SoK: Credential-Based Trust Management in Decentralized Ledger Systems

Yanna Jiang[1], Haiyu Deng[1]✉, Qin Wang[2], Guangsheng Yu[1], Xu Wang[1], Yilin Sai[2], Shiping Chen[2], Wei Ni[1], Ren Ping Liu[1]
[1]*University of Technology Sydney* | [2]*CSIRO Data61*

***Abstract*—Trust management systems (TMS) are crucial for managing trust in distributed environments. The rise of decentralized systems and blockchain has sparked interest in credential-based decentralized trust management systems (DTMS). This paper bridges the gap between theory and practice through a systematic review of credential-based DTMS. We analyze existing DTMS solutions through multiple dimensions, including their architectural designs, credential mechanisms, and trust evaluation models. Our survey provides a detailed taxonomy of credential-based DTMS approaches and establishes comprehensive evaluation criteria for assessing DTMS implementations. Through extensive analysis of current systems and implementations, we identify critical challenges and promising research directions in the field. Our examination offers valuable insights for researchers and practitioners working on DTMS, particularly in areas such as access control, reputation systems, and blockchain-based trust frameworks.**

***Index Terms*—Trust Management Systems, Decentralized Systems, Credentials**

I. Introduction

With the rise of Internet, a growing number of individuals and organisations are connected with each other to share information and services. The emergence of Internet of Things (IoT) and blockchain accelerate the trend, enabling networks that are more diverse, dynamic, and open.

The nature of such networks brings new security challenges, as interacting entities may be unfamiliar with each other, rendering identity-based security mechanisms inadequate for regulating interactions [1]. Trust Management Systems (TMS) [2] were introduced to enhance network security by enabling entities to assess whether another entity is qualified to provide or utilize specific information or services [1], [3]. This assessment is based on evaluating the trustworthiness of entities using various evidence and criteria [4], [5]. TMS have garnered significant interest from the research community and have been applied in areas such as access control and authorization [2], [6]–[8], identity and data authentication [9]–[12], malicious node detection [13]–[15], and the prevention of internal attacks [14], [16], [17], including attacks by authenticated but hostile entities, such as Sybil attacks. In addition, TMS has been applied to enhance service quality of networks by optimizing routing path selection [18], [19], service provider selection [5], [20], [21], and resource allocation [22], [23].

TMS can be classified into credential-based and behavior-based systems [24], with the former verifying entity credentials [4] and the latter assessing historical behaviors [5]. While credential-based TMS provide robust security analysis but face dynamicity challenges, behavior-based systems offer dynamic evaluation but suffer from cold start problems and security uncertainties [4], [25]. This paper focuses more on credential-based TMS.

Architecturally, TMS can be implemented in centralised, decentralised, or hybrid architectures [26]. Centralized systems rely on a central authority for trust management through credential stores [27] or periodic evaluations [28], but face issues with single points of failure and scalability [7], [29]. In contrast, decentralized TMS (DTMS) enable autonomous trust management by individual entities, improving scalability and robustness while aligning with trust's inherent subjectivity [2]. With the emergence of Blockchain [30], [31] and Web3 [32], [33], DTMS have gained significant traction [3], [7] and form the focus of this paper.

Despite growing interest in DTMS, existing research remains fragmented across three dimensions: (a) Studies predominantly focus on specific technical implementations (e.g., blockchain-based solutions [7]) without systematic analysis of architectural patterns; (b) Current classifications lack multi-layered perspectives integrating governance models with technical implementations [3]; (c) Evaluation criteria for dynamicity and explainability remain inconsistent across domains [29]. We address these gaps with the following contributions.

- We provide a detailed analysis of trust characteristics, including dynamicity and explainability, and their implications for system design, forming the theoretical foundation for credential-based DTMS.
- We conduct a comprehensive classification and layered analysis of existing credential-based DTMS, focusing on trust formation, trust verification, and trust management, to highlight the integration of governance, network, and data layers for enhanced system interoperability.
- We establish a set of evaluation criteria focusing on dynamicity, privacy, scalability, and explainability, offering a systematic approach to assess the effectiveness of credential-based DTMS implementations.

