Chapter 8
Decentralized Identity Management Using Blockchain Technology: Challenges and Solutions

Ahmed Mateen Buttar, Muhammad Anwar Shahid, Muhammad Nouman Arshad, and Muhammad Azeem Akbar

1 Introduction

Blockchain-powered decentralized identity management provides consumers with authority over their personal data and increases online company privacy, security, and interoperability. Traditional identity systems are administered by governments or enterprises. Blockchain, on the other hand, empowers users in its decentralized identity management. Blockchain records transactions and data across computers. Cryptographically linking each transaction, or "block," creates an immutable chain of information. Decentralized and tamper-resistant blockchain is ideal for secure and transparent identity management [1].

Decentralized identity management systems create and manage digital IDs by using cryptography. Blockchain secures their identities. Selectively sharing names, ages, and addresses with numerous service providers avoids providing unnecessary personal information. Decentralized identity management leads to self-sovereignty. Individuals can manage their identities without intermediaries. Controlling data access prevents identity theft, fraud, and misuse. Interoperability improves with decentralized identity management. The Decentralized Identity Foundation (DIF) and World Wide Web Consortium (W3C) verifiable credentials (VCs) make verifying and sharing digital identities across platforms, apps, and organizations easy [2].

Blockchain secures identity management. Cryptography secures blockchain transactions and identities. Blockchain's decentralized nature makes it more secure.

A. M. Buttar (✉) · M. N. Arshad
Department of Computer Science, University of Agriculture Faisalabad, Faisalabad, Pakistan

M. A. Shahid
Univeristy of Windsor, Windsor, ON, Canada

M. A. Akbar
Department of Software Engineering, LUT University, Lappeenranta, Finland

S. M. Idrees, M. Nowostawski (eds.), *Blockchain Transformations*, Signals and Communication Technology, https://doi.org/10.1007/978-3-031-49593-9_8

Blockchain platforms are developing decentralized identity management. Sovrin, uPort, and Microsoft's ION leverage blockchain develop open, interoperable, and privacy-preserving identity systems for computer-to-computer transactions.

1.1 Background and Motivation

Traditional centralized identification systems' flaws prompted blockchain-based decentralized identity management. Centralized identification systems compel users to share sensitive personal data with several service providers, increasing the risk of data breaches and identity theft. Hackers target centralized databases, which can harm individuals. Decentralized identity management enables people to own their data and share only what they need to.

Less user control: Traditional identification systems govern identities centrally. Unauthorized data collection, storage, and use occur frequently. Decentralized identity management empowers individuals. Users can choose who sees what and why. Centralized identity schemes are also incompatible. Each service provider or organization may have its own identity databases and verification methods, causing duplications in data collection and poor user experiences. Decentralized identity management using open standards and protocols lets people use verifiable credentials across platforms and services, increasing interoperability [5].

Identity fragmentation: People have multiple digital identities across platforms and services. Password management is challenging. Decentralized identity management solves this identity fragmentation by providing a single, portable, self-sovereign identity that can be used across apps and services.

Credibility: Identity management demands trust. Traditional systems verify IDs centrally. These authorities may be corrupt or make mistakes. Decentralized identity management verifies credentials by using blockchain's immutability and transparency. Cryptographically linking IDs to the blockchain prevents forgery.

1.2 Objectives and Scope

Blockchain-based decentralized identity management seeks user control. Digital identities must be controlled to create, manage, and cancel identities. They can also select who can access their personal data and how. Decentralized identity management emphasizes privacy and security. Personal data should be protected, and cryptography and blockchain's immutability safeguard identities and attributes against manipulation and fraud. The interoperability of systems, services, and organizations are essential. Decentralized identity management should streamline the exchange and verification of digital identities and credentials, improving user experiences. This goal requires protocol and format standardization.

Digital identities must be trusted. Blockchain's immutability should offer a tamper-proof way to verify identification credentials. Cryptographic and consensus algorithms maintain system confidence. Decentralized identity management solutions must be usable and adopted by users. For this, simple and easy identity management is needed. Developers, stakeholders, and service providers must work together to create user-friendly apps and interfaces. The decentralized identity management system must be able to handle multiple users and transactions. Digital identities and transactions should keep the system efficient and responsive. Decentralized identity management must comply with regulations and laws. The system must preserve data and privacy. Identity issues and legal recourse should be addressed [6].

1.3 Overview of Blockchain Technology

Blockchain-based decentralized identity management is secure, transparent, and user centric. Blockchain identity management boasts many features.

Distributed ledgers: Blockchain stores identity-related data in a decentralized, tamper-resistant ledger. Each identity-related transaction, like generating, modifying, or canceling an identity, is stored in a block and connected to the previous block, producing an immutable data chain.

Self-sovereign identities: Blockchain enables people to control their digital identities. Public–private key pairs create and manage blockchain identities, thus eliminating centralized identity validation and administration. Blockchain-identifying records are unchangeable and transparent. This secures and verifies the identification data. Blockchain transparency allows people and businesses to verify identity credentials without needing intermediaries [7].

Digital credentials: Blockchain can issue and validate digital credentials. Parties who rely on blockchain can verify issuers' public key–signed credentials. Verifying identification permits selective sharing. Standards enable decentralized identity management interoperability. DIF and W3C open standards like decentralized identifiers (DIDs) and verifiable credentials provide blockchain-based identification system compatibility and interoperability.

Privacy-preserving features: With decentralized identity management, someone can choose to share the required traits or credentials without revealing their whole identity. Attribute-based access control safeguards personal data. Blockchain security promotes decentralized identity management. Blockchain encryption safeguards IDs. Finally, blockchain's decentralized nature resists attacks.

Chapter Objectives:

Examine blockchain-based decentralized identity management difficulties.

Help blockchain-based identity systems to scale.

Present zero-knowledge proofs and confidential transactions to address privacy and security issues in decentralized identity management.

Discuss decentralized identification system interoperability issues and provide solutions for data flow between platforms.

Analyze regulatory compliance needs and suggest ways to comply with applicable laws.

Investigate user-adoption issues and propose user-centric interfaces and educational campaigns to promote decentralized identity solutions.

Showcase successful decentralized identity management installations and case studies.

Discuss blockchain-based decentralized identity management research and development.

Chapter Organization

This chapter overviews blockchain-based decentralized identity management and the benefits associated with it. After that, a discussion of the challenges posed by distributed identity management follows. Scalability, privacy and security, interoperability, regulatory compliance, and user adoption each has its own section in this chapter. This chapter provides solutions and strategies, and it explores the specific difficulties in and complexity of each challenge. The solutions include cross-chain communication, off-chain storage, layer 2 protocols, zero-knowledge proofs, governance frameworks, user-centric interfaces, and education programs. Case studies and actual implementations from the real world provide the reader with useful insights throughout the chapter. The chapter comes to a close with research and development on a type of decentralized identity management that is based on blockchain technology, as shown in Fig. 8.1 [8].

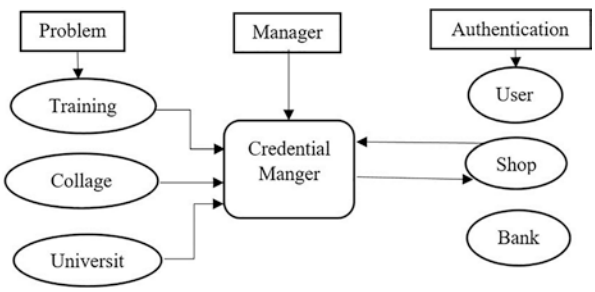

Fig. 8.1 Credential verification guide using dock certs and dock wallets

2 Fundamentals of Decentralized Identity Management

Decentralized identity management in blockchain technology has the following core concepts and components.

Decentralization: Identity management is decentralized. Instead of having a central authority control users' identities, the users control them. Users create, manage, and share their blockchain-stored digital identities. Decentralized identity management uses blockchain technology. It is a transparent, tamper-proof distributed ledger. By cryptographically linking blocks, blockchain creates an unchangeable chain of identifying data. Decentralized identity management requires self-sovereign identification. It lets people manage and confirm their identities without central authorities. Users can also create, amend, and revoke IDs. Decentralized identity management requires cryptography. It secures blockchain identification data. Public-key cryptography, digital signatures, and hash functions protect these identity data. Decentralized identity management uses digital identity traits to represent personal information. Names, ages, addresses, credentials, and other information may be included. Users can selectively share attributes and limit whom to share them with [9].

Verifiable credentials: Verifiable credentials are blockchain-issued, stored, and verified identification credentials. Reliant parties can verify them by using the issuer's public keys because they are cryptographically signed. Credentials verify identification information.

Decentralized identifiers (DIDs): Blockchain users are allocated unique identifiers. DIDs enable decentralized identity reference and interaction. They facilitate interoperability and both identity resolution and identity discovery across platforms and services.

Interoperability standards: Blockchain-based identification systems must be interoperable for decentralized identity management to work. DIDs and verifiable credentials, established by the Decentralized Identity Foundation (DIF) and the World Wide Web Consortium (W3C), enable interoperability and compatibility across platforms.

2.1 Concepts and Terminology

Blockchain-based decentralized identity management is undergirded by several concepts and terminologies.

Digital identity: A digital identity marks a person's online presence. Their name, age, address, biometric data, and other information may be included.

Decentralization: Power is distributed. Decentralized identity management lets users control their digital identities without intermediaries.

Self-sovereign identity: People can control their digital identities. Such an identity allows identity management, regulation, and authentication without third parties.

Blockchain: Blockchain stores data across computers. Cryptography secures immutable and transparent data. Blockchain underpins decentralized identity management.

Cryptography: Algorithms protect data. Decentralized identity management protects data via cryptography, public-key cryptography, digital signatures, and hash functions. Digital IDs and qualifications are available from trusted partners. Reliant parties can validate them because they are cryptographically signed by the issuer. Credentials allow selective identity disclosure.

