The Scientific Temper (2025) Vol. 16 (4): 4136-4150
Doi: 10.58414/SCIENTIFICTEMPER.2025.16.4.17
E-ISSN: 2231-6396, ISSN: 0976-8653
https://scientifictemper.com/

REVIEW ARTICLE

A critical review of blockchain-based authentication techniques

Neeraj*, Anita Singhrova

Abstract

Technology is very agile when it comes to securing data integrity, privacy and identity generally, and by extension, technology is very fit for use in the authentication of users and as a device. The focus of this paper lies in an attempt to find alternatives to the authentication in the blockchain, which is based on tokens, biometrics or knowledge. Further, the paper reviews the use of public, private and consortium blockchain in the field of healthcare, IoT, and cloud services. In this review, I will be looking at how strong blockchain-based authentication is compared with the old-school centralized authentication. It covers the advantages to security of decentralizing, but also practical limitations. Next, the challenges of scaling, spending energy, and compliance with legal regulations of blockchain in secure authentication are elaborated and the ways of improvement for blockchain in secure authentication are suggested. It provides a descriptive analysis of blockchain technologies that were recently published and a case study to compare and contrast different blockchain technologies and their usage in authenticating. This is not a systematic review as it does not discuss concepts from one perspective but rather discusses a handful of studies that contain peer-reviewed sources and evaluates the conceptual models and then accordingly assesses their performance in the real world. It offers the advantage of using different blockchain-based authentication instead of centralized systems. It eliminates single points of failure, has light tamper-proof reach back audit trials and controls personal data. The technology itself is still not close to solving those issues, which makes things too costly and too energy consuming, unable to scale and there is little point in the framework of legs. To broaden adoption for future systems, they must be more lightweight and more efficient in consensus protocols and further aligned with regulation.

Keywords: Blockchain technology, Authentication mechanisms, Digital security, Decentralized identity, Scalability, Privacy compliance

Introduction

Today, in the digital environment, security is the paramount need in protecting user data and privacy. Traditional authentication systems have been based on centralized servers and databases that become the single points of failure and are prone to be breached. Data management process through decentralization, transparency and immutability has a good solution by blockchain technology. The verification process spreads onto a network of nodes, deprives it of having a central authority and guarantees the secureness of the recording and verifiability of the authentication events (Şahan, Ekici, & Bahtiyar, 2019).

As opposed to centralized, blockchain-based authentication is totally different. After a user registers in credentials, like passwords, biometrics, and cryptographic keys, they map them with transactions written on a distributed ledger. No single entity that is not accountable can alter or delete the stored records permanently after each authentication event (e.g., login or identity check). Cardoso *et al*. (2019) presented a decentralized access control system based on the blockchain that was more tamper-resistant and reliable than usual. Moreover, blockchain enables a smart contract to automate the verification process, a function to enforce access control policy thereby minimizing human error and consistency.

However, there are some challenges that come with it. One example is when a malicious actor sets up multiple fake identities that s/he uses to disrupt a system, as in the case of Sybil's attack. To tackle this issue, Siddarth *et al*. (2020) proposed reputation-based of voting systems in 'proof of personhood' consensus models to put in check Sybil attacks. There also is the hurdle of integration into legacy systems. Companies are also offering blockchain as a Service (BaaS)

Deenbandhu Chhotu Ram University of Science and Technology, Murthal, Haryana, India.

***Corresponding Author:** Neeraj. Deenbandhu Chhotu Ram University of Science and Technology, Murthal, Haryana, India., E-Mail: neeraj.schcse@dcrustm.org

How to cite this article: Neeraj, Singhrova, A. (2025). A critical review of blockchain-based authentication techniques. The Scientific Temper, 16(4):4136-4150.

Doi: 10.58414/SCIENTIFICTEMPER.2025.16.4.17

Source of support: Nil

Conflict of interest: None.

Received: 15/03/2025 **Accepted:** 14/04/2025 **Published** : 25/04/2025

solutions, such as Amazon's and Microsoft Azure's platforms, in order to create a good adoption of blockchain through cloud computing so the deployment can be scalable (Neeraj & Singhrova, 2023a). Such services allow organizations to use blockchain-based authentication without dealing with any infrastructure on their own, which will encourage adoption in sectors like finance, IoT and healthcare.

Vulnerabilities in the current ways of authentication include a need for more resilient authentication systems that can be used against brute force or phishing attacks. If the biometrics or tokens are multi-factor, then they offer improved protection, but at the cost of new issues. For example, improper storage of biometrics data such as fingerprints, facial scans may cause privacy violations (Bhartiya *et al*., 2018). Additionally, these systems still usually rely on external devices or third-party services as failure points.

Decentralization, given by blockchain, can eliminate many such issues by eliminating the reliance on centralized systems. It, however, lacks scalability and energy consumption performance and thus faces technical challenges. Such high-frequency tasks are not well suited for systems like Bitcoin's Proof-of-Work, which are resource-intensive. Layer 2 solutions and alternative consensus mechanisms that aim to decrease latency and deployment cost are less predicated on the computational load of the blockchain, though there is still much research to be done to bring the blockchain to a level where it can be used by, among other things, real-time IoT authentication (Panait *et al*., 2020; Lesavre *et al*., 2019).

It is also a concern that it is compliance with the privacy laws, such as the GDPR. The legal 'right to be forgotten' is disadvantaged by blockchain's immutability and such design conflicts of privacy-compliant blockchain identity systems (Delgado Mohatar *et al*., 2020; Sanchez Reillo *et al*., 2019; Truong *et al*., 2019).

Considering this, blockchain-based authentication methods have to be critically evaluated. This paper discusses the application of the main token-based, biometric and knowledge-based authentication approaches and how blockchain can add strength to them. In addition, we study the impact on data integrity, privacy and reliability of public, private and consortium blockchain models in different domains. The general situation and specific advances and limitations (energy costs, non-throughputs and legal) are illustrated with case studies of existing research.

Motivation

Real-world implementation challenges are often not considered in most existing reviews on blockchain security, which tend to provide more theoretical discussion. Energy efficiency, scalability, or how practical the system is is mostly either ignored or treated as though it were a simple matter concerning itself only with practical issues. Furthermore, this specific analysis of token-based, biometric and knowledge-based authentication modalities in blockchain environments is seldom found.

To fill these gaps, this review briefly studies the applicability of different blockchain architectures such as in public, in private, or in a consortium for different authentication use cases. Secondly, the performance, legal compliance and scalability of representative schemes in each category are also evaluated. Through this approach, we supply a complete and comparative viewpoint that may help scholarly investigation and practical implementation of safe, decentralized authentication frameworks.

This paper applies a bunch of essential contributions. It classifies and compares blockchain-based authentication mechanisms in a detailed manner and shows how blockchain provides security in token based, biometric and knowledge-based systems. In addition, it evaluates performance and regulatory as well as practical considerations that influence real-world adoption. Also, the paper discusses the importance of smart contracts, quantum resilient authentication and identity systems protected from surveillance. The paper is organized as follows: Section 2 describes fundamental blockchain concepts, i.e., layered architecture and the principal ways of authentication. Section 3 discusses core blockchain features, including peer-to-peer networking, cryptographic techniques, distributed ledgers and smart contracts, as well as a drawerwise comparison and summary of Table 1. Table 2 presents the latest advances in cryptography and applications of blockchain in cloud security reviewed in Section 4. Section 5 identifies the main challenges and possible directions, of blockchain based authentication and discuss the underlying question of scalability, regulations, as well as the integration with other technologies such as cloud and decentralized identity. Section 6 concludes by summarizing the potential of blockchain to change authentication and pointing out the remaining areas that need more innovation.

Blockchain Fundamentals and Authentication Approaches

Overview of Blockchain Technology

Blockchain took its shape with the arrival of bitcoin or being an innovative platform in the year 2008 by Satoshi Nakamoto. In a nutshell, a blockchain is a distributed ledger that makes all the occurring transactions credible and permanent and does not require any central control. It defines a list of records (blocks) that are created and connected sequentially and protected by an encrypted key. Since each block has a record of the hash of the preceding block, in an endeavor to change data in the blocks, all subsequent blocks are rendered useless, thus ensuring that the ledger cannot be corrupted. Initially designed for virtual money, blockchain is now used also as the basis

of smart contracts and decentralized digital identity. The transition from a centralized approach of user and device authentication to a decentralized one practically expands the range of participants that are addressed since trust is not centralized in an organization.

Layered Composition: When it comes to Blockchain systems, they are known to have compositions that are layered. There are six layers, namely, the data layer, the network layer, the consensus layer, the incentive layer, the contract layer, and the applications layer. Each layer also has a specific responsibility in executing the functions, as illustrated below (figure 1).