The rest of this paper is organized as follows. Section II explores trust characteristics and system design implications, Section III analyzes credential-based DTMS, Section IV

presents evaluation criteria, and Sections V and VI discuss future directions and conclusions.

II. Trust System Foundations

A. Trust

Trust originated from social sciences has been adapted to computer science and network security [17]. In distributed systems, trust represents a quantifiable belief about an entity's capability to perform specific tasks [34], [35].

Trust has several key characteristics that can be divided into two categories. The first category includes implicitness, transitivity, asymmetry, antonymy, asynchrony, and gravity [20], [36], [37]. The second includes subjectivity, dynamicity, and context-awareness [29], [36]. These characteristics are interconnected - for example, subjectivity influences asymmetry and gravity, while dynamicity emerges from transitivity and context-awareness.

1) Implicitness: Trust exhibits implicitness in two ways. First, entities cannot easily quantify trust due to complex evidence [20], [29]. Second, trust emerges implicitly through actions [4], such as granting access permissions. Security systems frequently rely on the implicit trust assumptions [38].

2) Transitivity: Trust can propagate: when A trusts B, A may also trust entities trusted by B. This indirect trust [36] enables delegation [7] and underlies graph-based trust models like SDSI/SPKI [39], [40]. It is particularly important in service-oriented architectures for provider selection [20].

3) Dynamicity: Trust relationships evolve over time based on context [36], [41], [42], including entity states and environmental conditions [43]. Trust levels can increase through positive interactions or decay naturally [29], [44]. Modern systems implement this through mechanisms like PKI certificate revocation [45] and IoT trust updates [42], [46], [47].

4) Subjectivity: Trust is inherently subjective [48], with each entity having its own standards for establishing and evaluating trust. This manifests through different access to evidence [44] and entity-specific evaluation criteria [49]. This subjectivity is fundamental to DTMS design [2], enabling local control over trust relationships [4], [7], [29].

These characteristics shape the design of trust-based systems, presenting both challenges and opportunities for implementing novel trust mechanisms.

B. Trust, Reputation, and Risk

In behavior-based DTMS, trust and reputation are related but distinct. Trust is a subjective, entity-driven assessment, while reputation reflects a passive, collective evaluation from the community [29], [50], [51]. This distinction allows trust to diverge from reputation in specific scenarios.

Some DTMS architectures incorporate reputation-based trust evaluation mechanisms [52], potentially leading to centralization through dominant highly-trusted entities [16]. This centralization stems from a positive feedback loop where elevated reputation scores reinforce trust levels, which enhances reputation. To maintain decentralization, implementations typically incorporate multiple trust evaluation factors, including direct interaction history.

Risk is a core element of trust. [53] defines trust as an entity's willingness to depend on another without failure mitigation, framing trust as a decision to accept potential failure. [14] builds on this by linking trust levels to risk-benefit analysis, as shown in a decentralized PKI model. Risk assessment both informs trust decisions and clarifies underlying assumptions. In networks, it helps evaluate vulnerabilities. [54] proposed a framework to assess attack impacts in trust-aware systems, showing how trust propagation [55], [56] can increase risk through the spread of trust scores.

C. Trust Policy, Proof and Verifiability

Trust policies are fundamental to TMS. Initially introduced for access control in early DTMS work [1], they were formalized as predicates evaluating actions [2] and implemented as unsigned credentials to define authority. As DTMS evolved, trust policies grew to include rules, algorithms, and parameters for credential-based trust decisions [10]. Recent approaches favor declarative expressions [15], [57], [58] to support security analysis and coordination.

Credential-based TMS employ proofs to demonstrate entity qualifications, subject to trust policy verification [3], [8], [59]. These proofs manifest as credentials, cryptographic computations, or combinations thereof. Beyond enhancing verification efficiency, proof mechanisms enable privacy preservation via cryptographic techniques like zero-knowledge proofs.

The integration of trust policies and proof lifecycle establishes system verifiability. In credential-based DTMS, verifiability encompasses multiple dimensions:

- **Mechanism-based**: Cryptographical (integrity verification), structural (semantic verification), and institutional (legitimacy verification) [15], [60];
- **Object-based**: Hierarchical verification spanning identity [12], cross-domain credentials [9], role statements [59], and data packets [15].