DIDs: DIDs are unique blockchain identifiers for individuals, entities, and items. They provide decentralized identification and engagement. They aid cross-platform identity resolution and discovery. Providers issue and manage these digital IDs. Decentralized identity management utilizes people, organizations, or machines as identity providers. Digital identities can also be authenticated. Identity wallets manage digital identities and credentials. These wallets protect private keys, manage verifiable credentials, and selectively share identity information with service providers [10].

Interoperability standards: Specifications and protocols allow distributed identity management systems to communicate. Interoperability standards include DIDs, VCs, and W3C DID and VC standards. Blockchain-based decentralized identity management is based on and requires these concepts and terminology. They start user-centric, safe, and privacy-enhancing digital identity management.

2.2 Self-Sovereign Identity

Blockchain-based identity management involves self-identification. It lets people control, regulate, and authenticate their digital identities without centralized authorities. Self-sovereign identity requires user control.

User control: Self-sovereign identification allows for digital identity management. IDs can be created, edited, and revoked. Users determine identification, data access, and conditions. Users no longer need centralized identity validation or administration. Blockchain supports self-sovereign identity. Blockchain's distributed ledger protects identification data. The blockchain lets several parties verify and validate identifying information. Cryptography promotes self-sovereign identification. Public-key cryptography helps users create and control cryptographic key pairs: private keys for identity management and public keys for verification. Digitally signing and encrypting identifiers guarantees privacy, integrity, and authentication [11].

Self-sovereignty demands verifiable credentials. Trusted organizations issue digitally signed credentials that can be verified. Public keys enable the selective

transmission of these credentials without revealing personal information. Self-sovereign identity systems use interoperability standards. DIDs and verifiable credentials allow cross-platform identity generation, exchange, and verification. Interoperability helps digital ecosystem elements verify identities. Self-sovereign identity applications, services, and domains to be portable. Portability eliminates the need for different accounts and credentials. Self-sovereign identification shifts confidence from authorities to users. Cryptography and blockchain transparency build trust. Cryptographic evidence, decentralized ledger integrity, and identity management build confidence. Decentralized identity management equips people with self-sovereign identification. It supports digital interoperability and privacy [12].

2.3 Decentralized Identifiers (DIDs) and Verifiable Credentials

Blockchain-based decentralized identity management requires DIDs and verifiable credentials. Digital identities and credentials can be created, exchanged, and verified in a decentralized way.

Decentralized IDs

- DIDs are assigned by decentralized identification systems. They are globally unique and platform resolvable.
- DIDs allow identity referencing and interaction without central authorities. Cryptographic key pairs and Uniform Resource Identifiers (URIs) can control and authenticate Decentralized Identifiers (DIDs).
- Blockchains and other decentralized systems can store and resolve DIDs, making identity management tamper-proof and available worldwide.

Trusted organizations issue verifiable credentials. They reveal selective identification without revealing personal information. Issuers cryptographically sign verifiable credentials. The issuer's public keys enable easy verification.

- Independently verifiable credentials include names, ages, educational qualifications, and membership statuses.
- Verifiable credentials allow users to verify, authenticate, and access services.

Verifiable credentials safeguard privacy in that users pick which credentials to reveal, when, and with whom.

DIDs and verifiable credentials support blockchain-based identity management. DIDs provide unique, decentralized DID identification and interaction, whereas verifiable credentials issue, exchange, and verify reliable, tamper-proof digital evidence of identity attributes or qualifications. These technologies provide user-centric blockchain identification, privacy, and interoperability [13].

2.4 Benefits and Use Cases

Blockchain-based decentralized identity management offers various benefits and uses. Decentralized identity management empowers and protects users. Maintaining, regulating, and selectively publishing identification attributes improves privacy and reduces centralized power.

Trust and safety: Blockchain's immutability and cryptography secure identification data. Tamper-resistant blockchains safeguard identities from fraud and data breaches. Decentralized identity management also improves platform/service compatibility. Overall, DIDs and verifiable credentials make digital life easier by helping people to recognize and trust one another.

Saving money: Decentralized identity management removes multiple service logins. Portable identities reduce administrative hassle. Decentralized identity management also lowers identity authentication costs.

2.5 Decentralized Identity Management

Digital identity verification: Decentralized identity management streamlines client onboarding, online service access, and knowing your customer (KYC). Verifiable credentials also streamline identification verification, and decentralized identity management facilitates cross-border verification. Securely communicating valid credentials with foreign authorities accelerates cross-border transactions and minimizes superfluous identification verification. Decentralized identity management lets people own their data. Allowing used to share only certain traits limits service providers' access to their personal data. Data breaches and illegal access are thereby reduced. Blockchain-based decentralized identity management can handle supply chains and product authenticity. Verifiable credentials prevent product counterfeiting and ensure supply-chain transparency. Decentralized identity management secures and exchanges patient data, improving healthcare systems. Sharing medical records with providers improves data privacy, interoperability, and care coordination. Blockchain-based identity management secures digital voting. It prevents voter fraud by verifying identities, as shown in Fig. 8.2 [14].

3 Challenges in Implementing Decentralized Identity

Blockchain-based decentralized identity management has many benefits but also many drawbacks.

Scalability: Concerns about scalability frequently arise with public blockchains because of the volume of transactions and identity information that they process.

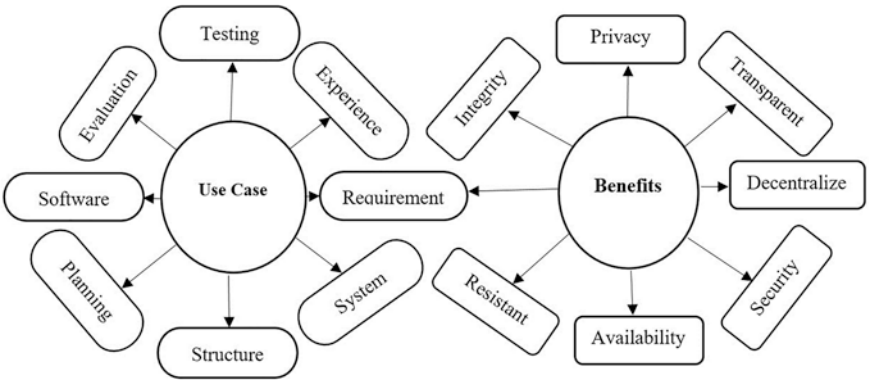

Fig. 8.2 Key features of and use cases for a blockchain

In decentralized identity management, which stores and manages identity attributes, scalability is crucial for efficient and quick verification and authentication. Scalability also stores and manages identity attributes.

Privacy and security: Blockchain technology ensures security through immutability and decentralized consensus; however, maintaining users' anonymity is challenging because of the nature of the platform. A compromise must be struck between protecting one's identity and maintaining transparency. It is challenging to protect the privacy of data and implement privacy-enhancing techniques such as zero-knowledge proofs without compromising the integrity of the system or its credibility [15].

Interoperability: Interoperability is a challenge because it is difficult to integrate blockchain platforms and identity systems. Fluidly sharing data between identity providers, reliant parties, and verification services is an essential component of decentralized identity management. Standards and procedures for interoperability are required in order to transfer identify attributes from one system to another.

Regulatory compliance: There may be problems with regulatory compliance if decentralized identity management is used. The laws governing identification, data protection, and privacy vary widely from country to country and from jurisdiction to jurisdiction. Significant thought and regulatory cooperation are required in order to bring decentralized identity solutions into compliance with these standards while also preserving appropriate governance and liability frameworks [16].

User adoption: It is difficult to change people's mentalities and actions so that they will utilize decentralized identification systems. Users need to be informed about self-sovereign identities, secure digital identity management, and the importance of placing their trust in the underlying technology and procedures. Increasing user adoption requires education, sound guidance, and interfaces that are easy to use.

Infrastructure and integration: Decentralized identity management requires DID registries, verifiable credential issuers, and reliant party systems. This type of

management also requires infrastructure and integration. The integration of these components with identification systems and apps is a complex process that needs the coordination of stakeholder interests. Both integration and compatibility are challenging to achieve [17].

Governance and standards: There is no governance model for and there are no standards in place for decentralized identity management. Ongoing challenges include developing governance frameworks that are compatible with the decentralized nature of blockchain identity management and developing agreed-on standards for interoperability, data formats, and verification procedures.

User experiences: User-friendliness drives adoption. Designing intuitive user interfaces and integrating technologies are difficult. Cryptographic key management and decentralized technology might hinder usability. Decentralized identity management promotes privacy but raises concern about data protection and General Data Protection Regulation (GDPR) compliance. Cross-border data flows and the blockchain storage of sensitive personal data make privacy and regulation challenging to reconcile. Integration and acceptance necessitate decentralized identity management solution interoperability. Common standards, protocols, and governance frameworks for identity interoperability across platforms and services are complex and require stakeholder consensus [18].

Traditional centralized identification systems allow identity recovery and revocation. Decentralized identity management, where users have full control over their identities, impedes identity recovery and revocation. Decentralized identity management laws are changing. Digital identity ownership, liability, dispute resolution, and cross-jurisdictional difficulties must be solved to legalize and promote decentralized identity solutions. Trusting decentralized identity management systems is hard. The goal is to encourage individuals, organisations, and service providers to use identity management solutions for the Internet of Things (IoT), as shown in Table 8.1 [19].

Table 8.1 Blockchain for IoT applications and features

Blockchain-based IoT descriptions					
Sr No.	Properties	Technology	Application	Project	Solution
01	Decentralization	Distributed ledger	Smart care	uPort	MyData
02	Immutability	Smart contracts	Smart grid	Idensys	Waypoint
03	Transparency	Cryptocurrency	Smart city	Tradle	Bloom
04	Latency	Consensus Protocols	Smart finance	Idensys	UniqueId

4 Management

4.1 Scalability

Blockchain-based decentralized identity management needs scalability. Scalability difficulties in public blockchain networks may make identity and transaction management challenging. Scaling involves the implementation of decentralized Identity management (DIM), a process aimed at decentralizing identity management. Blockchain transactions are constrained by time, allowing only one transaction per second. Increased identities and transactions may shut down the network and raise transaction fees. Scaling network throughput improves identity management and allows the network to handle more users [20].

