919.
[146] Q. Wang, D. Wang, C. Cheng, D. He, Quantum2fa: Efficient quantum-resistant two-factor authentication scheme for mobile devices, IEEE Transactions on Dependable and Secure Computing 20 (1) (2021) 193–208.
[147] Y. Gong, B.-J. Hu, A quantum-resistant key management scheme using blockchain in c-v2x, IEEE Transactions on Intelligent Transportation Systems (2024).
[148] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, D. Stehlé, Crystals-kyber: a cca-secure module-lattice-based kem, in: 2018 IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, 2018, pp. 353–367.
[149] M. Mehic, et al., Quantum Key Distribution: A Networking Perspective, ACM Comput. Surv. 53 (5) (2020). doi:10.1145/3402192.
[150] Z. Yang, Q. Shi, T. Cheng, Q. Zhang, Q. Liu, Y. Liu, S. Peng, Qbma-biv: Quantum-key-distribution (qkd)-based multi-server authentication scheme for blockchain-enabled internet of vehicles, IEEE Transactions on Intelligent Transportation Systems (2024).

Declaration of interests

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐ The author is an Editorial Board Member/Editor-in-Chief/Associate Editor/Guest Editor for *[Journal name]* and was not involved in the editorial review or the decision to publish this article.

☐ The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

CRediT author statement

Hoang-Anh Pham: Conceptualization, Methodology, Supervision, Writing - Reviewing & Editing.

Cong T. Nguyen.: Conceptualization, Investigation, Visualization, Writing - Original Draft.

Thuong C. Lam: Methodology, Writing – Reviewing.