- The data layer includes the block Data along with the characteristics such as the chain structure that consists of hashes and timestamps, Merkle trees and fundamental cryptographic algorithms, which are Hashing and Encrypting.
- In the network layer information exchange is performed among the nodes, the transaction of data and verification of the node's information in the decentralized network. Besides, there is a consensus layer to have all nodes accept the fact that the ledger of a specific blockchain has the same state with a specific agreement algorithm (for example, PoW, PoS, or PBFT). This layer is essential mostly for the blocks' validation and the creation of new ones within the framework of the blockchain technology.
- The last layer from the above classification, or sometimes it can be considered as part of the consensus layer given the models of classification, actually involves the incentives that encourage participants to be truthful such as mining rewards or fees charged on transactions.
- Subsequently, the contract layer allows for the formation and enforcement of smart contracts, which can be described as programs or scripts carrying out the transaction or some rules when certain parameters are met. At the last layer of the OSI layer model for blockchain integration, there are the applications and use cases on the blockchain platform that include cryptocurrency transactions, identity, and supply chain, etc. Dividing the system into several layers also decentralizes the functionality of a blockchain for better comprehension and enhancement.

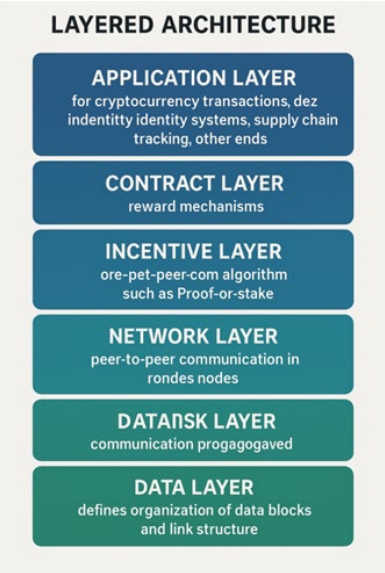

Figure 1: Six-layer architecture of a blockchain system

The stack from bottom to top consists of: (1) Data layer – block data structure, linking (hash pointers), timestamps, basic cryptographic functions; (2) Network layer – peer-to-peer network protocols for node communication, transaction broadcasting, and authentication of nodes; (3) Consensus layer – algorithms (PoW, PoS, DPoS, PBFT, etc.) that achieve agreement on the blockchain state; (4) Incentive layer – mechanisms like mining rewards or token economics that encourage desired behavior; (5) Contract layer – smart contracts and scripts implementing business logic; (6) Application layer – high-level applications (cryptocurrency, identity management, smart grids, etc.) built on the underlying layers. All these layers contribute to achieving secure decentralization of operations such as transactions and data management.

In practice, however, these layers are very closely linked. Indeed, in effective teaching and learning processes, these layers are usually overlapping. For instance, one can assume a cloud service auction to be developed on a consortium blockchain platform. The contract layer could adopt the auction as a smart contract where no honest auctioneer is required in order to composite the buyer and seller in determining the winners. Actually, they were termed as the network and consensus layers, which would make certain that all the nodes working under it, for example, the other participating organizations, would see the same outcomes of the auction and there would be no controversy over the results obtained. At the same time, the data layer logs every bid and transaction as a permanent record of the auction, while the application layer displays the auction front-end to the users. This article demonstrates how blockchain may facilitate large collaborative tasks—as done in the auction process—replacing middlemen by using different parts of the blockchain. Platforms, including campus Ethereum and Hyperledger mentioned in Section 2 offer much of this layered functionality to the developers, hence proving blockchain as an influential tool in almost every industry.

Blockchain-Based Authentication Methods

By overcoming weaknesses of conventional methodologies, such as the single point of failure or trust and the risk of modification of data stored on the system, blockchain can improve additional processes used in authentication techniques. This chapter elaborates on how blockchain enables three forms of authentication tokens: biometrics

and knowledge. In each type, the basic themes of decentralization, immutability and cryptographic trust make it easier for blockchain to provide more security, visibility and user choice.

- *Token-Based Authentication*

In token-based authentication, the user possesses a token, smart card, and cryptography certificate to ensure the person's identification. Regarding token-based systems, blockchain has the capacity to enhance them by decentralizing the procuring and confirmation of such tokens. For instance, Certcoin (Fromknecht *et al*., 2014) is a PKI system that incorporates blockchain and replaces CA with a ledger. Certain stores the fingerprints of users and subscriptions, as well as the corresponding names mapped to keys on the public channels. Nevertheless, it is not private since the activity of users in the blockchain can be traced.

- *Biometric Authentication*

Biometric authentication is based on the use of biometrics such as fingerprints facial or voice recognition. Biometric data is highly secure as well as irreversible and this makes having it incorporated in blockchain a challenge. The first implementations of blockchain-biometric systems, as by Hammudoglu *et al*. (2018), even stored the fingerprint templates on-chain. This approach used the blockchain attributes of immutability but was risky because plaintext biometrics data became exposed. The second was a more secure two-factor cross-domain authentication system by Zhou *et al*. (2018).

- *Knowledge-Based Authentication*

Knowledge-based authentication makes the user prove what he knows, including passwords, Personal Identification numbers (PINs) and questions. These ones are commonly used but they are more sensitive to phishing, reusing, and brute force types of attacks. Such schemes may be strengthened in solutions built on the principles of blockchain, as password management is decentralized and backed by cryptographic protocols. In our previous study, Lu *et al*. identified and recommended a blockchain of a one-time password system that employs the hash chain mechanisms and the given secret seed generates a sequence of login tokens upon iteration. However, by using many hashing functions iteratively, Hastad and Naslund opine that there are some weaknesses, particularly when a MATLAB attacker has partial info on the chain or when two distinct users choose the same seed.

Open-Source Blockchain Platforms Supporting Authentication

Blockchain facilities are available on major open-source authentications that support the development and deployment of the blockchain. From them, Ethereum and Hyperledger are relatively popular due to their flexibility, modularity, and popularity.

Ethereum

As suggested by Vitalik Buterin in 2013, Ethereum is a public blockchain that added a smart contract layer to the blockchain system. It has a virtual machine that supports various programming languages, such as Solidity, for deployment of 'decentralized applications,' commonly referred to as dApps. Regarding the authentication process, Ethereum SCs provide capabilities to regulate access rights, check the solvency of various credentials, and issue NFTs or VC to Ethereum addresses.

Hyperledger

The project was started in 2015 by Linux Foundation and it is an umbrella containing enterprise-level blockchain solutions. Specifically, Hyperledger Fabric is a node of the Hyperledger Project that is specifically designed for an industrial consortium. It also does not elaborate on the use of cryptocurrency and mining, which Ethereum harnesses and is accompanied by the capability of modularity and pluggability of consensus. Hyperledger Fabric uses the Membership Service Provider to manage the authentication, which provides digital certificates, usually in X.509 format. These certificates are used for identification and authorization control in the chain code (smart contract) exercise. In Hyperledger, there are concepts of private channels where some transactions are made between selected participants only. Hyperledger Indy is an identity solution stipend created as a part of Hyperledger that serves as an open-source tools to build, operate, and manage DIDs and verifiable credentials.

Peer-to-Peer Networks for Decentralized Authentication (Revised with References)

In fact, blockchain networks are based on peer-to-peer (P2P) architecture, which means that nodes communicate directly with a lack of a centralized intermediary. It facilitates authentication with some benefits. It kills single points of failure that are usual in typical client-server authentication systems, which means that if one of the nodes fails then the rest of the nodes in the network run. Secondly, authentication requests are spread over the nodes to improve scalability and load balancing. Third, a lack of a central credentials repository increases the privacy of your data and reduces the risk of mass data breaches.

Depending on how the P2P network is structured, they are distributed among three categories: unstructured (such as in Bitcoin's gossip protocol), structured (using Distributed Hash Tables), or hybrid models that try to strike the right balance between efficiency and decentralization (Neeraj & Singhrova, 2022). Authentications can be very good optimized using structured overlays to find credential data among blockchain shards or into other subnetworks.

Furthermore, blockchain networks are "small-world," which implies that nodes have short lengths of paths

between nodes and high clustering coefficients (Watts & Strogatz, 1998; Newman, 2001). Robustness of the authentication in such large scale or intermittently connected environments as the Internet of Things (IoT) is possible due to these characteristics. As an example, Abbas *et al*. (2019) and Qu *et al*. (2018) proposed the lightweight blockchain framework which blockchains were IoT devices scattered out a decentralized peer network to verify each other, cutting down on the traditional centralized brokers.

Such systems operate in the presence of nodes that can be placed into different roles (e.g., non-recording (lightweight) nodes that perform authentication requests, and recording nodes (be responsible for storing the ledger and performing consensus.) That is, resource-constrained devices will not be overloaded with heavy computational tasks, while the network in question will provide this service for their authentication.

It provides such architecture in which devices join, leave, or change roles without breaking authentication consistency. Decentralized verification eliminates relief of denial of service attacks against centralized servers and helps to provide scalable and resilient authentication services to dynamically changing environments like IoT.