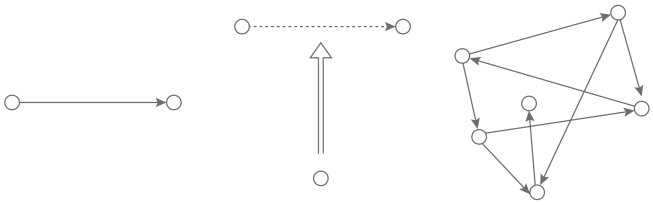
This hierarchical verification structure creates dependencies from higher-level (roles, data) to lower-level (credentials, identities) verifications [61].

Credential verification in DTMS operates peer-to-peer between prover and verifier [7], without issuer involvement. This decentralized model, supported by cryptography and DLT, enables autonomous trust management and verification [60].

III. Credential-Based DTMS Framework

DTMS require a systematic framework to analyze their architectures and functionalities. While existing research has proposed various approaches to decompose trust systems - such as the six-phase trust computation model for IoT [62] and the four-layer Decentralized Identifier (DID)-based trust stack [61] - these frameworks are either too specific to certain

domains or lack consideration of the distributed nature of modern trust systems. To address this gap, we propose a two-dimensional framework specifically designed for analyzing DTMS, where one dimension is sequential and the other is spatial. The sequential dimension captures trust lifecycle phases while the spatial dimension describes architectural layers. This comprehensive framework enables systematic classification and analysis of state-of-the-art DTMS solutions.



(a) Trust Formation (b) Trust Verification (c) Trust Management

Fig. 1: Three-Phase Sequential Classification

For the sequential dimension, as illustrated in Figure 1, DTMS encompasses three fundamental phases:

- **Trust formation**. Trust formation focuses on establishing and evaluating trust relationships through empirical evidence, including behavioral history, consensus mechanisms, and existing trust networks. This phase facilitates trust establishment between a trustor and trustee through systematic evaluation methodologies.
- **Trust verification**. Trust verification enables cryptographic validation of established trust relationships by third parties. This phase implements verification protocols that allow external verifiers to authenticate the existence and validity of trust relationships.
- **Trust management**. Trust management encompasses the systematic maintenance and governance of trust relationships, including dynamic updates, certificate lifecycle management, and cross-domain interoperability. This phase ensures network sustainability through robust trust infrastructure maintenance.

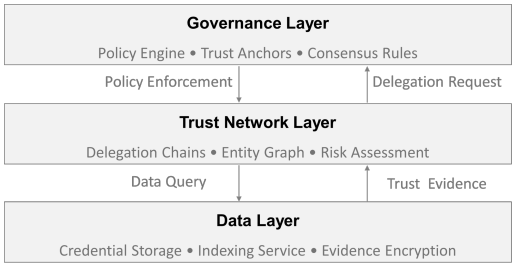


Fig. 2: Three-Layer Spatial Classification

For the spatial dimension, as illustrated in Figure 2, DTMS can be decomposed into three distinct architectural layers:

- **Data layer.** The data layer focuses on the fundamental infrastructure for credential management, including efficient mechanisms for indexing, querying, and distributing trust-related data [63]. This layer ensures data integrity, privacy preservation, and non-repudiation through cryptographic primitives and secure storage protocols.
- **Trust network layer.** The trust network layer addresses the topology and structural aspects of trust relationships. By modeling entities and their interactions as a network, this layer enables sophisticated trust evaluation and verification through graph-theoretic analysis [64], [65] and network algorithms.
- **Governance layer.** The governance layer establishes protocol specifications and consensus mechanisms that regulate network operations. This includes defining trust anchor roles, authority delegation protocols, and election procedures for administrators. The layer provides a standardized framework for decentralized trust management.

Table I presents a systematic three-by-three classification matrix that integrates temporal phases and architectural layers, enabling comprehensive analysis of DTMS solutions.