Possible answers: State channels or sidechains can offload transaction processing from the main blockchain, increasing network capacity.

Sharding: Shards process independently transactions on the blockchain network. Sharding parallelizes transactions, scaling these networks.

Storage: As identities and credentials grow, so does the need for blockchain storage. This impacts storage costs and availability.

Off-chain storage: Storing identity-related data off chain in decentralized storage networks like the Interplanetary File System (IPFS) reduces blockchain storage while ensuring data availability and integrity.

Data compression and optimization: Compressing and optimizing blockchain data storage reduces storage without compromising anyone's identity. Creating, maintaining, and confirming IDs require significant computational resources. As identities and operations grow, blockchain computations can overwhelm those resources.

- Identity-related techniques and data structures reduce computing overhead.
- TEEs help offload computation, which lessens the blockchain-processing burden.

Interoperability: Decentralized identity management systems must be interoperable, although scaling may be problematic. Identity and credential communication across blockchain networks and services requires scalable and efficient cross-chain communication protocols. DIDs, VCs, and W3C DID and VC standards can help decentralized identity systems integrate and interoperate. Efficient cross-chain communication techniques for secure and scalable identification data transmission can improve interoperability without sacrificing scalability.

4.2 Privacy and Security

Blockchain-based identity management needs privacy and security. Blockchain is secure, but decentralized identity management privacy and security must still be considered.

Selective disclosure promotes privacy: Verifiable credentials allow people to exchange only transactional information and to do so without revealing personal information. Minimal disclosure protects privacy. Blockchain-based decentralized identity management allows anonymity, and even pseudonymity protects private information.

Off-chain storage: IPFS or encrypted storage can protect private data. This safeguards sensitive identifying data.

Zero-knowledge proofs: These proofs can verify a claim without needing data. Cryptographic methods authenticate identification without revealing attribute values.

Safety issues: Decentralized identity management requires strong cryptography. Public-key cryptography authenticates identities. Identification data are encrypted and signed. Key management safeguards decentralized identities. Users must safeguard their identity-controlling private keys. Hardware wallets, multifactor authentication, and secure key storage help to mitigate key risks. Blockchain's immutability safeguards identity-related transactions and data. Changes to blockchain identity information require authority [21].

Consensus mechanisms: The blockchain network's consensus process should be secure to avoid identity data modifications or attacks. Proof of Work (PoW) and Proof of Stake (PoS) consensus algorithms secure blockchain networks. Decentralized identity management requires blockchain network security. Identity data require network-level encryption, safe node connectivity, and Distributed Denial of Service (DDoS) avoidance. Blockchain allows identity management audits. Tracking and validating identification data transactions and modifications improves accountability [22].

4.3 Interoperability

Blockchain-based identity management requires compatibility. Decentralized identity systems, platforms, and services easily share and analyze identity-related data, credentials, and interactions. Interoperability is essential for a connected, efficient ecosystem that trusts identities across domains. Decentralized identity management interoperability requires specific protocols, technologies, and methods.

Standard protocols: Interoperability requires standardization. W3C standards for decentralized identity management include DIDs, VCs, and DID authentication. Standards help systems to read identity-related data uniformly. Cross-chain communication between blockchain networks or decentralized identity platforms promotes interoperability. ILP and Polkadot exchange identity-related data and transactions across chains for smooth interoperability [23].

ID bridge technologies: Identity bridges share information across identity systems. Bridges that transfer credentials and attestations promote network interoperability. Chainlink, Sovrin Bridge, and Aries Interop bridge identities. Systems must

exchange identification data and terminology for semantic interoperability. JSON-LD standards, for example, provide semantic data interpretation and allow for the exchange of identity features and credentials. Interoperability requires blockchain developers, identity management experts, standards groups, and regulators. Governance mechanisms and industry consortia regulate interoperability standards. Plug-and-play solutions for decentralized identification systems promote interoperability. These solutions should follow common standards and offer interoperability out of the box, allowing enterprises and service providers to seamlessly join and engage with decentralized identity networks [24].

User-centric methods: User identities should be interoperable across platforms and services. Users should manage, control, and selectively disclose their identity attributes regardless of the decentralized identification system. Interoperability should comply with regulations like GDPR. Interoperable data management technologies are needed to maintain user confidence and to comply with privacy rules.

4.4 User Adoption

Users drive blockchain-based decentralized identity management. Adoption limits the benefits of decentralized identities.

Usability/user experiences: Easy user uptake is needed. Decentralized identity management systems should include simple setup, onboarding, and use instructions. Reducing technical complexity and integrating user activities improve usability.

Education and awareness: Users must grasp the value of decentralized identities. Few people understand self-sovereign identification and decentralized identity management. Real-world use cases and success stories may convince skeptics and encourage adoption. Benefits and incentives may boost the adoption of decentralized identity solutions. These incentives reduce transaction costs and improve privacy, security, service access, and identity verification. Demonstrating how decentralized identity management simplifies and protects users can increase adoption. User adoption necessitates collaboration between service providers and businesses. Decentralized identity systems in online marketplaces, social networks, and banks benefit users. If decentralized identification enhances user experiences and enables new functions, service providers may adopt and promote it [25].

Confidence and security: Decentralized identity management solutions require user confidence. Security measures, user control, data protection, and transparency about technology and protocols increase user trust. Third-party audits, certifications, and privacy compliance ensure system security and compliance. User adoption requires integration with existing identity systems and infrastructure. Single Sign-On (SSO) lets consumers use their digital identities while moving to

decentralized identity management. User adoption requires standardization and industry cooperation. When systems and platforms follow standards, users can more seamlessly connect with multiple services and businesses can integrate decentralized identity solutions. Standardization and industry consortia accelerate the development and implementation of decentralized identity management. User trust demands GDPR compliance. Demonstrating that decentralized identity management solutions respect privacy and rules can enhance user confidence [26].

4.5 Regulatory Compliance

Blockchain-based identity management needs regulation. Decentralized identity systems handle sensitive data, so legal compliance is essential. Regulations on decentralized identity management must protect users from several concerns.

Data security: Many nations have data-privacy legislation. The European Union (EU) created the General Data Protection Regulation (GDPR), which governs data processing and protection. Decentralized identity management solutions must comply with these rules and lawfully handle user data.

Minimizing personal data: Collecting and processing must use the least number of personal data needed for identity management and must minimize data retention.

User consent: Users must be informed and express consent before their personal data are collected and processed. Data-processing objectives must be defined.

Data subject rights: These rights guarantee access to, corrections to, and the deletion of personal data. Data subject requests must be optimized. Decentralized identity management systems may require identity verification and KYC. Financial compliance and healthcare compliance are strict to prevent fraud, money laundering, and identity theft.

Risk-based approach: Transaction and user risks must be identified.

Sector-specific rules: Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) requirements may demand further identification verification; users must understand this and comply.

Jurisdictional compliance: Decentralized identity management companies must follow local laws and regulations. Country-specific rules govern personal data processing and transfer.

Cross-border data transfers: Use data transfer safeguards like Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). when moving personal data across borders.

Data localization needs: Data localization requirements may restrict personal data storage and processing outside particular geographical borders.

Crisis: Identity data must be protected, so responses to security breaches and data breaches must be planned.

Monitor regulatory changes and communicate with regulatory agencies or industry bodies to understand decentralized identity management needs and expectations.

Compliance must be maintained, and updates must be processed. Complex decentralized identity management regulatory compliance is evolving. Legal counsel and regulatory bodies should advise organizations employing such technologies to comply with local legislation [27].

5 Solutions to Address Challenges

Blockchain-based identity management is hard, requiring layer 2 scaling.

Layer 2 scaling: State channels, sidechains, and off-chain technologies increase the number of transactions and decrease blockchain network pressure.

- For parallel transaction processing and scalability, shard the blockchain network.
- Optimized consensus mechanisms such as PoS or dPoS improve performance and scalability.
- For privacy/security issues zero-knowledge proofs can be used for private, data-free verification.
- To ensure encryption and confidentiality, only authorized parties can access sensitive identity data stored on the blockchain or in off-chain storage options.

Hardware wallets, multifactor authentication, and safe storage protect private keys and identities.

Auditable smart contracts: Smart contracts should undergo rigorous security evaluations to find and fix problems.

Interoperability challenges: DIDs, verifiable credentials, and W3C-developed decentralized identity-related standards can be used to overcome interoperability challenges. In this way, interoperability and identity data exchange can be improved [28].

Identity bridge technologies: Interoperable decentralized identity systems and blockchain networks use identity bridge technologies to exchange credentials and attestations.

Industry stakeholders, developers, and standards groups should be encouraged to collaborate and deploy suitable solutions.

User-adoption challenges: To improve user experiences, create simple interfaces and onboarding for decentralized identity management solutions. Simplify setup, and give clear instructions.

Education and awareness: Inform users of decentralized identity management's security, privacy, and other benefits. Promote awareness, education, and use cases to highlight decentralized identity's benefits.

Service providers: Service provides should integrate decentralized identification solutions, and the ways that decentralized identity can benefit service providers and users should be demonstrated to them.

To promote decentralized identity systems, users should be offered lower transaction costs, better privacy, or exclusive access to services.

Compliance issues: Consider GDPR and privacy while designing decentralized identity management solutions. Start development with privacy, data reduction, and user approval.

Collaboration with regulatory bodies and authorities: Understand and comply with decentralized identity management laws and regulations. Decentralize identity regulation frameworks.

5.1 Scalability Solutions

Blockchain identity management needs scalability. Scalability is a problem with many potential solutions.

Layer 2 scaling: Layer 2 scaling features off-chain transaction processing with blockchain security. State channels, sidechains, and off-chain protocols work. Off-chain identity-related transactions improve scalability by recording just the final judgment on the main blockchain.