Distributed Ledger for Immutable Authentication Logs

A distributed ledger is an append-only, tamper-proof database at the heart of any blockchain system that is replicated across all nodes in the network. It helps in maintaining the integrity, transparency and readability of authentication records. However, in traditional systems, authentication logs are stored in centralized databases, which can be altered, erased, lost and in rare instances, gibberish is added to it by an admin or malicious member of staff. On the other hand, the blockchain ledger guarantees that after a record of an auth event (like login or credential issuance), it cannot be altered or deleted back in time. The enforced immutability is through cryptographic linking of the blocks and consensus algorithms. To produce an attack chain that works, an attacker should be able to control a majority of the network, or he should compromise strong hash functions, which is an extremely difficult task for a well protected blockchain network (Narayanan *et al*., 2016). Because blockchain has these properties, it is an ideal place to store high intelligence authentication logs essential for auditing, forensic investigation, and regulatory compliance. Additionally, the ledger is distributed across many nodes so they can still draw from authentication data even in the event some nodes are offline or compromised. The validation and maintenance of the ledger is done by each node, so no authority can have sole control of the records. This collective validation makes sure that the authentication records that were forged somehow, are not accepted, even if some part of the network is under attack.

The thing that distributed ledgers like a good deed are helpful for is verifying the provenance of things. In federated or multi-organizational systems, where entities issue different credentials (universities, employers, government agency), they are located and traced on the chain. The timestamps, origin signature and revocation record (the latter, if any), are done for each credential. It allows for processing of credentials by time and institutions, in a granular, verifiable way. For instance, all stakeholders can transparently review the user's digital certificate from Authority A revoked by Authority B.

Nevertheless, some level of discretion is required. Such metadata leakage of information like login timestamps, IP ranges, or user identifiers may be provided by recording detailed authentication events on a public blockchain. To do so, permissioned blockchains restrict the access to the authorized nodes (Zheng *et al*., 2017), and privacy enhancing ones are used, for instance, storing only hashed references to the off chain data or applying zero knowledge proofs. For instance, Bhartiya *et al*. (2018) and Alrehaili & Mir (2020) also studied systems where the data such as only verifiable commitments and not raw authentication details are posted on-chain. This balance is achieved between transparency and confidentiality because systems can attest in a public manner that authentication has occurred without leaking any data about a person or their sensitive information. Distributed ledgers do so (Zulkifl *et al*., 2022; Huang *et al*., 2019) as they help increase trustworthiness of authentication by providing verifiable, immutable, and tamper evident records.

Asymmetric Cryptography and Encryption Techniques

Underlying blockchain systems, and more importantly, used in authentication, is asymmetric (also called public key) cryptography. In such a blockchain based network, each user or device is identified uniquely with a public key and the authentication is verified by proving the possession of the private key corresponding to it. In contrast with traditional client-server password systems where a server owns a secret from which client credentials are derived, blockchain authentication grants users to keep private keys to themselves and only to sign cryptographic challenges rather than revealing credentials.

This model enhances security significantly. An example is that when a user tries to authenticate itself by signing a nonce (random challenge) with their private key. Using this public key corresponding to this signature, any node in a blockchain network can verify this signature, therefore confirming that the user is authentic but never revealing the private key. It is this process that defends against replay attacks, eavesdropping and server side credential leak. This model can be also be used by devices in an IoT environment to securely authenticate themselves with the public key of a trusted gateway or recipient for example, to encrypt messages for confidentiality and integrity.

Often, blockchain systems create this basic mechanism even more advanced in cryptography via more complex cryptographic schemes. For example, multi-signature (multisig) authentication involves multiple private key holders needing to validates a transaction or request. This is very handy in the high security situations like enterprise login or common custody of digital assets. In the authentication contexts, multisig can be considered a cryptographic form of multi factor authentication and this means that no single key holder can independently act. Privacy enhancement is performed by blind signatures and zero knowledge proofs (ZKPs). A blind signature allows a user to sign a credential by an authority whilst never revealing the content of the credential. Thus, anonymous tokens (such as age verification credentials) can be issued without linking them to the real user identities. For example, Blind signatures in Systems such as Anonymous Verifications (AV) are used to verify users' rights and preserve user anonymity (Aitzhan & Svetinovic, 2018). Another method of a privacy preserving technique is zero knowledge proof (ZKP), a method through which a user can prove a knowledge of the secret (such as a password or a biometric match but without the secret itself. The research on these techniques for decentralized authentication is active and it is highly promising in use for identity systems (Truong *et al*. 2019). Decentralized recovery and revocation mechanisms are also achieved by asymmetric cryptography. As it is, in some identity systems, recovery protocols are run via smart contracts and social guardians, trusted individuals or organizations who can step in in case of a lost private key without having to engage with a central authority. Nevertheless, private keys have to be kept secure. The attacker can have full access to the identity or device if a key is compromised. For this reason, numerous systems protect themselves against theft by using hardware security modules (HSMs), exclusive enclaves, or mnemonic recovery systems. The advent of quantum computing threatens to break current cryptographic primitives, and in addition, leads to a tremendous desirable for mathematical theorems that provide certificates to the safety of cryptographic algorithms. To do this, researchers are looking at quantum resistant algorithms, i.e, lattice based encryption. As a pre-quantum secure data protection, the Lattice-Based RSA (LB-RSA) scheme was proposed by Mustafa *et al*. (2020) as an IoT data security approach against an emerging threat.

The scope of this paper is to summarize the usefulness of asymmetric encryption as the security base of blockchain while other solutions are used with it to mitigate possible weaknesses and shortcomings. Blockchain's integration with advanced cryptographic techniques goes a long way in providing security, user-focus, and making blockchain based authentication systems future ready.

Smart Contracts for Access Control and Automation

A smart contract is a self-executing script stored on the blockchain that is executed automatically as soon as some set conditions come into place. To a certain extent, smart contracts can play the role of decentralized enforcement mechanisms for access control policies in the context of authentication. Authentication rules are immutable after deployment, i.e. users and administrators cannot change the authentication rules at will aud nonlinearly, making it transparent and consistent how the rules will be enforced. Stub selection using authentication gates is discarded in favor of a smart contract. For instance, in a decentralized storage system, a smart contract can maintain a whitelist of users underneath which permission has been granted (via the public keys). When a user requests to access a file, it is the policy of this contract that must be checked to see if the request complies — eg., identity, time constraints, etc., or payment conditions; if the request complies, it is granted and if this is not the case, then it is denied. And every single decision made and the logic behind it is recorded transparently on the blockchain to hold each other accountable and be audit able. Sources of programmability are one reason why smart contracts drew attention. Some oracles (trusted off chain data feeds) allow them to integrate with oracles which can adapt access control rules according to real world events. For instance, a contract could take away access if a regulation was triggered or change permissions depending on the state of a system external to the user interface's controlled system. Dynamic access control systems do not achieve this level of dynamism.

Also, smart contracts allow blockchain components to be interoperable. For example, an authentication contract may call an arbitrary token contract if the login happens only if the user holds a certain token. In certain scenarios, authentication can be tied to identity system such as decentralized the decentralized identifiers (DIDs) and verifiable credentials, so portable and cross platform identity system. The power of smart contract, however, brings new risks along with it. Even if the contract is vulnerable, an attacker can exploit the technology, and have, for instance, unauthorized access or have users permanently locked out. Examples like the DAO exploit on Ethereum in 2016 are examples of important incidents that are dominated by the security of developed contract. To prevent such risks, developers have to adopt formal verification techniques, exhaustively code audits and use battle tested libraries such as OpenZeppelin to develop authentication related smart contracts (Dai *et al*., 2017).

Singh *et al*. (2021) suggested an authentication mechanism that would be based on the integration of smart contracts with Lamport Merkle Digital Signatures and lightweight cipher algorithm. This system enabled secure employee data management and enforced the cryptographic policies always through automation. The approach decreased the likelihood of human error and administrative misuse with an expected performance in

resource constrained environment. Governance models that can be added to smart contracts in order to enhance authentication systems further. For example, one can upgrade access rules in a condition that occurs due to multi party consensus among stakeholders, reducing the risk of unilateral changes, as well as building trust in a common environment. And the summary of the smart contract is that it is a powerful tool for automating, decentralizing, and safeguarding the access control components. They do away with centralized oversight to give policy enforcement, helps reduce administrative overhead, and transparency in authentication workflows. Putting the cryptographic identity models of blockchain together with smart contracts enables self sustaining authentication ecosystems where tension can be removed from trust, from having it exist in institutions, and instead encoded into code.

Applications of Blockchain in Authentication Systems

Nowadays, these core blockchain mechanisms discussed earlier are being used actively in multiple areas to enhance the authentication frameworks. In Table 1, these applications are compared by Table 1's unique approach, key features, and domain specific benefits. In the ensuing, we take a look at some of the case studies used to establish how the blockchain offers improved security, privacy and scalability to authentication systems across actual environments.