A. Trust Formation

Trust formation is a critical phase in DTMS that focuses on establishing and evaluating initial trust relationships between entities. This section examines three key approaches: Certificate Authority (CA)-based trust evaluation in maritime networks, blockchain-based PKI root management, and decentralized multi-agent PKI. These solutions demonstrate how trust can be established through hierarchical CA structures, democratic blockchain voting, and distributed agent-based systems respectively.

1) CA-Based Trust Evaluation in Maritime Networks: Wang *et al.* [16] proposed a hierarchical CA-based architecture for trust evaluation in Maritime Autonomous Surface Ship (MASS) networks. Root CAs delegate to intermediate CAs, forming CA trees, and each entity receives a certificate for secure communication.

At the trust network layer, trust is computed as $T(entity_i \rightarrow entity_j) = \lambda^{DTL(entity_j|entity_i)}$, where $\lambda \in (0, 1)$ and DTL is the shortest path to the nearest common CA. Initial trust is based on CA topology and dynamically updated through interaction behaviors.

Entities manage Inherent Trains of Trusted CAs (ITTCs), which are exchanged via gossip protocol to compute trust degrees. Results are stored on a blockchain through a trust-aware consensus. Simulations show effectiveness in isolating malicious entities and supporting cross-tree trust, though certificate updates, privacy, and scalability require further investigation.

2) Blockchain-Based PKI Root Management: Sarker *et al.* [66] proposed a Blockchain-Based Root Management (BBRM) scheme to enhance the US DOT's Security Credential Management System by improving transparency and resilience over the Elector-Based Root Management (EBRM) model. The governance layer enables democratic root CA

TABLE I: Two-dimensional Classification of Credential-based DTMS Papers

Layer	**Trust Formation**	**Trust Verification**	**Trust Management**
Governance	[66], [14]	[9], [15]	[11], [13] , [67], [68]
Trust Network	[16]	[3], [59], [69]	[70]
Data	[16], [14]	[8], [3], [9], [15], [12]	[10], [11]

control via smart contracts, where electors vote on Root Certificate (RC) operations and manage membership through Elector Certificates (ECs).

Implemented on Hyperledger Fabric, the system showed feasible performance with up to 9 electors. BBRM supports dynamicity and explainability through blockchain voting records, though privacy remains an open issue.

3) Decentralized Multi-Agent PKI: Baudet *et al.* [14] introduced MAKI (Multi-Agent Key Infrastructure), a decentralized PKI for open multi-agent systems. MAKI eliminates the need for external CAs by distributing CA responsibilities among network agents.

The governance framework allows agent self-nomination as CAs based on local CA density, with trust levels (Low/Moderate/High) derived from direct and indirect signals. MAKI extends X.509 certificates to support decentralization, and its Sybil resistance is achieved through trust limitations on newcomers [71]. While dynamic trust evaluation is supported, the absence of persistent trust evidence limits decision verifiability, and privacy and scalability remain open issues.

4) Summary: Trust formation solutions in credential-based DTMS demonstrate strong architectural foundations but share common challenges. Privacy concerns, especially around sensitive trust metadata, require further analysis. Scalability and performance evaluations are also often limited, particularly for solutions involving complex trust computations or blockchain components.

B. Trust Verification

Trust verification is a critical phase in DTMS that focuses on cryptographically validating established trust relationships. This section examines six key approaches, showing how trust can be verified through blockchain consensus, trust schemas, graph-based algorithms, cryptographic accumulators, decentralized identifiers, and hardware security modules.

1) Blockchain-Based Cross-Domain Authentication: Zhao *et al.* [9] proposed a double-layer blockchain architecture to enhance cross-domain authentication efficiency over traditional PKI systems. At the governance layer, Authentication Servers (AS) manage a consortium blockchain for verifying blockchain-based certificates, whose hashes serve as cross-domain proofs.

The data layer simplifies X.509 certificates by removing issuer and signature fields, relying on hash verification for integrity. A private blockchain manages intra-domain certificates, while the consortium chain handles cross-domain verification. Implementation on Hyperledger Fabric showed improved efficiency and scalability, though the explainability of verification decisions remains a challenge.