Sharding: Sharding splits the blockchain network. Each shard independently handles transactions, increasing network throughput. Sharding parallelizes transactions, reducing congestion and improving scalability. Sharding decentralized identity systems allows for more identity-related transactions to be carried out. Consensus procedures also scale blockchains. PoS/dPoS consensus mechanisms have higher throughput and scalability, and these consensus methods can scale decentralized identifying systems and require less processing power than PoW does [29].

Off-chain storage: Storing plenty of identity data on the blockchain can pose scalability concerns. Distributed file systems or decentralized storage networks store identity data off chain. These systems store identity data safely and cheaply.

Batch processing: Batch processing combines identity-related blockchain transactions. This reduces on-chain transactions, improving scalability. Batch records contain multiple identity verifications or credential issuances, reducing latency and transaction throughput by optimizing network architecture. Network partitioning, data compression, and efficient peer-to-peer communication protocols improve decentralized identification system efficiency and scalability. Blockchain protocols must be updated. Ethereum 2.0 scales with shard chains and speedier consensus. Decentralized identity management is subject to upgrades [30].

Continuous R&D: Scalability needs constant innovation. Scalable identity management protocols and solutions should be built with researchers from the decentralized identity community.

5.1.1 Off-Chain Storage

Blockchain identity management uses off-chain storage. Storing massive volumes of identity data on the blockchain is wasteful and limits scalability. Storing identity data off chain is cheaper and more scalable. Off-chain storage systems store data and both secure and verify identity data [31].

Decentralized storage: IPFS and Swarm segment data, distribute them between nodes, and ensure data availability.

- Blockchain-based storage marketplaces include Filecoin and Sia. Renting network storage guarantees data durability and redundancy.
- Amazon S3 and Google Cloud Storage store identification data off chain. Blockchains store cloud data references and cryptographic evidence.
- Off-chain storage helps blockchains scale by reducing the number of on-chain data. Decentralized identification systems can manage more transactions and users.

Cost-effectiveness: Computational and storage requirements make blockchain data storage expensive. Off-chain identity data storage is cheaper.

Flexibility: Off-chain storage solutions offer a variety of data formats, protocols, and access controls. They can save images, videos, and papers for identity data.

Privacy: Off-chain storage options keep personal data off the blockchain. Off-chain data are secure and confidential, while on-chain data are just cryptographic proofs.

Blockchain security: Blockchains secure off-chain data. Merkle trees, digital signatures, and hash pointers enable this link. These methods audit off-chain data by using blockchain data.

Tradeoffs and considerations: Off-chain storage offers affordability, scalability, and tradeoffs. Storage providers safeguard off-chain data. Users should choose only reliable storage networks.

Data availability: Off-chain storage systems need redundancy and availability to prevent data loss and must encrypt data and restrict off-chain data access to only authorized parties.

Synchronization and consistency: Keep blockchain and off-chain identifying data consistent. Decentralized identity management can handle huge identity data with off-chain storage. Off-chain storage saves money, scales decentralized identity systems, and protects privacy [32].

5.1.2 Sharding and Layer 2 Solutions

Sharding and layer 2 enable blockchain-based decentralized identity management.

Sharding: Sharding splits the blockchain network. Each shard performs transactions independently and simultaneously.

Benefits of sharding: Sharding lets multiple shards process transactions simultaneously, increasing network throughput. Decentralized identity systems handle a

greater volume of identity-related transactions compared to centralized alternatives, and sharding optimizes efficiency by distributing transaction loads across multiple shards, reducing network congestion and improving efficiency. This scales with the speed of transaction confirmations.

Shards process transactions individually. Decentralized identification systems scale horizontally.

Layer 2: Layer 2 refers to blockchain-secured off-chain transaction processing. On-chain transactions can be reduced to scale.

Layer 2 decentralized identity management methods: State channels allow off-chain transactions without blockchain recording. Blockchain transactions are private and safe. Identification verification uses state channels. Sidechain identity transactions lighten blockchains, and sidechains are faster and more customizable for decentralized identity systems.

Off-chain protocols: Bitcoin's lightning network offers secure, scalable off-chain transactions. Participants use payment channels to settle off-chain transactions on the main blockchain. Off-chain identity interactions scale. Layer 2 solutions scale decentralized identification systems by off-chaining transactions. These solutions improve identity-related transaction confirmation speeds, reduce costs, and increase scalability. However, sharding and layer 2 have perks and cons. Decentralized identity management systems must be properly planned, implemented, and tested to ensure data confidentiality, integrity, and consistency and to improve scalability [33].

5.2 Privacy Solutions

Blockchain identity management demands secrecy.

Privacy options: Off-chain storage solutions keep sensitive identifiable data off the blockchain. Off-chain encryption provides privacy. On-chain data access and sharing improve privacy.

ZKPs: Zero-knowledge proofs use cryptography to verify a statement without revealing any facts. ZKPs can validate identities without revealing personal information, thanks to decentralized identity management. They enable users show their qualifications without sharing their sensitive data. Differential privacy makes query responses and statistical analysis noisy, making data points hard to identify. Aggregating and analyzing identification data in decentralized identity systems protects user privacy. ZKPs encrypt blockchain or off-chain identification data, and encryption protects data. Symmetric, asymmetric, or homomorphic encryption protects identity data.

Data minimization: Only important identity-related data should be stored *on* the blockchain. Data minimization reduces privacy breaches. Decentralized identity systems should store only those data needed for specific interactions and should keep sensitive data off chain. Privacy-protecting smart contracts can privately

carry out identity-related computations by using state channels or encrypted data structures. Users should control their identity data and carefully choose which credentials to share, with whom, and why. Transparent consent and user-friendly interfaces enable privacy control [34].

Privacy by design: Decentralized ID systems start with privacy. To prioritize privacy throughout the system's lifecycle, privacy-enhancing methods and best practices should be followed and privacy impact evaluations should be carried out.

5.2.1 Zero-Knowledge Proofs

Zero-knowledge proofs (ZKPs) use cryptography to prove a proposition to a verifier without giving any additional information. ZKPs increase blockchain-based identity management privacy and secrecy and have several other uses.

Identity authentication: ZKPs can authenticate an identity without revealing it. Users can prove they're at least 18 years old without disclosing their respective birthdays. ZKPs enable the prover to prove characteristics or circumstances without revealing sensitive information. ZKPs allow selective identity-related disclosure. Users can verify themselves anonymously and can confirm their academic degree without revealing their university or course. ZKPs authenticate knowledge without revealing it. A verifier can verify users without revealing network credentials. This reduces credential theft and interception [35].

Privacy-preserving transactions: ZKPs can be used to prove whether participants have sufficient cash or meet certain conditions, without disclosing their transaction history or the amount transferred. This safeguards financial transactions. ZKPs preserve input privacy for safe multiparty computing. This may help with complex identity-related data operations like aggregating statistics or data analysis in decentralized identity management without revealing individual data points.

Credential revocation: ZKPs can authenticate credential revocation without revealing the credentials or user privacy. This detects revoked credentials and blocks their use.

5.2.2 Confidential Transactions

Blockchain-based decentralized identity management uses cryptographic confidential transactions to protect privacy. Confidential transactions hide blockchain transaction quantities. Traditional blockchains show transaction amounts to all participants. Confidential transactions encrypt amounts for only the intended recipients while allowing the network to validate the transaction.

Pedersen commitments: Cryptographic frameworks hide and verify value in confidential transactions. Pedersen commitments blindly encrypt transaction amounts. The blockchain verifies this promise without revealing the amount.

Range proofs validate confidential transactions. Cryptographic range proofs confirm that the committed value is positive or within a given maximum value. Range proofs enable the network to verify transaction amounts without releasing them. Decentralized identity management hides identity-related transaction quantities with confidential transactions. To prevent identity-related behavior-inference or behavior-correlation attacks, identity verification systems can keep transaction amounts private. Confidentiality protects decentralized identity management systems during financial transactions. Participants can trade without disclosing account balances or transfer amounts. This safeguards identity management ecosystems during financial transactions [21].

Privacy-safe smart contracts: Confidential smart contracts protect sensitive data. Smart contracts may compute secret transaction amounts without disclosing them, maintaining blockchain integrity and privacy in complex procedures. Decentralized identity management protects privacy with confidential transactions. Confidential transactions let users privately carry out identity-related tasks while they benefit from blockchain transparency, immutability, and security.

5.3 Interoperability Solutions

Interoperability lets blockchain-based decentralized identity management systems and networks share identify data.

Interoperability Standards

Interoperability standards allow decentralized identification systems to share data. DIF, W3C verifiable credentials, and DID standards promote identity management solution interoperability.

Universal identifiers: Decentralized identifiers (DIDs) standardize blockchain identity descriptions. DIDs enable blockchain and decentralized identity platform interoperability by recognizing and referencing identities. Cross-chain interoperability lets blockchain networks share assets, including identity data. Atomic swaps, sidechains, and interoperability protocols (e.g., Polkadot and Cosmos) allow data and assets to smoothly migrate across blockchains, boosting decentralized identification system compatibility. Blockchain networks connect by using interchain communication protocols. Protocol-level interoperability is enabled by secure, trustless interblockchain communication (IBC). Interblockchain communication protocols transmit identification data and credentials across blockchain networks [36].

Bridge solutions: Bridge solutions allow the interoperation of dispersed identity systems. These bridges allow systems to communicate and exchange identity-related data between formats, protocols, and standards. Developers can combine many decentralized identification systems by using open Application Programming Interfaces (APIs) and Software Development Kits (SDKs). Open

APIs help identity management platforms to share data. Blockchain platforms, identity suppliers, and standardization organizations must collaborate for interoperability. Collaboration may involve standardization, best practices, and cross-platform compatibility. Decentralized identification systems can overcome siloed approaches by using interoperability solutions. Interoperability makes decentralized identity management more useful, scalable, and successful by integrating the digital identity ecosystem [37].