Huang *et al*. (2019) proposed a blockchain based authentication framework in industrial IoT (IIoT) using Directed Acyclic Graph structure with credit based Proof of Work scheme. In this model, the trust scores provided by this model (or the credits), which represented how much we trusted the node, were such that only reliable devices could contribute to consensus. With this DAG based structure, parallel transaction validation is enabled, and thus it uses well in a very high throughput environment such as smart factory. It ensured exchange of sensor data and had Sybil attack prevention, proving blockchain's efficiency in distributed machine identification.

Zulkifli *et al*. (2022) presents the FBASHI system (Fuzzy Blockchain based Authentication, Authorization and Audit) based on Hyperledger Fabric in the healthcare domain. It uses blockchain along with fuzzy to dynamically and dynamically authenticate the user according to his contextual behavior. Suppose that it proves to be suspicious way to act as if a medical device does, the system demands for more authentication in spite of. Access logs and authorization rules together the blockchain preserve patient anonymity by pseudonymization.

For example, Secure authentication has also been adapted in vehicular networks (VANETs). Liu *et al*. (2022) proposed a dual blockchain architecture for vehicle identity and credentials ledgers and their message exchange ledger. The separation has positive scalability and reputation based validation; vehicles that transmit a lot of reliable messages get higher trust scores. It offers real time authorization of messages that are broadcast about safety, and independence from centralized transportation authorities.

Alkhliwi (2022) presents the Blockchain-Based Data Access and Secure Sharing (BDASS) model in cloud based data sharing. By integrating blockchain with ciphertext-policy attribute based encryption (CP-ABE), it enables only the decryption of the data by users having specific attributes (e.g., job role or clearance level). This makes blockchain store access policies and track key distribution transparently so that policies can be ensured without a centralized administrator. This design provides an extensive improvement on data confidentiality and traceability in multi-organization environments.

Vignesh and Prasad (2022) conducted research to create an authentication system which is a combination of Lamport Merkle Digital Signatures (LMDS) and a light weight cipher algorithm (NLCA) for corporate identity management. One time signatures are used to verify each employee login so that there is no replay attack. These sessions get recorded in the blockchain and kept on the network free from hacking or tampering of the files just in case any record of credentials goes missing from the server. In this, blockchain and cryptography are made to work together to secure internal enterprise authentication while increasing the data retrieval speed.

There are other sectors which are equally promising applications. In cloud setting, Gao *et al*. (2021) log and verification multy party computations' integrity and fairness through blockchain. A mutual authentication protocol for smart farming IoT devices was developed by Vangala *et al*. (2021) allowing decentralized, cellular independent authentication between gateways and devices which is very suitable for rural setting. Building on work by Li *et al* (2021) blockchain is applied to satellite ground communication space, biasing all commands sent to satellites on the ledger and authentically and valided. Abbas *et al* (2019), Qu *et al* (2018) along with Abbas *et al* (2019) are for lightweight IoT authentication via simplified blockchain architecture with minimal consensus protocols fit for edge computing scenario. In a private blockchain model in the smart home context, Dorri *et al*. (2017) performed the authentication and the management of device interactions without resorting to cloud services and maintain the privacy. As per Dwivedi *et al*. (2019), they developed a system of using hybrid blockchain for managing electronic medical records. Permissioned chains controlled by hospitals for data access and the public chains for audit trail, which allows for the patients to control their data as well as meet compliance needs.

Bubbles of trust framework as proposed by Hammi *et al*. (2018) and scalable IoT architectures (Singh *et al*. (2021) are the extensions of this paradigm. IOT bubbles of trust form the micro blockchain around small group of IOT

Table 1: Comparative Analysis of Blockchain-Based Authentication Applications

Authors	*Sector*	*Blockchain solution*	*Key features*	*Benefits*
Huang *et al*., 2019	Industrial IoT	Credit-based consensus with PoW (DAG-based chain)	Uses a DAG structure for blockchain; assigns trust credits to nodes for consensus; secures sensor data access confidentially	Improved transaction efficiency and system security in smart factory environments
Zulkifl *et al*., 2022	Healthcare IoT	FBASHI on Hyperledger (Fuzzy Blockchain AAA)	Integrates fuzzy logic for dynamic Authentication, Authorization, Audit; permissioned ledger (Fabric) ensuring anonymity	Ensures adaptive security and privacy for patient data in dynamic IoT environments
Liu *et al*., 2022	Vehicular Networks	Dual blockchain for VANETs	One blockchain for vehicle identity & certificates; another for message integrity and sender reputation in VANET communications	Enhances communication security and authenticates users (vehicles) while preserving privacy in VANETs
Alkhliwi, 2022	Data Management	BDASS – Blockchain-Based Data Access & Sharing	Employs ciphertext-policy attribute-based encryption (CP-ABE) with blockchain-managed access policies	Only authorized users can access encrypted data; significantly improves data confidentiality in sharing scenarios
Vignesh & Prasad, 2022	Enterprise (HR)	Blockchain authentication with LMDS & NLCA	Uses Lamport–Merkle one-time signatures and a custom lightweight crypto algorithm; records employee data events on-chain	Strengthens encryption for employee data; enables secure, efficient data retrieval and tamper-proof record management
Gao *et al*., 2021	Data Integrity	Blockchain-secured *searchable encryption* model	Blockchain logs all data access and verification steps; ensures fairness in multi-party computations	Guarantees data integrity and fair results in collaborative computations with fine-grained access control
Vangala *et al*., 2021	Smart Farming IoT	Blockchain-based key agreement protocol	IoT devices and gateways perform mutual authentication via a shared blockchain ledger	Facilitates secure device-to-device communication; ensures only trusted devices join the farm network
Li *et al*., 2021	Satellite Comm.	Blockchain architecture for satellite-ground security	Distributed ledger linking satellites and ground stations; smart contracts for transmission rights and payment settlement	Secures data transmission between satellites and ground; transparent management of transmission authentication and rights
Abbas *et al*., 2019	IoT (General)	Lightweight blockchain model for IoT	Simplified consensus for resource-constrained devices; privacy-preserving data storage	Maintains high security with minimal resource use; suitable for IoT nodes with limited power and bandwidth
Qu *et al*., 2018	Smart Homes IoT	Private blockchain for home IoT security	Local blockchain at home; focuses on data privacy and low-power operation; minimal external dependencies	Enhances privacy and reduces reliance on cloud; efficient, autonomous security management in smart homes
Dorri *et al*., 2017	Healthcare (Records)	Hybrid blockchain for medical data sharing	Combines private (hospital) and public blockchain: private for data access, public for audit logs; emphasizes patient consent	Protects electronic medical data with user-centric access control; provides transparent audit trail for compliance
Dwivedi *et al*., 2019	IoT Ecosystems	*Bubbles of Trust* architecture	Forms isolated trust domains («bubbles») among IoT devices; each bubble manages its own micro-blockchain for internal authentication	Isolates and contains security incidents; improves overall IoT system performance and energy efficiency by localizing trust decisions
Singh *et al*.,2021	General IoT	Scalable & energy-efficient IoT blockchain	Studies novel consensus and sharding methods; explores reducing complexity for IoT nodes without sacrificing security	Addresses key challenges of scalability and high energy use; moves toward making blockchain feasible in large-scale IoT deployments

devices to make the intra group authentication secure. To address the energy and scalability constraints of IoT-Blockchain Systems, Singh *et al*., modified the consensus algorithms and storage strategies to make it sure that even resource limited devices can participate in secure decentralised authentication without storing the full chain.

All of these examples collectively show that blockchain-based authentication can be adapted to a wide range of environments, such as realizing IIoT, healthcare, smart home and VANETs, among others. Decentralized trust models, tamper-proof audit trails, and privacy preserving tools being provided by blockchain provide better security than the

commonly used traditional one on the central point system. Despite these implementations, they also emphasize that for customization of the domain, it matters. To be applicable to a specific sector, the resource, regulatory and operational needs of each sector must be adapted to consensus protocols, data handling models, and privacy controls.

Across these different applications, one theme that is common is that blockchain-based solutions are able to overcome a lot of the problems that exist in traditional authentication. In blockchain systems, scalable, tamper resistance and privacy conscious authentication frameworks are offered by the use of the peer to peer trust networks, immutable logs, cryptographic authentication and smart contract automation. They serve either as replacements or an addition to centralized authentication servers, addressing issues of single points of failures, data silos, and no user control in fields as disparate as IIoT, smart grids, electricity storage, etc. As you can see, solutions that report improved security (resilient to certain attacks) and comparable or not bad performance at the cost of care, sometimes, expansive system design to lessen additive blockchain's postage. These implementations encapsulate blockchain's capacity to safeguard today's digital intermediation in a new way — self sovereign identity, multi party access control transparency and trustless authentications are now realized even if they are maturing economies.