2) Schema-Based IoT Access Control: Nichols [15] proposed an Information-Centric Networking architecture for IoT that achieves fine-grained access control using trust schemas. Built on Named Data Networking, the system secures data directly rather than communication channels.

At the data layer, packets follow a structured naming format including capability, topic, location, and issuer. The governance layer uses Versec DSL to define verification rules for different devices. A prototype showed feasible performance across CPUs. While the architecture supports dynamic policy updates and encrypted privacy, it lacks explainability due to non-persistent trust schemas.

3) Role-Based Trust Verification: Franceschi *et al.* [3] proposed DART (Decentralized Authority Recognition with Trust), a blockchain implementation of the role-based Trust management framework. DART manages RT^0 credentials via smart contracts and implements weighted trust evaluation.

At the trust network layer, DART employs a backward search algorithm to build proof graphs for role verification, utilizing trust weights to calculate cumulative trust across credential chains. However, executing this algorithm on-chain has shown significant computational overhead on Ethereum.

To address DART's scalability issues, De Salve *et al.* [59] proposed L2DART as a layer-2 solution. L2DART moves graph computation off-chain while maintaining on-chain verification of proof paths. This hybrid approach significantly reduced gas costs while preserving auditability.

4) Anonymous Credential Authorization: Lauinger *et al.* [8] addressed credential issuer verification in Self-Sovereign Identity Management (SSIM) systems through Anonymous Proof of Authorization (A-PoA). The scheme enables Root Authorities (RA) to authorize Certificate Issuing Authorities (CIA) while preserving CIA anonymity.

At the data layer, the solution employs Rivest-Shamir-Adleman (RSA) accumulators for membership verification and Non-interactive Zero Knowledge Proof of Knowledge of Exponent (NI-ZKPoKE) for anonymous proofs. The protocol achieves O(1) verification complexity while maintaining O(n) complexity for authorization operations.

5) DID Trust: Yin *et al.* [69] proposed DidTrust, a novel decentralized identity trust verification protocol that focuses on robust trust verification while achieving privacy preservation and attack resilience. At the trust network layer, DidTrust models trust relationships through a directed graph structure

where vertices represent DID entities and edges capture trust attestations with associated feedback data. Trust values are aggregated using weighted path multiplication with configurable decay parameters to control propagation scope. Experimental results demonstrated superior attack detection rates compared to existing approaches while maintaining strong privacy guarantees through UC-secure protocols.

6) Hardware-Based Vehicle Authentication: Javaid *et al.* [12] proposed a blockchain-based authentication protocol for Internet of Vehicles (IoV) networks using Physical Unclonable Functions (PUF). The protocol leverages PUF-derived challenge-response pairs as hardware fingerprints for vehicle authentication.

At the data layer, vehicle identities combine blockchain addresses with PUF credentials [72]. Road Side Units (RSU) verify vehicles through challenge-response protocols and maintain certificates on-chain. Implementation with dynamic Proof of Work (dPoW) demonstrated 36% lower communication overhead compared to existing approaches.

7) Summary: Trust verification solutions demonstrate strong scalability support, particularly in blockchain-based approaches. Solutions at the trust network layer face dynamicity challenges, while simpler credential models generally achieve better capability coverage than graph-based approaches. Future work should address privacy preservation in trust networks and explainability of verification decisions.

C. Trust Management

Trust management focuses on maintaining and governing established trust relationships through systematic approaches. This section examines four key solutions: blockchain-based trust certification, schema-based certificate revocation, game-theoretic certificate management, and Sovereign Identity (SSI) integration. These approaches demonstrate how trust can be managed through decentralized trust networks, structured naming conventions, and behavior-based evaluation respectively.

1) Blockchain-Based Trust Certification: Chen et al. [67] propose a consortium blockchain-based DTMS featuring cross-layer trust evaluation between vehicles and RSUs, TEE-accelerated VDF consensus for efficient synchronization, and attack-resistant smart contracts for behavioral pattern analysis. More *et al.* [10] proposed a blockchain-based Web of Trust (WoT) system that enables decentralized certification of credential issuer legitimacy. The system implements a graph-based trust model where trust certifiers publish verifiable statements about issuers.