5.3.1 Cross-Chain Communication

Blockchain-based identity management requires cross-chain communication for interoperability. Blockchain networks can share identity data and transactions. Atomic swaps enable blockchains to trade assets, including identity data, without a trusted intermediary. Users can securely transport currencies or data across blockchains without carrying out centralized exchanges.

Pegged assets: Sidechains are interoperable. Transferring identity-related data and assets between the main blockchain and sidechains enables scalability and specialized services. Backing tokens on one blockchain with assets on another confers cross-chain value and allows data exchanges. interoperability protocols such as Polkadot, Cosmos, and Aion connect blockchains. These protocols allow blockchain transactions, data sharing, and decentralized identification system interoperability. Interblockchain communication (IBC) lets Cosmos blockchains interchange data. It secures and decentralizes identification data interchange between blockchains.

Wrapped tokens: One blockchain represents another. They confer cross-blockchain value and enable data transactions. Wrapped tokens link blockchain credentials and reputation scores. Oracles link blockchains to external data. Smart contracts and decentralized apps leverage their data. Oracles can connect blockchain networks and add identification data. Cross-chain smart contracts execute logic and actions. They allow for identifying transactions between blockchain-based decentralized identity systems. Cross-chain communication solutions move identity-related data, assets, and transactions between blockchain networks for decentralized identity management. Security, consensus, and governance are needed to protect identity-related interactions across blockchains [29].

5.3.2 Standardization Initiatives

Standardization aids blockchain-based decentralized identity management and interoperability. Field standardization requires the DIF to create interoperable decentralized identification standards and protocols. The DIF specifies DID, verifiable credentials, and DID authorization. Standards enable decentralized identity management and system interoperability. W3C standards are global, and W3C

standardizes decentralized identity technology. This group developed the verifiable credentials specification for issuing, verifying, and sharing digitally signed credentials. Linux Foundation open-source Hyperledger Indy has also created a decentralized identity platform. It provides decentralized identity management tools, libraries, and protocols. Hyperledger Indy's Aries framework supports identity system compatibility and safe peer-to-peer connectivity.

Internet identity workshop (IIW): The community-driven IIW gathers people and organizations working on decentralized identity and related technologies. IIW standardization can be explored by industries, researchers, and practitioners.

European Blockchain Services Platform (EBSI): This EU initiative offers a reliable and interoperable blockchain platform for public services. EBSI's eSSIF covers identity management standards and specifications.

The nonprofit InterWork Alliance (IWA) has created tokenization, smart contract, and blockchain interoperability standards. The IWA may affect multichain identity management. Developers, researchers, and stakeholders establish specifications, protocols, and best practices. Standards enable decentralized identity management interoperability, adoption, and consistency. These projects work together to develop blockchain-based decentralized identities [38].

5.4 User-Adoption Solutions

Users drive blockchain-based decentralized identity management through their acceptance, which is facilitated by several features.

User-friendly interfaces: Intuitive interfaces retain users. Decentralized identification apps should require no technological expertise. User education is needed, however, for decentralized identity acceptance. Consumers may learn to understand decentralized identity management through workshops, webinars, and education. Incentives can encourage decentralized identity solution adoption and use. Token-based loyalty schemes boost ecosystem participation.

Collaboration: Decentralized identification solutions can help people embrace existing platforms and processes. Integration with popular apps, social media, and financial institutions can attract users and simplify decentralized identity.

Privacy and data ownership: Privacy-conscious consumers would like this. Decentralized identity's data control and privacy can boost adoption.

Pilots and use cases: Successful pilots and real-world use cases demonstrate decentralized identification. Effective decentralized identification solutions for healthcare, supply chains, and finance can enhance confidence and acceptance.

Industry partners: Governments, businesses, and service providers increase user adoption. Strategic partnerships can increase the value of decentralized identity as more organizations and people join the ecosystem.

User assistance and feedback: Reliable user help and active user feedback improve the user experience and fix issues. User feedback promotes advancements to

decentralized identity solutions. Regulations and standards increase user trust. Data security, data privacy, and industry standards improve the legitimacy and adoption of decentralized identification systems.

Scalability and performance: Large user and transaction counts necessitate scalable and performant decentralized identity solutions. Users choose technologies that meet their needs quickly and smoothly.

5.4.1 User-Centric Interfaces

User-centric interfaces boost blockchain-based decentralized identity management adoption and experience. User-centered interface design has several important features.

Easy onboarding: Decentralized identity setup should be easy upon onboarding. Clear explanations and minimal technical jargon facilitate basic setup. Consumers' mental models must align with sensible user flows. The decentralized identity management system should have an intuitive User Interface (UI) and should avoid information overload. Visual cues, icons, and tooltips provide context and interface direction. Users' credentials and transaction information should easily be displayed.

Visualizations: Complex decentralized identity ideas should be explained with diagrams or flowcharts. Visuals can explain blockchain identification and data management. Visuals must allow interface customization for layouts, colors, and notifications. Ownership and customization let users access the decentralized identity management system [14].

Transparent control: Users need to be able to view and manage their identity-related data, so transparent controls must allow users to choose which identity information to share and with whom. These controls prioritize consent and make access revocation easy.

Mobile-friendly design: Such a design creates responsive interfaces on various devices for the users of decentralized identity management systems. For consistency, mobile apps and responsive web interfaces should be tailored to being used on smaller screens.

Help: User-centered interface design offers significant interface-based supports, such as frequently asked questions (FAQs), knowledge bases, chatbots, and customer service. To improve user confidence in the decentralized identity system, it must swiftly respond to user inquiries and provide clear support.

Usability testing and iterative design: Such testing provides user feedback, which will inform future improvements. An iterate UI is based on user feedback. To generate a user-centered design, always test and validate it.

Accessibility: A multiuser interface improves user accessibility. Consider color contrast, typeface size, screen reader compatibility, and keyboard navigation. Accessible interfaces promote adoption.

5.4.2 Education and Awareness

Blockchain-based identity management requires education and awareness. There are several awareness-raising methods available.

Educational resources: Decentralize identity management concepts, benefits, and use cases via whitepapers, manuals, tutorials, and movies. Technical and non-technical audiences should find these items useful.

Workshops and training: Decentralized identity management workshops, seminars, and training are available for individuals, corporations, and organizations. These events offer real use cases, demonstrations, and hands-on experiences.

Online forums: Decentralized identity management aficionados should have online groups and forums for them to discuss, learn, and share ideas. Participation, cooperation, and best-practice sharing boost learning on these platforms.

Industry conferences: Identity, blockchain, and digital identity conferences should present, conduct panels, and engage participants to promote decentralized identity management and its benefits. Professionals network at these events. Decentralized identity management should be integrated into academic courses and university-research cooperation. This connection can nurture future specialists and innovators and can improve academic–industry information transfer. Success stories on decentralized identity management should be showcased. These examples demonstrate the technology's applications, benefits, and consequences, encouraging others to explore it [39].

Tech communities: Developer networks and technology forums need to reach techies. Developer guides, code samples, and SDKs incorporate decentralized identity management into new and existing applications. Developers can improve technology by experimenting. Social media, blogs, podcasts, and online publications can be used to promote decentralized identity management; useful articles, interviews, and success stories promote the technology; and working with digital identification and blockchain technology industry alliances, standards bodies, and advocacy groups also promotes the technology. Industry-wide initiatives, working groups, and standardization increase awareness, align best practices, and establish a cohesive ecosystem [40].

Public education: Educating the public should promote decentralized identity management. These advertisements support self-sovereign identification, data privacy, and security and warn against centralized identity systems.

5.5 Regulatory Compliance Solutions

Blockchain identity management involves regulatory compliance. Although regulatory compliance comes with problems, several solutions are available.

Comply with laws: GDPR, identity verification, and sector-specific compliance standards should be monitored. Decentralized identity management solution must meet these laws' exact requirements.

Privacy by design: Privacy must be built into any decentralized identity management system. Privacy regulations require data reduction, consent management, and purpose limitation. They must encrypt and pseudonymize user data.

Data governance and consent management: User data must be handled with effective data governance, such as by following data ownership, storage, and access policies. User consent management technologies let people control their data and make informed decisions about their use and dissemination.

Compliance auditing and reporting: Any decentralized identity management system's regulatory compliance must be regularly examined. Records must be maintained to establish compliance and report to regulators.

Secure and immutable audit trails: Blockchain technology's transparency and immutability enable secure, tamper-proof audit trails. These audit trails track user interactions, credential issuances, and consent management to ensure compliance. Any decentralized identity management system should have strong identity verification and anti–money laundering protocols. Fraud prevention requires AML-compliant user onboarding, identity verification, and transaction monitoring. Compliance requirements can be discussed with regulatory agencies and authorities. Joining regulatory compliance industry alliances and working groups can help [41].

Compliant smart contracts: Decentralized identity management smart contracts must meet legal and regulatory requirements. Contracts should stipulate compliance.

Legal issues: Knowing how a decentralized identity management system affects jurisdiction will help when adjusting to them. Identity, data, and privacy regulations vary by country and jurisdiction, so every system must be adjusted accordingly.

Monitoring and adjusting: Compliance legislation changes. Every decentralized identity management system should meet the new regulations. When a compliance program's rules change, adjust the system to maintain compliance.

5.5.1 Collaboration with Regulatory Bodies

Blockchain-based decentralized identity management needs regulatory cooperation, which necessitates communicating with decentralized identity management regulators. Government, regulatory, and industry-specific identity management and data-privacy organizations must be considered when working with regulators.

Join regulatory consultations: Participate in digital identification, blockchain, and data-protection regulatory working groups. Consult industry experts on decentralized identity management regulatory frameworks. Discuss regulations and blockchain-based identity systems [5].

Request regulations: Ask regulators about decentralized identity management compliance and best practices. Discuss regulatory requirements and the technical capacity to comply.