It has been shown to be viable in several domains and blockchain as an authentication technology can certainly be expected to grow from strength to strength. These models are further being developed with an aim to be energy efficient and scalable for broad deployment in future research and development. In controlled environments, such lightweight blockchain models (e.g. models trialed in IoT scenarios) will be important in order to maintain real time performance with adequate security. In the following section, I will discuss other advancements that bring a combination of blockchain and other cryptographic innovations to increase the authenticity and protect data in the cloud environment.

Advanced Blockchain and Cryptographic Solutions for Cloud Security

Blockchain technology has been enhanced to the fore sources through integration with the most cutting edge cryptographic approaches as cyber assaults deteriorate in affixing. They further enrich the cloud and distributed environments with various kinds of user authentication, data confidentiality, and integrity improvements. This section discusses a number of them and goes in depth into cryptographic frameworks, hybrid encryption methods and quantum resilient approaches promising to make blockchain cloud security stronger. A summary of these solutions is compared at the end of the section in Table 2.

Advanced Cryptographic Frameworks for Secure Authentication

To improve identity protection in cloud service, Shrivastava *et al*. (2022) proposed the Modified Infinite Chaotic Elliptic Cryptography (MICEC) framework. The validated content is provided through MICEC by infinite elliptic curve key generation, chaotic neural network hashing and LDA based AI recommendation layer. The design allows for a multi-stage interposition which provides better ownership protection and prevents from identity spoofing. Confidentiality is ensured by encryption, integrity by chaotic hashing and contextual intelligence by LDA-based verification are combined in one complete defense for cloud based authentication. Singh and Jha (2022) introduced a biologically inspired approach namely African Buffalo Based Elapid Crypto Model (AB-ECM). It is a two stage encryption in which the encryption involves compression followed by pattern encoding, decryption isn't possible until and unless receiver's decryption key exactly matches with that of the sender's. In this design, if the mutual authentication is meaningful, mutually authenticated secrets are assumed to be held by both parties. The model is tolerant to the man in the middle and key guessing attacks and provides for protecting data in transit.

Almajed and Almogren (2019) developed then the Secure and Efficient Encoding (SE-Enc) technique per have a better symmetric encryption schemes. In order to avoid the vulnerability to Known-Plaintext, Chosen-Plaintext, and Chosen-Ciphertext attacks, SE-Enc uses elliptic curve cryptography (ECC) to randomize plaintext prior to encryption. In particular, their proof based analysis confirms that SE-Enc provides stronger confidentiality with relatively little performance trade-offs, so it is suitable for secure blockchain transactions and storage.

Patterned Cipher Block (PCB) is a low latency cipher mode for mutual authentication and integrity checks, it was introduced by Oh *et al*. (2020) in the encryption itself. Symmetric encryption algorithms (e.g. AES) are enhanced by PCB that interleaves authentication steps, while verifying messages only if a specific format is observed. It has a modular nature that does not require any change in other blockchain layers of communication allowing data exchange between nodes in a secure and fast manner. While each of these solutions provides a specific improvement, they collectively demonstrate how design of advanced cryptographic primitives can enhance the inherited security strength of blockchain while maintaining efforts to prevent spoofing, replay and cryptanalysis, and to enhance operational efficiency.

Hybrid Encryption and Optimization Techniques

According to Wahab *et al*. (2021), a hybrid model was proposed, based on RSA encryption, Huffman coding and wavelet image compression. In this multi layer pipeline,

Table 2: Comparative Analysis of Advanced Blockchain and Cryptographic Solutions

Authors	*Solution (Technique)*	*Application area*	*Key mechanisms*	*Key benefits*	*Challenges addressed*
Shrivastava *et al*.,2022	Modified Infinite Chaotic Elliptic Cryptography (MICEC)	Cloud security/ identity	Infinite-dimensional ECC for key generation; chaotic neural network hashing; LDA-based content validation	Enhanced authentication and ownership proof (multi-layer security)	Identity theft, data tampering in cloud
Singh and Jha,2022	African Buffalo-based Elapid Crypto Model (AB-ECM)	Data transmission security	Two-stage data compression + encryption; secret key verification (mutual auditing)	Secure and efficient data transmission (requires matching keys)	Interception, unauthorized decryption («man-in-middle»)
Almajed and Almogren,2019	Secure and Efficient Encoding (SE-Enc)	Cloud security	Symmetric encryption with ECC-based encoding phase; minimal padding	Resists KPA, CPA, CCA attacks on symmetric ciphers	Encryption vulnerabilities in symmetric schemes (KPA, CPA, CCA)
Oh *et al*.,2020	Patterned Cipher Block (PCB)	Cryptography (block ciphers)	New cipher operation mode with built-in mutual authentication	Reduces latency, improves security for any symmetric cipher	Compatibility with new symmetric algorithms (future-proofing cipher modes)
Wahab *et al*.,2021	Hybrid Data Compression & Encryption	Data compression & security	Huffman coding + DWT compression; RSA encryption; LSB steganography embedding	Efficient data transmission with confidentiality and stealth	Slow networks, bandwidth limitations; secure transfer over untrusted channels
Kim *et al*.,2019	Random Phase Key Exchange (with Ring extension)	Image cryptography / key sharing	Diffie–Hellman using sinusoidal waveforms (optical signals); ring-type multi-party key exchange	Secure shared secret key establishment for groups (including images)	Challenges in generating shared keys for multiple parties (esp. for multimedia data)
Khari *et al*.,2020	Elliptic Galois Cryptography + Steganography	Medical data security	Encrypt medical data (ECC); embed in image via XOR matrix; optimize embedding with Firefly algorithm	Greatly enhances privacy and security of sensitive data (hidden and encrypted)	Privacy of sensitive health information; resisting data exposure attacks
Li and Han,2019	Educational Records Secure Storage & Sharing (EduRSS)	Educational data security	Permissioned blockchain with smart contracts for access control; anti-tampering audit system	Secure cross-institutional record sharing; user-controlled access revocation	Data integrity and privacy in academic records; trust in cross-domain data sharing
Mustafa *et al*.,2020	Lattice-Based RSA (LB-RSA)	IoT and cloud security	RSA variant using lattice-based cryptography (quantum-resistant)	Quantum-resistant encryption; strong security proofs; scalable to IoT	Quantum computing threats; classical RSA side-channel vulnerabilities

encrypted data is embedded in steganographically altered media via LSB substitution. A bandwidth efficient and covert transmission channel is obtained for the secure distribution of authentication credentials in constrained or surveilled cloud environments. By extending key exchange protocols into the optical domain utilizing random phase sinusoidal waveforms for image based cryptography, Kim *et al*. (2019) was able to extend key exchange protocols. By means of a ring type key exchange system, multiple parties can derive a common secret after each optical exchange. Secure group authentication goals are supported by this innovation, useful for blockchain network consortiums, or multicast cases where visual or biometric data are exchanged. In Khari *et al*. (2020), a privacy preserving medical data serves with Elliptic Galois cryptography and Matrix XOR steganography is devised. Using Adaptive Firefly optimization to optimize data placement while distorting as little as possible, our system embeds data encrypted in optimized image blocks. It provides dual layer protection, such that instead of just concealing data or encrypting data, it can concealing encrypt data while it is stored, or authenticated, via the blockchain network. In their paper Li and Han (2019) describe the Educational Records Secure Storage and Sharing Scheme (EduRSS), a blockchain based identity and credential management system. EduRSS is built on top of smart contracts and hash based tamper detection to provide

students with the control over their academic records while making the records traceable. Given that authentication is enforced by programmable access policies, this makes the system more secure and transparent than conventional transcript sharing. Hybrid approaches are shown to achieve security along with performance, especially in cloud systems where performance constraints are highly relevant as well as security.

Quanta-Resistant and Future-Proof Authentication

Second, Lattice Based RSA (LB-RSA) was presented by Mustafa *et al*. (2020) as a quantum secure post quantery encryption. Hard lattice problems are used to provide cryptographic strength in the LB-RSA, yet it maintains compatibility with current RSA like signature work flows. Being lightweight, it is suitable for IoT authentication, providing forward security for devices that will run into the quantum era. Since blockchain and authentication systems are moving to locations where they can trust neither the execution environment nor its inhabitants (i.e. untrusted environments), integrating quantum resistant algorithms like LB-RSA will protect the trust layer from future adversaries. In addition, these methods address the current vulnerabilities—timing attacks or key reuse at least by improving key distribution and resistance to side channel attack.

In the past decade, authentication based on blockchain has been quickly progressing and is now much better than the traditional systems. Nevertheless, significant technical and organizational challenges stand between its broad adoption and, for instance, scalability, energy efficiency, regulatory compliance, governance, among others. In this section we describe some key challenges for future work to overcome to enable broader deployment of authentication systems which will utilize blockchain facilities.