At the data layer, trust statements are structured as tuples containing: certifier identity, issuer identity, legitimacy level $LL \in [-1, 1]$, confidence level $LC \in [-1, 1]$, digital signature, and timestamp. The system maintains two key graph structures: (1) A WoT graph where vertices represent entities and edges represent trust statements; (2) A transformation graph where vertices represent credential schema URIs and edges represent schema transformation rules.

The governance framework allows dynamic trust updates and revocation via timestamp-based supersession, with certifier authority validated through the Web of Trust. Ethereum implementation demonstrated sub-second performance on 10,000-edge graphs. Recent studies [68], [70] extend this approach to cross-domain trust, though privacy remains an open issue.

2) Schema-Based Certificate Revocation: Yu *et al.* [11] introduced CertRevoke, a certificate revocation framework for Named Data Networking (NDN) that leverages structured naming conventions and trust schemas. The architecture organizes entities into trust zones, each managed by a trust anchor that issues certificates to zone members.

At the data layer, the framework defines:

- Structured naming conventions for certificates and revocation records;
- Mapping rules between certificate names and corresponding revocation records;
- Support for both issuer-initiated and owner-initiated revocation.

The governance layer enforces trust schemas that define validation rules for revocation records, while an in-network caching mechanism enhances performance by minimizing ledger interactions.

Experimental results demonstrated 45-84.5% improvement in record-checking latency with caching. The framework provides strong support for scalability and privacy while maintaining explainability through blockchain records.

3) Game-Theoretic Certificate Management: Boudagdigue *et al.* [13] proposed a cluster-based certificate management protocol for Industrial Internet of Things (IIoT) networks using game theory. Cluster Leaders (CLs) oversee member behavior and certificate lifecycles. At the governance layer, certificate revocation is modeled as a repeated signaling game between a CL with actions {revoke, update} and potentially Malicious Node (MN) with actions {normal, malicious}.

The framework calculates mixed-strategy Perfect Bayesian Equilibrium (PBE) using:

- ω_j^*: Equilibrium probability of malicious behavior;
- λ_j^*: Equilibrium probability of certificate revocation.

MATLAB simulations demonstrated accurate detection of malicious behavior across multiple scenarios. While the solution provides strong dynamicity via behavior-based evaluation, explainability is limited by a lack of parameter persistence.

4) SSI Integration: SSI represents the latest evolution in identity management, transitioning from centralized to user-centric control [73]. It empowers individuals with full authority over their digital identities and credentials [60], offering enhanced privacy, scalability, and interoperability [74].

Credential and identity management lie at the core of DTMS. Modern architectures [9], [15] employ entity identifi-

cation and credential-based trust metrics [16], as exemplified by the RT Framework [75]. SSI reinforces DTMS by offering a cryptographically sound and privacy-preserving identity infrastructure.

Conversely, DTMS addresses SSI's limitations. While SSI ensures *technical trust* through cryptographic proofs, it lacks *institutional trust* for authority validation [60]. DTMS frameworks such as [8] complement SSI with governance and authorization mechanisms. Together, SSI and DTMS form a unified foundation for decentralized identity and trust, enhancing overall system trustworthiness.

5) Summary: Trust management solutions demonstrate robust explainability support, particularly in blockchain-based approaches. However, privacy preservation during data collection and comprehensive scalability analysis remain key challenges. Future work should address these gaps while maintaining the strong dynamicity and explainability characteristics of current solutions.

IV. Credential-based DTMS Evaluation

Recent studies have proposed evaluation criteria for trust management. [29] lists factors such as subjectivity, dynamicity, context-awareness, privacy, scalability, robustness, overhead, explainability, and user acceptance. [36] highlights decentralization, simplicity, adaptability, and efficiency for IoT, while [7] addresses delegation, verification, and offline management in decentralized authorization. Based on these, we propose four evaluation dimensions for credential-based DTMS: dynamicity, explainability, privacy, and scalability.