Educate regulators: Inform authorities on blockchain-based decentralized identity management's benefits, technicalities, and prospects. Explain how the technology improves privacy, security, and user control. Help regulatory agencies to understand and address decentralized identity management.

Pilot programs: Pilot or test decentralized identity management technologies in regulatory sandboxes. These applications simulate blockchain-based identity system regulations and practicalities. They allow regulator–innovator collaboration and real-world testing.

Proportional regulation: Balance innovation with consumer protection regulations. Decentralized identity management can address privacy, security, and user empowerment, but flexible regulatory procedures are needed to enable innovation, interoperability, and market competitiveness.

Regulatory compliance: Create a decentralized identity management system that meets regulations. Comply with regulators and apply system controls. Compliance conversations help to ensure regulatory compliance.

Transparency and regulatory reporting: Alert regulators. Generate reports, respond to regulatory enquiries, and resolve compliance issues swiftly. Decentralized identification systems are trustworthy when transparent and regulated.

Industry standards and certification: Create decentralized identity management standards and certification frameworks with regulatory authorities and industry associations. Standards and certification collaboration ensure system and provider standardization, interoperability, and compliance. Actively monitor compliance in any decentralized identity management system. Internal audits, proper compliance records, and regulatory compliance analysis are essential. Fix compliance issues [42].

5.5.2 Adaptable Frameworks

Blockchain-based decentralized identity management must adapt to user, enterprise, and regulatory needs. Making adaptable frameworks requires attending to several considerations.

Modular architecture build: Use a modular architecture build to produce a modular, decentralized identity management platform. Modularity lets the system adapt to changing needs without disrupting any infrastructure.

Standards adherence: Integrate with various identity management systems by following industry standards and compatible protocols. Standardization promotes interoperability, cross-platform communication, and decentralized identity.

Plug-and-play parts: Create a plug-and-play framework for users and organizations to choose and integrate components. Customers can modify and scale, add-

ing features as needed. Customize the system with framework configuration options. Privacy, consent, authentication, and identity verification are included. Established user settings ensure privacy and regulatory compliance.

Governance and consensus systems: Establish governance mechanisms for decision-making and community involvement. Stakeholders can influence identity management through consensus, voting, or Decentralized Autonomous Organizations (DAOs).

Upgradability and compatibility: Support new blockchain, identity, and cryptography standards. The framework can adapt to technical, security, and regulatory changes without rebuilding.

Legality: Regulate framework design and architecture. Data protection, identity verification, and compliance are included. The framework's flexibility permits regulatory-specific compliance.

Cooperative feedback: Facilitate framework input to engage users, developers, and stakeholders. Examples of feedback input includes user input, developer communities, and open-source contributions. Community input improves the framework.

Developer tools: Provide detailed documentation, developer resources, and APIs to integrate and develop applications and services on the framework. Clear documentation lets developers personalize the framework.

Trials and pilots: Test and pilot the framework's functionality, usability, and flexibility in the real word. User, organization, and regulatory agency comments can improve the framework [43].

6 Case Studies and Existing Implementations

Decentralized identity management case studies use blockchain.

Sovrin: Blockchain-based Sovrin gives global self-sovereign identity. Individuals and organizations can govern their digital identities with its decentralized identification infrastructure. Sovrin protects identity interactions with DIDs, VCs, and ZKPs.

uPort: This Ethereum-based self-sovereign identity manages digital identities and personal data and selectively shares information with service providers. Decentralized Identifiers (DIDs), Distributed Key Management System (DKMS), and smart contracts personalize identity management for uPort.

Microsoft's DID framework: W3C standards underpin Microsoft's DID framework. Users can create, own, and control their digital identities for privacy and interoperability. Microsoft supports blockchain, identity hubs, and decentralized key management.

Civic: Civic authenticates identities and shares personal data with trusted entities by using blockchain technology. Civic's decentralized identification enables users

to save and share their identity information on their devices. Civic uses blockchain to safely and openly verify IDs.

Verity: Evernym's decentralized identity platform allows organizations to issue and verify VCs. Sovrin's distributed ledger secures and interoperates self-sovereign identification for Verity. It manages passwords, data, and privacy-enhanced disclosures [44].

6.1 Identity Management in Healthcare

Blockchain-based decentralized identity management benefits healthcare. Healthcare blockchain-based decentralized identification management has several key features.

Blockchain protection: Blockchain protects patient identity verification. Decentralized ledgers protect patient data against identity theft and fraud. Patients can easily share verified information with healthcare institutions and control their identities. Blockchain-based decentralized identity management interoperates medical records. Patients may access and share their medical records among providers with a single digital identity, eliminating data entry and improving care coordination. While sharing, blockchain secures patient data. Blockchain technology enables patients to give fine-grained data-sharing consent. The blockchain allows patients to choose which healthcare institutions can access their medical data and for what purposes. This enhances patients' data-sharing decisions and safeguards their privacy [45].

Clinical trials and research: Blockchain-based decentralized identity management simplifies patient recruitment. Securely combining patients' identities with their health data on the blockchain lets researchers quickly identify qualified participants while maintaining patients' privacy and data integrity. Patients may thus entrust their data to research.

Prescription and medication management: Blockchain enhances security and traceability. The blockchain can link patients' digital identities to their pharmaceutical records, reducing medication errors, counterfeit drugs, and supply-chain tracking. Blockchain-based identity management protects healthcare data. Only authorized parties can decrypt blockchain-stored patient IDs and sensitive health data. Decentralized identities (DIDs) and verifiable credentials (VCs) increase privacy by reducing the level of personal data disclosure.

Blockchain-based identity management detects and prevents healthcare fraud. A secure patient identity and healthcare transaction record helps detect fraud. Blockchain's transparency allows auditors and authorities to investigate suspicious activities and protect the healthcare system. Decentralized identity management allows patients to have more control over their health data. Patients can choose healthcare providers, revoke access to their data, and view data use. Patient trust and healthcare engagement therefore increase. Decentralized identity management must

involve healthcare providers, technology vendors, regulators, and patients. Legal, regulatory, data-protection, and healthcare industry norms and sensitivities must be addressed. Blockchain-based decentralized identity management could improve patient care, data security, and interoperability in the healthcare industry [46].

6.2 Digital Identity for Financial Inclusion

Financial inclusion is possible with blockchain-secured digital IDs. Decentralized identity management helps financial inclusion in several ways:

Identity verification: Blockchain-based decentralized identity management lets undocumented people construct digital identities. Financial businesses can verify IDs by using blockchain's immutability and cryptography. This helps people who lack official documentation or who have limited identity verification systems.

Financial services: Decentralized identity management enables remote access to financial services. Blockchain-based identities establish trust and trustworthiness, enabling bank accounts, loans, and formal financial participation.

Cross-border payments: Blockchain-based identities enable faster, cheaper cross-border payments, especially for those without bank accounts. Decentralized identities offer fast, secure identity verification and cross-border transactions. Decentralized identity management improves microfinance and peer-to-peer lending networks. Blockchain-based identities help financially excluded people to access microloans and peer-to-peer loans and showcase their creditworthiness [47].

Transfers: Blockchain-based digital IDs simplify and safeguard underserved transfers. By establishing their identities on the blockchain, individuals can verify their eligibility to receive remittances, reducing transaction costs and expediting and securing cross-border transactions.

Financial data privacy and security: Blockchain-based decentralized identity management gives people control over their financial data. Self-sovereign identities allow individuals to choose to share financial information to financial service providers, retaining data privacy while accessing crucial services. This safeguards data and gives users more control. Blockchain-based decentralized identity management simplifies KYC for financial institutions. The blockchain can verify identity once and share it with several organizations, saving time. Financial institutions can meet regulations without burdening consumers. Financial inclusion requires financial institutions, technology vendors, regulators, and local communities to adopt decentralized identity management. Legal, regulatory, data privacy, and underrepresented demographic demands must be addressed. Blockchain technology for decentralized identity management can promote financial inclusion by allowing safe and portable identities to access important financial services and participate in the global economy [48].

6.3 Decentralized Identity for IoT Devices

Blockchain-based decentralized identity management improves IoT-device security, interoperability, and data privacy. Decentralized IoT identity builds trust in using IoT devices:

Device trust: Blockchain-based decentralized identity management secures IoT-device authentication and confers trust. A blockchain-stored DID can identify each device. Authenticating and securely connecting devices, networks, and apps reduces the risk of unauthorized access and device spoofing. Decentralized identities allow IoT devices to safely share data and communicate with other platforms. Verifiable credentials and cryptography protect shared data. Decentralized identity management makes IoT devices and platforms compatible. Identity protocols and blockchain-based IDs allow IoT devices to share data across networks and ecosystems. This simplifies IoT system management. IoT-device owners can control their data by using decentralized identity management. Companies using device data can receive granular approval from owners. Finally, privacy and IoT-device data management are protected [49].

Blockchain-based decentralized identity management can provide supply-chain IoT devices with unique identities, boosting transparency. These IDs can verify the origin, legitimacy, and supply-chain movement of products, boosting stakeholder trust [50]. Decentralized identity management secures IoT firmware updates. Blockchain device IDs allow approved firmware changes. Blockchain immutability allows firmware auditing and verification, reducing malicious manipulation. Decentralized identity management helps IoT systems save electricity. Blockchain identities and cryptographic keys enable device energy optimization and safe access control. Optimization saves energy and money. Blockchain, identity protocols, and IoT platforms enable decentralized IoT identity management, addressing scalability, interoperability, and device resource restrictions. Decentralized identity unlocks the full potential of the Internet of Things by ensuring data integrity, user control, and security for IoT devices [51].

6.4 Cross-Border Identity Verification

Cross-border ID verification is difficult. Blockchain-based decentralized identity management improves the efficiency, security, and privacy of cross-border identity verification. Decentralized identity management grants autonomy. Cross-border verification lets people pick which identification information to share, which enhances data security. Decentralized identification aids cross-border identity verification.