While Proof-of-Work (PoW) provides for security, such consensus is not suitable for high throughput authentication systems on account of high latency and computational intensity. To achieve proper authentication, especially in IoT or real time applications, consensus is required to be both rapid and scalable. ProofofStake (PoS), Delegated poS (DPoS) and Practical Byzantine Fault Tolerance (PBFT) are alternatives that are more energy efficient than PoW and faster in stamping consensus; they are more appropriate for the purpose of identity verification (Xie *et al*., 2019). Network bottlenecks (Buterin, 2021) are also worked around with layer-2 solutions such as state channels and rollups as well as sharding. Using these mechanisms, we certify and authenticate real time across large networks with finality and communication overhead as low as possible in sub second time span.

A significant limitation in terms of high energy consumption, particularly for authentication use cases, is inherent of PoW based systems such as Bitcoin. Small blockchains and consensus mechanisms for such authentication like Proof-of-Authentication, hardware based consensus using Trusted Execution Environments (TEEs) are promising (Abbas *et al*., 2019). Also, legitimate energy savings cannot be ignored, and energy awareness could bring down the energy consumed per authentication transaction order of magnitude (Neeraj and Singhrova, 2023b). Wherever IoT and mobile applications exist, a good balance must necessarily be met between decentralization and sustainability.

However, due to the immutability of blockchain, it is challenging to comply with data privacy laws such as the GDPR, which prescribes that data is to be erasable (Zhang & Xue, 2019). In order to comply, ways to do this such as destructive keys for encrypted data in the chain or off chain storage anchored by on chain commitments are being worked on. Second, there has been study in multi party mutability models where changes need collective agreement to satisfy legal requirements without eroding decentralization (Finck, 2018). In addition to that, jurisdiction and liability in a decentralized system are quite ambiguous. However crucial legal technical bridges are to adoption in regulated fields such as finance and healthcare, large scale blockchains today do not provide those.

For example, decentralized governance does not go well with ordinary organizational models. On the other hand, public blockchains can work very well on open governance while permissioned blockchains may be needed where mission critical systems achieve trust based on votes of trusted stakeholders (Androulaki *et al*., 2018). The other barrier is to interface with an existing identity systems (OAuth, SAML). Key solutions here, though, are the ones like a blockchain based OAuth gateway or an identity or even a private blockchain oriented blockchain would be great solutions for a bridge between the legacy layers and the layers built on decentralized ledger. But this is where hybrid architectures will play a key role in the transition from partial to full control of the adopted identity in blockchain.

There are many technological trends that will define decentralized authentication. Self sovereign identity (SSI) frameworks are becoming popular where users have ability to store and own verifiable credentials (uPort, Sovrin). In order to prepare the authentication for quantum era, post quantum cryptography such as lattice based encryption (Mustafa *et al*., 2020) is being worked upon. A reduction in infrastructure overhead, and the ease of experimentation on Blockchain-as-a-Service (BaaS) solutions offered by AWS, Azure and other platforms have helped make the experimentation on the core blockchain a scalable proposition. Further, these domains such as smart city, energy grids and healthcare are carrying out domain specific authentication protocols using blockchain for trustworthy and robust authorization control (Vangala *et al*., 2021; Dwivedi *et al*., 2019).

Conclusion

This paper conducted a detailed review of blockchain based authentication systems by covering, its fundamental principles as well as other current emerging developments in the evolution of these systems. The blockchain technology offers an unprecedented potential for disruption of current authentication paradigm by removing dependence on centralized authorities, multi points of failures, and shifting to the highly tamper resistant cryptographically secured methods. The architecture of blockchain through decentralization, immutability, smart contract based automation is a perfect fit to modern authentication challenges in different sectors. About how blockchain can further strengthen each token based, biometric, and knowledge based authentication methods was analyzed. Decentralized certificate issuance and verification are useful on token-based systems. However blockchain can be used to trust integrity and facilitate distributed identity validation as part of biometric models though privacy preserving techniques are needed in order to prevent the data exposure. Decentralized storage, cryptographic proofs, and such resilience can be gained by knowledge based methods with care taken to avoid replay and phishing vulnerabilities. Blockchain provides better auditability across all methods, a greater level of users' control, as well as enhanced resistance to insider or external attacks.

The advanced cryptographic innovations that are integrated into the blockchain is also one of the reasons beyond the core mechanisms that the blockchain is regarded as an authentication. Multi layered security is introduced on new frameworks via, elliptic encryption, chaotic hashing, AI driven validation, blind signatures and post quantum algorithms. Such solutions, which fortify both performance and protection, particularly within the cloud or IoT ecosystems where existing identity systems suffer, are definitely improving overall and reducing complexity. There are applications in healthcare, smart cities, vehicular networks, and education to justify the fact that this kind of verification isn't simply viable, but the amounts of benefits that are being realized are measurable. But there are challenges to making it to broad adoption. Nevertheless, there are still very important issues such as scalability, energy efficiency, interoperability with legacy systems, and regulatory compliance. The solutions to these problems involve further improvements of the consensus algorithms, privacy preserving techniques, legal frameworks or decentralized governance models. This is a good signal towards energy aware protocols, blockchain as a service platforms, self soverign identity systems. It will be also key to create global standardized decentralized identifiers and verifiable credentials so that secure cross platform authentication can be possible. In short, blockchain will change digital authentication overall as it brings the power of the users, increases data integrity and creates a trustless, yet secure ecosystem. The technological progress continues to be a promising factor for future evolution, but needs to be in line with legal and social expectations, while industries, academia and policymakers should cooperate. Interestingly, when these two elements come together, the outcome may be a kind of blockchain secure authentication on its basis as the bedrock for a better, more private, more private digital world with users as the center.

References

Abbas, N., Asim, M., Tariq, N., Baker, T., & Abbas, S. (2019). A mechanism for securing IoT-enabled applications at the fog layer. *Journal of Sensor and Actuator Networks, 8*(1), 16. https://doi.org/10.3390/jsan8010016

Abughazalah, S., Markantonakis, K., & Mayes, K. (2014). Secure mobile payment on NFC-enabled mobile phones formally analyzed using CasperFDR. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 422–431). IEEE. https://doi.org/10.1109/TrustCom.2014.58

Aitzhan, N. Z., & Svetinovic, D. (2018). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing, 15*(5), 840–852. https://doi.org/10.1109/TDSC.2016.2616861

Alkhliwi, S. (2022). An efficient dynamic access control and security sharing scheme using blockchain. *International Journal of Advanced Applied Sciences, 9*(8), 28–40. https://doi.org/10.21833/ijaas.2022.08.004

Almajed, H. N., & Almogren, A. S. (2019). SE-enc: A secure and efficient encoding scheme using elliptic curve cryptography. *IEEE Access, 7*, 175865–175878. https://doi.org/10.1109/ACCESS.2019.2957087

Al-Naji, F. H., & Zagrouba, R. (2020). CAB-IoT: Continuous authentication architecture based on Blockchain for Internet of Things. *Journal of King Saud University - Computer and Information Sciences, 34*, 2497–2514. https://doi.org/10.1016/j.jksuci.2020.04.015

Alrehaili, A., & Mir, A. (2020). Poster: Blockchain-based key management protocol for resource-constrained IoT devices. In *Proceedings of the 2020 First International Conference on Smart Systems and Emerging Technologies (SMARTTECH)* (pp. 253–254). IEEE. https://doi.org/10.1109/SMARTTECH49988.2020.00058

Athanere, S., & Thakur, R. (2022). Blockchain-based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing. *Journal of King Saud University - Computer and Information Sciences, 34*, 1523–1534. https://doi.org/10.1016/j.jksuci.2022.02.002

Axon, L., & Goldsmith, M. (2016). PB-PKI: A privacy-aware blockchain-based PKI. *arXiv preprint arXiv:1605.07659*. https://arxiv.org/abs/1605.07659

Bertot, J. C., Jaeger, P. T., & Hansen, D. (2012). The impact of policies on government social media usage: Issues, challenges, and recommendations. *Government Information Quarterly, 29*(1), 30–40. https://doi.org/10.1016/j.giq.2011.04.004

Bhartiya, N., Jangid, N., & Jannu, S. (2018). Biometric authentication systems: Security concerns and solutions. In *2018 3rd*

International Conference for Convergence in Technology (I2CT) (pp. 1–6). IEEE. https://doi.org/10.1109/I2CT.2018.8529582

Bhumichitr, K., & Channarukul, S. (2020). Acachain: Academic credential attestation system using blockchain. In *Proceedings of the 11th International Conference on Advances in Information Technology* (pp. 1–8). ACM. https://doi.org/10.1145/3406601.3406637

Brousmiche, K. L., Heno, T., Poulain, C., Dalmieres, A., & Hamida, E. B. (2018). Digitizing, securing and sharing vehicles life-cycle over a consortium blockchain: Lessons learned. In *Proceedings of the 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1–5). IEEE. https://doi.org/10.1109/NTMS.2018.8328744

Buldas, A., Laanoja, R., & Truu, A. (2017). Keyless signature infrastructure and PKI: Hash-tree signatures in pre-and post-quantum world. *International Journal of Services Technology and Management, 23*(1–2), 117–130. https://doi.org/10.1504/IJSTM.2017.083489