A. Dynamicity

Trust in distributed systems is inherently dynamic, requiring mechanisms to manage its temporal evolution. This dynamicity arises from multiple factors:

- **Event-driven updates**: Trust relationships evolve continuously in response to contextual changes, emerging events, and interactions with other trust relationships. A robust DTMS must maintain trust data currency (including trust relationships, credentials, claims, and decisions) across the distributed network with minimal latency. This requires efficient event detection, propagation mechanisms, and update protocols.
- **Transactional consistency**: Trust data updates frequently involve multiple distributed entities and credentials, demanding ACID-compliant transaction management [76]. The system must guarantee atomicity to ensure all related updates succeed or fail together, consistency to maintain trust relationship validity, isolation to prevent interference between concurrent updates, and durability to persist trust state changes reliably.
- **Network dynamics**: Modern distributed systems face continuous entity churn, with participants joining and departing frequently. DTMS must handle these topology changes gracefully, including special considerations for offline participants [7]. This encompasses efficient join/leave protocols, state synchronization mechanisms, and robust recovery procedures for reconnecting entities.
- **Temporal consistency**: The system must maintain temporal consistency of trust relationships across distributed entities, implementing appropriate timestamp mechanisms, version control, and conflict resolution protocols to handle concurrent updates and ensure a coherent trust state across the network.

B. Explainability

A credential-based DTMS must provide comprehensive explainability across multiple dimensions:

- **Decision transparency**: The system should offer clear explanations for trust-driven decisions throughout the trust lifecycle, including relationship establishment, maintenance, and revocation. This encompasses both trust-specific decisions and application-level determinations such as access control, data acceptance, and entity classification. The explanation mechanism should provide both human-readable justifications and machine-processable logical derivations.
- **Trust articulation**: Despite the inherent complexity of trust quantification, DTMS must provide mechanisms to explicitly capture and communicate trust reasoning. This includes maintaining evidence records, documenting decision rationales, and implementing formal trust policies that clearly define evaluation criteria and decision procedures. The system should transform implicit trust assumptions into explicit, verifiable rules.
- **Verification and audit**: DTMS must support multi-level verification, enabling entities to validate both individual trust decisions and broader trust patterns. This requires maintaining verifiable evidence chains, implementing secure audit logging mechanisms, and supporting temporal analysis of trust evolution. Blockchain technology can provide immutable audit trails, while formal verification techniques can validate trust policy compliance.
- **Reasoning framework**: The system should implement a structured reasoning framework that combines multiple trust factors, including direct experiences, recommendations, reputation scores, and contextual parameters. This framework must support both rule-based and probabilistic reasoning, with a clear articulation of how different factors are weighted and combined in trust computations.

C. Privacy

Privacy protection in credential-based DTMS requires a comprehensive security architecture:

- **Data minimization**: Following privacy-by-design principles [77], the system must implement strict data minimization. This involves carefully defining essential trust data elements, implementing fine-grained disclosure controls, and supporting selective revelation of credentials. The system should provide mechanisms for

TABLE II: Evaluation of Credential-based DTMS Papers

Task Category	Reference	Layer Category	Dynamicity	Explainability	Privacy	Scalability
Trust Formation	[16]	TrustNet,Data	○	◉	-	-
	[66]	Govern	●	●	-	●
	[14]	Govern,Data	●	○	-	-
Trust Verification	[9]	Govern,Data	◉	-	●	●
	[15]	Govern,Data	●	○	●	●
	[3]	TrustNet,Data	○	●	○	○
	[59]	TrustNet	○	●	○	●
	[8]	Data	●	◉	●	◉
	[12]	Data	●	●	◉	●
	[69]	TrustNet,Data	◉	◉	●	◉
Trust Management	[10]	Data	●	●	○	-
	[11]	Govern,Data	-	●	●	●
	[13]	Govern	●	◉	-	-
	[67]	Govern,TrustNet	●	◉	◉	◉
	[68]	Govern,TrustNet	●	◉	◉	◉

●: Well supported; ◉: Partially supported; ○: Not supported; -: Up to further discussion;
Govern: Governance Layer; TrustNet: Trust Network Layer; Data: Data Layer

entities to control their privacy exposure levels while maintaining necessary trust functionality.