Valid credentials: Blockchain-based decentralized identity management leverages the digitally signed statements of trusted institutions. Names, birthdates, and addresses are verifiable. These credentials can be transferred internationally and confirmed by trusting parties without relying on centralized identity providers, reducing dependence on identification certificates. Blockchain verifies identifying records. Blockchain-stored identity data can lessen the risk of fraudulent IDs or tampering during cross-border verification. Blockchain-based decentralized identity management improves international interoperability and homogeneity. By using similar identity protocols and standards, cross-border verification systems may verify identities across blockchain platforms and jurisdictions [52].

Blockchain-based decentralized identity management lets trusted entities attest to identities. These attestations authenticate identity. Cross-border verification can create confidence and confirm identities through these attestations. Blockchain consensus checks identity. Consensus techniques in cross-border verification systems verify identities and thwart fraudulent information. Zero-knowledge proofs or selective disclosure can protect privacy during cross-border identity verification with blockchain-based decentralized identity management. These technologies allow consumers to verify their identities without disclosing personal information, increasing privacy and lowering data exposure. Collaboration among governments, identity issuers, dependent parties, and technology suppliers is needed for decentralized cross-border identity verification. Legal, regulatory, data-protection, and privacy issues must be addressed to ensure compliance and build trust. Blockchain-based decentralized identity verification could simplify and secure cross-border identity verification, boosting privacy and user control, as shown in Fig. 8.3 [53].

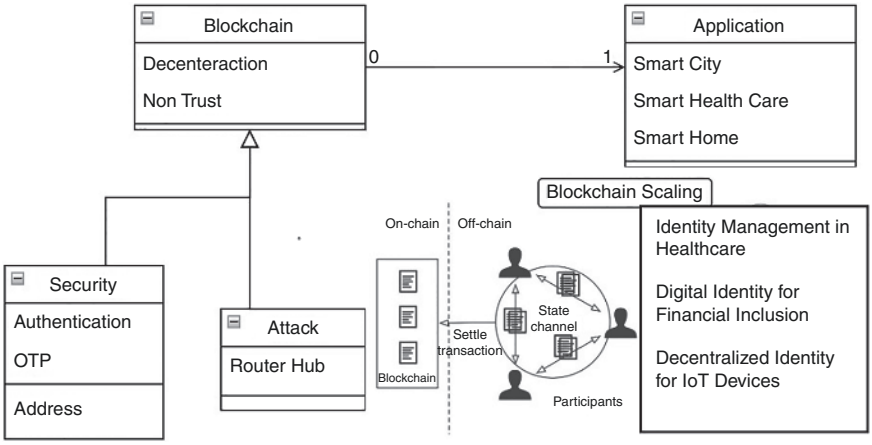

Fig. 8.3 Blockchain transformations in cryptocurrency and the traditional financial world

7 Conclusion and Future Directions

Blockchain-based decentralized identity management can solve identification system issues and offer new avenues for individuals, corporations, and industries. Blockchain's immutability, security, and decentralization enhance identity management's privacy, control, and interoperability. DIDs, self-sovereign identities, and verifiable credentials provide users with more identity control. They can selectively share verified credentials with trusted partners, eliminating centralized identity providers and reducing data breaches and instances of identity theft. Identity management empowers users. Blockchain-based identification solutions can improve security, streamline processes, and enable new business models in healthcare, finance, supply chains, and the IoT. Decentralized identification may affect patient identification, financial inclusion, supply-chain transparency, and IoT-device management.

Making decentralized identity management more popular would require overcoming many difficulties. Scalability, privacy, interoperability, regulatory compliance, and user acceptance matter. Off-chain storage, sharding, zero-knowledge proofs, and regulatory involvement can address these challenges and expand adoption.

Blockchain-based identity management needs further research, standardization, and industry involvement. Consensus algorithms, privacy-preserving approaches, and cross-chain communication protocols improve the scalability, security, and interoperability of decentralized identification solutions. User adoption and compliance require user-friendly interfaces, education, and regulations. Blockchain technology has the potential to transform digital identity management. Decentralized blockchain identity management might empower individuals, improve privacy and security, and enable trusted cross-border transactions.

7.1 Summary of Findings

Blockchain-based decentralized identity management alters digital identities. Identity management is also decentralized. The conceptual framework of blockchain is undergirded by self-sovereign identities, where users can choose to share verified credentials with trusted parties. Decentralized identity management enhances privacy, security, and control. It secures identity verification, promotes platform and jurisdiction compatibility, and removes centralized identity suppliers. Healthcare, finance, supply-chain, IoT, and cross-border identity verification use can be leveraged for decentralized identity management. Decentralized identity management promotes financial inclusivity, supply-chain transparency, secure service access, and IoT-device connectivity. Decentralized identity management challenges include scalability, privacy, interoperability, regulatory compliance, and user uptake. Off-chain storage, sharding, zero-knowledge proofs, standardization,

user-centric interfaces, education, and regulatory collaboration are needed to overcome these challenges.

Decentralized identity management has numerous solutions, namely sharding, layer 2 scaling, and off-chain storage scaling. Confidential transactions and zero-knowledge proofs promote privacy and security. Standards and cross-chain communication enable interoperability; user-centric interfaces and education encourage uptake; and regulatory body participation ensures compliance. Decentralized identity management needs research, standards, and collaboration. Consensus techniques, privacy-preserving procedures, and cross-chain communication protocols can increase the scalability and security of decentralized identification solutions. Adoption and compliance require user-friendly interfaces, education, and regulatory frameworks.

7.2 Future Research and Development Opportunities

Blockchain-based decentralized identity management research could focus on user experiences, regulatory frameworks, case studies, scales, and decentralized identification solutions:

Studying scales and decentralized identification solutions: Researchers could study solutions for sharding, off-chain storage, and layer 2 that accommodate additional users and transactions without compromising security or performance. Research could improve decentralized identity management privacy and security. Zero-knowledge proofs, homomorphic encryption, and secure multiparty computing protect user data and transactions while speeding up verification and authentication. Decentralized identification systems and platforms need interoperability standards. To facilitate data exchange among blockchain-based identity solutions, future research could create and promote common identity protocols, data formats, and interoperability standards.

User experiences: For widespread use, decentralized identity systems must improve the user experience. Thus, researchers could study user-centric interfaces, intuitive mobile apps, and user-friendly decentralized identity management solutions. Awareness campaigns could boost decentralized identity management acceptance.

Governance and regulatory frameworks: Research could provide decentralized governance and regulatory frameworks for blockchain identity management. Legal issues, liability frameworks, decentralized dispute resolutions, and identity management systems should be included. Integrating decentralized identity management with upcoming technologies could offer new avenues. Research could connect decentralized identities with IoT devices, artificial intelligence (AI), Machine learning (ML), and edge computing to enable secure, privacy-preserving interactions in complex and dynamic scenarios.

Case studies: Industry-wide case studies could improve decentralized identification solutions. Application cases could be explored in healthcare, finance, supply chains, other industries, and government services to identify and learn more about decentralized identity management's issues, benefits, and effects.

References

1. Venkatraman, S., & Parvin, S. (2022). Developing an IoT identity management system using blockchain. *System, 10*(2). https://doi.org/10.3390/systems10020039
2. Prasad, S. N., & Rekha, C. (2023). Block chain based IAS protocol to enhance security and privacy in cloud computing. *Measurement: Sensors, 28*, 100813. https://doi.org/10.1016/j.measen.2023.100813
3. Chandan, A., John, M., & Potdar, V. (2023). Achieving UN SDGs in food supply chain using blockchain technology. *Sustain., 15*(3), 1–21. https://doi.org/10.3390/su15032109
4. Kişi, N. (2022). Exploratory research on the use of blockchain technology in recruitment. *Sustainability, 14*(16). https://doi.org/10.3390/su141610098
5. Kairaldeen, A. R., Abdullah, N. F., Abu-Samah, A., & Nordin, R. (2023). Peer-to-peer user identity verification time optimization in iot blockchain network. *Sensors, 23*(4). https://doi.org/10.3390/s23042106
6. Juneja, G., & Naswa, R. (2023). Bittrack-A decentralized trust based identity and access management approach. *International Journal of Intelligent Systems And Applications In Engineering, 2023*(5s), 368–388. [Online]. Available: www.ijisae.org
7. Bai, P., Kumar, S., Aggarwal, G., Mahmud, M., Kaiwartya, O., & Lloret, J. (2022). Self-sovereignty identity management model for smart healthcare system. *Sensors, 22*(13), 1–25. https://doi.org/10.3390/s22134714
8. Akbar, M. A., Leiva, V., Rafi, S., Qadri, S. F., Mahmood, S., & Alsanad, A. (2022). Towards roadmap to implement blockchain in healthcare systems based on a maturity model. *Journal of Software: Evolution and Process, 34*(12), 1–15. https://doi.org/10.1002/smr.2500
9. Gilani, K., Ghaffari, F., Bertin, E., & Crespi, N. (2022). Self-sovereign identity management framework using smart contracts, *Proc. IEEE/IFIP Netw. Oper. Manag. Symp. 2022 Netw. Serv. Manag. Era Cloudification, Softwarization Artif. Intell. NOMS 2022*. https://doi.org/10.1109/NOMS54207.2022.9789831.
10. Shobanadevi, A., Tharewal, S., Soni, M., Kumar, D. D., Khan, I. R., & Kumar, P. (2022). Novel identity management system using smart blockchain technology. *International Journal of Systems Assurance Engineering and Management, 13*(s1), 496–505. https://doi.org/10.1007/s13198-021-01494-0
11. Wu, A., Guo, Y., & Guo, Y. (2023). A decentralized lightweight blockchain-based authentication mechanism for Internet of Vehicles. *Peer-to-Peer Networking and Applications, 16*, 1340. https://doi.org/10.1007/s12083-022-01442-0
12. Geetha, R., Padmavathy, T., & Umarani Srikanth, G. (2022). A scalable block chain framework for user identity management in a decentralized network. *Wireless Personal Communications, 123*(4), 3719–3736. https://doi.org/10.1007/s11277-021-09310-5
13. Deng, W., Huang, T., & Wang, H. (2023). A review of the key technology in a blockchain building decentralized trust platform. *Mathematics, 11*(1). https://doi.org/10.3390/math11010101
14. Taherdoost, H. (2023). Smart contracts in blockchain technology: a critical review. *Information, 14*(2). https://doi.org/10.3390/info14020117
15. Vaigandla, K. K. (2023). Review on blockchain technology: architecture, characteristics, benefits, algorithms, challenges and applications. *The Mesopotamian Journal of Cybersecurity, 2023*, 73–85. https://doi.org/10.58496/mjcs/2023/012