Cachin, C. (2016). *Architecture of the Hyperledger blockchain fabric*. IBM Research. Retrieved April 16, 2025, from https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf

Cardoso, J. A., Ishizu, F. T., de Lima, J. T., & de Souza Pinto, J. (2019). Blockchain-based MFA solution: The use of hydro raindrop MFA for information security on WordPress websites. *Brazilian Journal of Operations & Production Management, 16*(2), 281–293. https://doi.org/10.14488/BJOPM.2019.v16.n2.a13

Chen, C., Wang, J., Qiu, F., & Zhao, D. (2016). Resilient distribution system by microgrids formation after natural disasters. *IEEE Transactions on Smart Grid, 7*(2), 958–966. https://doi.org/10.1109/TSG.2015.2418032

Cheney, J., Chiticariu, L., & Tan, W. C. (2009). Provenance in databases: Why, how, and where. *Foundations and Trends in Databases, 1*(4), 379–474. https://doi.org/10.1561/1900000006

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access, 4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation, 2*, 6–10. https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf

Cui, Z., Xue, F., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A hybrid blockchain-based identity authentication scheme for multi-WSN. *IEEE Transactions on Services Computing, 13*, 241–251. https://doi.org/10.1109/TSC.2017.2740384

Dai, P., Mahi, N., Earls, J., & Norta, A. (2017). *Smart-contract value-transfer protocols on a distributed mobile application platform* [White paper]. Qtum Foundation. Retrieved from https://qtum.org/uploads/files/cf6d69348ca50dd985b60425ccf282f3.pdf

Delgado-Mohatar, O., Fierrez, J., Tolosana, R., & Vera-Rodriguez, R. (2020). Blockchain and biometrics: A first look into opportunities and challenges. In R. De Paz Santana, J. Bajo, & M. Corchado (Eds.), *Blockchain and Applications: International Congress* (pp. 169–177). Springer. https://doi.org/10.1007/978-3-030-23813-1_21

Diallo, N., Sanou, J., Ahmed, M. H., & Ouedraogo, A. (2018). eGov-DAO: A better government using blockchain-based decentralized autonomous organization. In *Proceedings of the International Conference on eDemocracy & eGovernment (ICEDEG)* (pp. 166–171). IEEE. https://doi.org/10.1109/ICEDEG.2018.8372357

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering, 30*(7), 1366–1385.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops).* https://doi.org/10.1109/percomw.2017.7917634

Dunphy, P., & Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. *IEEE Security & Privacy, 16*(4), 20–29.

Dwivedi, A., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors, 19*(2), 326.

Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM, 61*(7), 95–102.

Fromknecht, C., Velicanu, D., & Yakoubov, S. (2014). *Certcoin: A Namecoin-based decentralized authentication system* [Unpublished class project].

Gao, H., Luo, S., Ma, Z., Yan, X., & Xu, Y. (2021). BFR-SE: A blockchain-based fair and reliable searchable encryption scheme for IoT with fine-grained access control in cloud environment. *Wireless Communications and Mobile Computing*, 1–21.

Gao, Z., Liu, Y., Zheng, H., Chen, R., & Wang, D. (2017). Scalable blockchain-based smart contract execution. *Proceedings of the 23rd International Conference on Parallel and Distributed Systems (ICPADS)*, 352–359.

Garay, J., Kiayias, A., & Leonardos, N. (2015). The Bitcoin Backbone Protocol: Analysis and applications. *Proceedings of the International Conference on Theory and Applications of Cryptographic Techniques*, 281–310. Springer.

Gervais, A., Karame, G. O., Capkun, V., & Capkun, S. (2016). On the security and performance of proof-of-work blockchains. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 1–16.

Gu, J., Sun, B., Du, X., Wang, J., Zhuang, Y., & Wang, Z. (2018). Consortium blockchain-based malware detection in mobile devices. *IEEE Access, 6*, 12118–12128.

Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security, 78*, 126–142. https://doi.org/10.1016/j.cose.2018.06.004

Hammudoglu, J., Garcia, S., Zhang, J., & Kim, S. (2017). Portable trust: Biometric-based authentication and blockchain storage for self-sovereign identity systems. *arXiv preprint arXiv:1706.03744*.

Hardjono, T., & Smith, N. (2016). Cloud-based commissioning of constrained devices using permissioned blockchains. *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security (IoTPTS '16)*, 29–36.

Hardwick, F. S., Akram, R. N., & Markantonakis, K. (2018). Fair and transparent blockchain-based tendering framework: A step towards open governance. *arXiv preprint arXiv:1805.05844*. https://arxiv.org/abs/1805.05844

Hastad, J., & Naslund, M. N. (2001). Practical construction and analysis of pseudo-randomness primitives. *Proceedings of the International Conference on Theory and Application of Cryptology and Information Security*, 442–459.

Hou, H. (2017). The application of blockchain technology in E-government in China. *Proceedings of the 26th International*

Conference on Computer Communications and Networks (ICCCN), 1–4. IEEE.

Huang, J., Xie, W., Liu, J., Xu, Y., Zhang, Y., & Zhu, Y. (2019). Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. *IEEE Transactions on Industrial Informatics, 15*(6), 3680–3689.

Huh, S., Cho, S., & Kim, S. (2017). Managing IoT devices using a blockchain platform. *Proceedings of the 19th International Conference on Advanced Communication Technology (ICACT)*, 464–467.

Hui, K. Y., Lui, J. C. S., & Yau, D. K. (2006). Small-world overlay P2P networks: Construction, management and handling of dynamic flash crowds. *Computer Networks, 50*(15), 2727–2746.

Imbault, F., Swiatek, M., de Beaufort, R., & Plana, R. (2017). The green blockchain: Managing decentralized energy production and consumption. *Proceedings of the 17th IEEE International Conference on Environmental and Electrical Engineering (EEEIC)*, 1–5. http://ieeexplore.ieee.org/document/7977613

Jiang, Y., Wang, C., Wang, Y., & Gao, L. (2019). A cross-chain solution to integrating multiple blockchains for IoT data management. *Sensors, 19*(9), 2042.

Khari, M., Garg, S., Kumar, A., & Srivastava, S. (2020). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50*(1), 73–80.

Kim, G., Park, J., & Ryou, J. (2018). A study on utilization of blockchain for electricity trading in microgrid. *Proceedings of the International Conference on Big Data and Smart Computing (BigComp)*, 743–746. IEEE.

Kim, Y., Sim, M., Moon, I., & Javidi, B. (2019). Secure random phase key exchange schemes for image cryptography. *IEEE Internet of Things Journal, 6*(6), 10855–10861.

Kishigami, J., Fujimura, S., Watanabe, H., Nakadaira, A., & Oishi, K. (2015). The blockchain-based digital content distribution system. *Proceedings of the IEEE International Conference on Big Data and Cloud Computing (BDCloud)*, 187–190.

La Porta, R., Lopez-de-Silanes, F., & Shleifer, A. (2008). The economic consequences of legal origins. *Journal of Economic Literature, 46*(2), 285–332.

Lesavre, L., Varin, P., Mell, P., Davidson, M., & Shook, J. (2019). A taxonomic approach to understanding emerging blockchain identity management systems. *arXiv preprint arXiv:1908.00929.*

Li, C., Sun, X., & Zhang, Z. (2021). Effective methods and performance analysis of a satellite network security mechanism based on blockchain technology. *IEEE Access, 9*, 113558–113565.

Li, H., & Han, D. (2019). EduRSS: A blockchain-based educational records secure storage and sharing scheme. *IEEE Access, 7*, 179273–179289.

Lin, C., Shen, C., Wang, J., Li, M., & Yang, J. (2018). A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems. *IEEE Access, 6*, 28203–28212.

Liu, G., Fan, N., Wu, C. Q., & Zou, X. (2022). On a blockchain-based security scheme for defense against malicious nodes in vehicular ad-hoc networks. *Sensors, 22*(14), 5361. https://doi.org/10.3390/s22145361

Liu, Y., Lu, Q., Chen, S., Qu, Q., O'Connor, H., Choo, K. K. R., & Zhang, H. (2020). Capability-based IoT access control using blockchain. *Digital Communications and Networks, 7*, 463–469. https://doi.org/10.1016/j.dcan.2020.07.004

Lu, P. J., Yeh, L.-Y., & Huang, J.-L. (2018). A privacy-preserving cross-organizational authentication/authorization/accounting system using blockchain technology. In *2018 IEEE International Conference on Communications (ICC)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICC.2018.8422836

Lu, Y., & Zheng, X. (2018). Block chain-based double auction design. In *Proceedings of the American Conference on Information Systems (AMCIS)*.

Lu, Y. (2019). Artificial intelligence: A survey on evolution, models, applications and future trends. *Journal of Management Analysis, 6*(1), 1–29.