16. Tahora, S., Saha, B., Sakib, N., Shahriar, H., & Haddad, H. (2023). *Blockchain technology in higher education ecosystem: unraveling the good, bad, and ugly*. arXiv preprint arXiv:2306.04071. [Online]. Available: http://arxiv.org/abs/2306.04071
17. Saha, B., Hasan, M. M., Anjum, N., Tahora, S., Siddika, A., & Shahriar, H. (2023). *Protecting the decentralized future: An exploration of common blockchain attacks and their countermeasures*. arXiv preprint arXiv:2306.11884. [Online]. Available: http://arxiv.org/abs/2306.11884
18. Javed, I. T., Alharbi, F., Bellaj, B., Margaria, T., Crespi, N., & Qureshi, K. N. (2021). Health-id: A blockchain-based decentralized identity management for remote healthcare. *Healthc., 9*(6), 1–21. https://doi.org/10.3390/healthcare9060712
19. Buttar, A. M., Bano, M., Akbar, M. A., Alabrah, A., & Gumaei, A. H. (2023). Toward trustworthy human suspicious activity detection from surveillance videos using deep learning. *Soft Computing, 0123456789*. https://doi.org/10.1007/s00500-023-07971-x
20. Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing. *Future Internet, 14*(11), 1–22. https://doi.org/10.3390/fi14110341
21. Khalid, M. I., et al. (2023). A comprehensive survey on blockchain-based decentralized storage networks. *IEEE Access, 11*, 10995–11015. https://doi.org/10.1109/ACCESS.2023.3240237
22. Florea, A. I., Anghel, I., & Cioara, T. (2022). A review of blockchain technology applications in ambient assisted living. *Future Internet, 14*(5). https://doi.org/10.3390/fi14050150
23. Djeddai, A., & Khemaissia, R. (2023). PrivyKG: Security and privacy preservation of knowledge graphs using blockchain technology. *Informatica, 47*(5), 137–152. https://doi.org/10.31449/inf.v47i5.4698
24. Bouras, M. A., Lu, Q., Dhelim, S., & Ning, H. (2021). A lightweight blockchain-based iot identity management approach. *Future Internet, 13*(2), 1–14. https://doi.org/10.3390/fi13020024
25. Waseem, M., Adnan Khan, M., Goudarzi, A., Fahad, S., Sajjad, I. A., & Siano, P. (2023). Incorporation of blockchain technology for different smart grid applications: Architecture, prospects, and challenges. *Energies, 16*(2). https://doi.org/10.3390/en16020820
26. Eremina, L., Mamoiko, A., & Aohua, G. (2023). Application of distributed and decentralized technologies in the management of intelligent transport systems. *Journal of Intelligent and Robotic Systems, 3*(2), 149–161. https://doi.org/10.20517/ir.2023.09
27. Du, Z., Jiang, W., Tian, C., Rong, X., & She, Y. (2023). Blockchain-based authentication protocol design from a cloud computing perspective. *Electronics, 12*(9). https://doi.org/10.3390/electronics12092140
28. Mateen, A., & Amir, H. (2016). Enhancement in the effectiveness of requirement change management model for global software development. *Journal of Science International Lahore, 28*(2), 1161–1164. [Online]. Available: http://arxiv.org/abs/1605.00770
29. Schlatt, V., Sedlmeir, J., Traue, J., & Völter, F. (2023). Harmonizing sensitive data exchange and double-spending prevention through blockchain and digital wallets: The case of E-prescription management. *Distributed Ledger Technologies: Research and Practice, 2*(1), 1–31. https://doi.org/10.1145/3571509
30. Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: Security issues, healthcare applications, challenges and future trends. *Electronics, 12*(3). https://doi.org/10.3390/electronics12030546
31. Badirova, A., Dabbaghi, S., Moghaddam, F. F., Wieder, P., & Yahyapour, R. (2023). A survey on identity and access management for cross-domain dynamic users: issues, solutions, and challenges. *IEEE Access, 11*(June), 61660–61679. https://doi.org/10.1109/ACCESS.2023.3279492
32. Mahmood, M. S., & Al Dabagh, N. B. (2023). Blockchain technology and internet of things: Review, challenge and security concern. *International Journal of Electrical and Computer Engineering, 13*(1), 718–735. https://doi.org/10.11591/ijece.v13i1.pp718-735
33. Tan, E., Lerouge, E., Du Caju, J., & Du Seuil, D. (2023). *Verification of education credentials on european blockchain services infrastructure (EBSI): Action research in a cross-border use case between Belgium and Italy* (Vol. 7).
34. Zhu, X., He, D., Bao, Z., Luo, M., & Peng, C. (2023). An efficient decentralized identity management system based on range proof for social networks. *IEEE Open Journal of the Computer Society, 4*(March), 84–96. https://doi.org/10.1109/OJCS.2023.3258188

35. Alanzi, H., & Alkhatib, M. (2022). Towards improving privacy and security of identity management systems using blockchain technology: A systematic review. *Applied Sciences, 12*(23). https://doi.org/10.3390/app122312415
36. Singh, D., Monga, S., Tanwar, S., Hong, W. C., Sharma, R., & He, Y. L. (2023). Adoption of blockchain technology in healthcare: Challenges, solutions, and comparisons. *Applied Sciences, 13*(4). https://doi.org/10.3390/app13042380
37. Rahmani, M. K. I., et al. (2022). Blockchain-based trust management framework for cloud computing-based internet of medical things (IoMT): A systematic review. *Computational Intelligence and Neuroscience, 2022*, 1. https://doi.org/10.1155/2022/9766844
38. Truong, H., et al. (2022). Enabling decentralized and auditable access control for IoT through blockchain and smart contracts. *Security and Communication Networks, 2022*, 1. https://doi.org/10.1155/2022/1828747
39. Mesías-Ruiz, G. A., Pérez-Ortiz, M., Dorado, J., de Castro, A. I., & Peña, J. M. (2023). Boosting precision crop protection towards agriculture 5.0 via machine learning and emerging technologies: A contextual review. *Frontiers in Plant Science, 14*(March), 1–22. https://doi.org/10.3389/fpls.2023.1143326
40. Xiao, Y., et al. (2022). Decentralized spectrum access system: Vision, challenges, and a blockchain solution. *IEEE Wireless Communications, 29*(1), 220–228. https://doi.org/10.1109/MWC.101.2100354
41. Zubaydi, H. D., Varga, P., & Molnár, S. (2023). Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: A systematic literature review. *Sensors, 23*(2). https://doi.org/10.3390/s23020788
42. Friedewald, M., & Kreutzer, M. (2022). *Selbstbestimmung, Privatheit und Datenschutz*. Springer.
43. Sung, C. S., & Park, J. Y. (2021). Understanding of blockchain-based identity management system adoption in the public sector. *Journal of Enterprise Information Management, 34*(5), 1481–1505. https://doi.org/10.1108/JEIM-12-2020-0532
44. Kumar, D., Kumar, S., & Joshi, A. (2023). Assessing the viability of blockchain technology for enhancing court operations. *International Journal of Law, 65*, 425. https://doi.org/10.1108/IJLMA-03-2023-0046
45. Sadique, K. M., Rahmani, R., & Johannesson, P. (2023). DIdM-EIoTD: Distributed identity management for edge Internet of Things (IoT) devices. *Sensors, 23*(8). https://doi.org/10.3390/s23084046
46. Chawla, P., Kumar, A., Nayyar, A., & Naved, M. (2023). *Blockchain, IoT, and AI technologies for supply chain management*. https://doi.org/10.1201/9781003264521.
47. Ghaffari, F., Gilani, K., Bertin, E., & Crespi, N. (2022). Identity and access management using distributed ledger technology: A survey. *International Journal of Network Management, 32*(2), 1–19. https://doi.org/10.1002/nem.2180
48. Wang, Z., Zhang, C., & Mu, X. (2023). Decentralized solution for cold chain logistics combining IoT and blockchain technology. *Journal of network intelligence, 8*(1), 47–61.
49. Uppal, S., Kansekar, B., Mini, S., & Tosh, D. (2023). HealthDote: A blockchain-based model for continuous health monitoring using interplanetary file system. *Healthcare Analytics, 3*(March), 100175. https://doi.org/10.1016/j.health.2023.100175
50. Han, R., Shapiro, G., Gramoli, V., & Xu, X. (2020). On the performance of distributed ledgers for internet of things. *Internet of Things, 10*, 1–11. https://doi.org/10.1016/j.iot.2019.100087
51. Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021). Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. *Blockchain: Research and Applications, 2*(2), 100014. https://doi.org/10.1016/j.bcra.2021.100014
52. Rathee, T., & Singh, P. (2022). A systematic literature mapping on secure identity management using blockchain technology. *Journal of King Saud University, Computer and Information Sciences, 34*(8), 5782–5796. https://doi.org/10.1016/j.jksuci.2021.03.005
53. Liao, C. H., Guan, X. Q., Cheng, J. H., & Yuan, S. M. (2022). Blockchain-based identity management and access control framework for open banking ecosystem. *Future Generation Computer Systems, 135*, 450–466. https://doi.org/10.1016/j.future.2022.05.015