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. In *Proceedings of the 23rd ACM SIGSAC Conference on Computer and Communications Security* (pp. 254–269). https://doi.org/10.1145/2976749.2978309

Maitra, S., Yanambaka, V. P., Abdelgawad, A., Puthal, D., & Yelamarthi, K. (2020). Proof-of-authentication consensus algorithm: Blockchain-based IoT implementation. In *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)* (pp. 2020–2021). IEEE. https://doi.org/10.1109/WF-IoT48130.2020.9221280

Mustafa, I., et al. (2020). A lightweight post-quantum lattice-based RSA for secure communications. *IEEE Access, 8*, 99273–99285. https://doi.org/10.1109/ACCESS.2020.2997325

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Applied Science*. https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

Neeraj, & Singhrova, A. (2022). Taxonomy for IoT authentication using blockchain. *Journal of Optoelectronics Laser, 41*(6), 452–456. https://www.gdzjg.org/index.php/JOL/article/view/545

Neeraj, & Singhrova, A. (2023a). Adaptive attribute-based encryption on blockchain with enhanced authentication mechanism. *Rivista Italiana di Filosofia Analitica Junior, 14*(1), 583–584. https://rifanalitica.it

Neeraj, & Singhrova, A. (2023b). Quantum key distribution-based techniques in IoT. *The Scientific Temper, 14*(3), 1008–1013. https://scientifictemper.com/ DOI: 10.58414/SCIENTIFICTEMPER.2023.14.3.69

Newman, M. E. J. (2001). Scientific collaboration networks. I. Network construction and fundamental results. *Physical Review E, 62*, 016131. https://doi.org/10.1103/PhysRevE.64.016131

Ngubo, C., Dohler, M., & Mcburney, P. (2019). Blockchain, IoT and sidechains. *Lecture Notes in Engineering and Computer Science, 2239*, 136–140.

Oh, S., Park, S., & Kim, H. (2020). Patterned cipher block for low-latency secure communication. *IEEE Access, 8*, 44632–44642. https://doi.org/10.1109/ACCESS.2020.2978295

Orman, H. (2018). Blockchain: The emperor's new PKI? *IEEE Internet Computing, 22*(2), 23–28. https://doi.org/10.1109/MIC.2018.022021651

Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2016). FairAccess: A new blockchain-based access control framework for the Internet of Things. *Security and Communication Networks, 9*, 5943–5964. https://doi.org/10.1002/sec.1748

Panait, A. E., Olimid, R. F., & Stefanescu, A. (2020). Identity management on blockchain—privacy and security aspects. *arXiv preprint* arXiv:2004.13107. https://arxiv.org/abs/2004.13107

Pradeepkumar, D. S., et al. (2018). Evaluating complexity and digitizability of regulations and contracts for a blockchain application design. In *IEEE/ACM International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)* (pp. 25–29). https://doi.org/10.1109/WETSEB.2018.00010

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The blockchain as a decentralized security framework. *IEEE Consumer Electronics Magazine, 7*(2), 18–21. https://doi.org/10.1109/MCE.2018.2797039

Qu, C., Tao, M., & Yuan, R. (2018). A hypergraph-based blockchain model and application in internet of things-enabled smart homes. *Sensors, 18*(9), 2784. https://doi.org/10.3390/s18092784

Saghiri, A. M., et al. (2018). A framework for cognitive internet of things based on blockchain. In *4th International Conference on Web Research (ICWR)* (pp. 138–143). https://doi.org/10.1109/ICWR.2018.8355219

Şahan, Ş., Ekici, A. F., & Bahtiyar, Ş. (2019). A multi-factor authentication framework for secure access to blockchain. In *2019 5th International Conference on Computer and Technology Applications* (pp. 160–164). https://doi.org/10.1145/3323933.3323939

Sanchez-Reillo, R., Ortega-Fernandez, I., Ponce-Hernandez, W., & Quiros-Sandoval, H. C. (2019). How to implement EU data protection regulation for R&D in biometrics. *Computer Standards & Interfaces, 61*, 89–96. https://doi.org/10.1016/j.csi.2018.03.010

Saraf, C., & Sabadra, S. (2018). Blockchain platforms: A compendium. In *Proceedings of the International Conference on Innovative Research and Development (ICIRD)* (pp. 1–6).

Shankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017). Survey of consensus protocols on blockchain applications. In *4th International Conference on Advances in Computing and Communications Systems (ICACCS)* (pp. 1–5). https://doi.org/10.1109/ICACCS.2017.8014583

Sharma, T., Satija, S., & Bhushan, B. (2019). Unifying blockchain and IoT: Security requirements, challenges, applications and future trends. In *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)* (pp. 341–346). IEEE. https://doi.org/10.1109/ICCCIS48478.2019.8974529

Shrivastava, P., Alam, B., & Alam, M. (2022). Security enhancement using blockchain-based modified infinite chaotic elliptic cryptography in cloud. *Cluster Computing*. https://doi.org/10.1007/s10586-022-03777-y

Siddarth, D., Ivliev, S., Siri, S., & Berman, P. (2020). Who watches the watchmen? A review of subjective approaches for Sybil-resistance in proof of personhood protocols. *Frontiers in Blockchain, 3*, Article 590171. https://doi.org/10.3389/fbloc.2020.590171

Singh, K. K., & Jha, V. K. (2022). Security enhancement of the cloud paradigm using a novel optimized crypto mechanism. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-022-13960-3

Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed IoT network. *IEEE Access, 9*, 13938–13959. https://doi.org/10.1109/ACCESS.2021.3051281

Tanaka, K., Nagakubo, K., & Abe, R. (2017). Blockchain-based electricity trading with digital grid router. In *International Conference on Consumer Electronics-Taiwan (ICCE-TW)* (pp. 201–202). IEEE. https://doi.org/10.1109/ICCE-China.2017.7991086

Truong, N. B., Sun, K., Lee, G. M., & Guo, Y. (2019). GDPR-compliant personal data management: A blockchain-based solution. *IEEE Transactions on Information Forensics and Security, 15*, 1746–1761. https://doi.org/10.1109/TIFS.2019.2948287

Vangala, A., Sutrala, A. K., Das, A. K., & Jo, M. (2021). Smart contract-based blockchain-envisioned authentication scheme for smart farming. *IEEE Internet of Things Journal, 8*(13), 10792–10806. https://doi.org/10.1109/JIOT.2021.3056372

Van Hamme, T., Rimmer, V., Preuveneers, D., Joosen, W., Mustafa, A. M., Abidin, A., & ArgonesRua, E. (2017). Frictionless authentication systems: Emerging trends, research challenges and opportunities. *IEEE Security & Privacy, 15*(3), 76–84. https://doi.org/10.1109/MSP.2017.55

Vignesh, R., & Prasad, K. M. (2022). Blockchain-based security enhancement mechanism for employee performance assessment system. *Concurrency and Computation: Practice and Experience*. https://doi.org/10.1002/cpe.7318

Vukolić, M. (2015). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *Open Research Problems in Network Security (iNetSec)* (pp. 112–125). Springer. http://www.vukolic.com/iNetSec_2015.pdf

Wahab, O. F., Khalaf, A. A., Hussein, A. I., & Hamed, H. F. (2021). Hiding data using efficient combination of RSA cryptography and compression steganography techniques. *IEEE Access, 9*, 31805–31815. https://doi.org/10.1109/ACCESS.2021.3059857

Wang, S., et al. (2019). Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. https://doi.org/10.1109/TSMC.2019.2895123

Wang, W., et al. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access, 7*, 22328–22370. https://doi.org/10.1109/ACCESS.2019.2896108

Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of 'small-world' networks. *Nature, 393*(6684), 440–442. https://doi.org/10.1038/30918

Wood, G. (2014). Ethereum: A secure decentralized generalized transaction ledger. *Ethereum Project Yellow Paper*. https://pdfs.semanticscholar.org/ac15/ea808ef3b17ad754f91d3a00fedc8f96b929.pdf

Xu, C., et al. (2019). Making big data open in edges: A resource-efficient blockchain-based approach. *IEEE Transactions on Parallel and Distributed Systems, 30*(4), 870–882. https://doi.org/10.1109/TPDS.2018.2865676

Yang, Z., et al. (2018). Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2018.2884101

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *IEEE International Congress on Big Data (BigDataCongress)* (pp. 557–564). https://doi.org/10.1109/BigDataCongress.2017.85

Zhou, Z., Li, L., Guo, S., Li, Z., & University, I. E. (2018). Biometric and password two-factor cross-domain authentication scheme based on blockchain technology. *Journal of Computer Applications*. *(citation details incomplete; DOI or volume/issue required)*

Zulkifl, Z., et al. (2022). FBASHI: Fuzzy and blockchain-based adaptive security for healthcare IoTs. *IEEE Access, 10*, 15644–15656. https://doi.org/10.1109/ACCESS.2022.3148545