- **Privacy-preserving protocols**: Advanced cryptographic techniques, particularly ZKP [8], [29], should be employed to protect sensitive trust information. The system must support various privacy levels, from pseudonymous interactions to strongly authenticated exchanges, adapting to different use case requirements [78]. Additional techniques such as homomorphic encryption and secure multi-party computation can enable trust computations over encrypted data.
- **Attack resistance**: DTMS must incorporate robust defenses against privacy-related attacks, e.g., correlation attacks, inference attacks, and identity linking attempts [69]. This requires careful protocol design, regular security analysis, and implementation of appropriate countermeasures such as mixing networks, dummy traffic, and privacy-preserving authentication mechanisms.
- **Regulatory compliance**: The system should implement privacy controls aligned with relevant data protection regulations [79], supporting features such as data portability, right to erasure, and consent management. This includes maintaining privacy policies, implementing data lifecycle management, and providing transparency about data usage.

D. Scalability

Scalability in credential-based DTMS encompasses multiple critical aspects:

- **Performance scaling**: The system must maintain consistent performance under increasing loads, including growth in network size, event frequency, and relationship complexity [29]. This requires efficient data structures, optimized protocols, and careful resource management. The architecture should avoid centralized bottlenecks and support horizontal scaling of management functions.
- **Algorithmic efficiency**: Core trust operations (e.g., establishment, verification, revocation) must employ efficient algorithms with acceptable computational complexity. This includes optimizing graph-based trust path discovery [3], implementing efficient game-theoretic strategies [13], and minimizing cryptographic overhead [8]. Algorithm selection should consider both time and space complexity relative to network parameters.
- **Resource optimization**: The system must efficiently manage computational, storage, and network resources. This includes implementing caching strategies, compression techniques, and adaptive resource allocation. Special attention should be paid to blockchain scalability challenges [59], implementing appropriate consensus mechanisms and data management strategies.
- **Architectural scalability**: The system architecture must support seamless growth, including mechanisms for dynamic resource allocation, load balancing, and fault tolerance. This encompasses both vertical scaling (increasing individual node capacity) and horizontal scaling (adding more nodes), with appropriate consistency and synchronization protocols.

Our evaluation framework provides key advantages for assessing credential-based DTMS research through a clear three-level scale (well supported (●), partially supported (◉), not supported (○)) and four fundamental dimensions: dynamicity, explainability, privacy, and scalability. As demonstrated in Table II, we evaluate the papers from Section III, marking some aspects with "-" where further discussion is needed. This evaluation approach effectively reveals support levels across papers and identifies both achievements and areas for improvement in current research, offering valuable insights for future directions.

V. Challenges and Future Directions

This section explores the critical challenges and future research directions in DTMS. Building upon our previous discussion of DTMS architectures, trust models, and implementation approaches, we identify key areas requiring further investigation and development to enhance the robustness, scalability, and practical applicability of these systems.

A. Architectural Challenges

The architectural design of DTMS presents fundamental challenges that must be addressed for successful implementation and deployment. These challenges span multiple layers, from governance and trust network management to data handling and storage.

1) Governance Layer.: The governance layer in DTMS must balance centralized control with entity autonomy [80]–[82]. Existing systems typically adopt either strict trust schemas or fully decentralized models. A hybrid approach could enforce baseline policies while supporting entity-specific customization, enabling runtime security validation, policy consistency checks, and flexible standard evaluation. Trust anchor implementations differ across domains, such as cluster heads in IoV, root certificate authorities in PKI, and trusted third parties in privacy systems. Each presents trade-offs in scalability, security, and overhead. Selection should consider network topology, trust propagation, and verification protocols to inform future DTMS designs.

2) Trust Network Layer.: RT management and backward chain discovery mechanisms must evolve for complex scenarios. Modern applications like supply chain management involve intricate certificate hierarchies and diverse relationships, creating multi-dimensional trust graphs with heterogeneous nodes and edges. Advanced graph modeling must address relationship representation, path discovery, and trust metrics. Optimization strategies for distributed environments remain crucial areas for investigation.

3) Data Layer.: Trust graphs present significant data management challenges requiring robust architecture for efficient operations and data integrity. ZKP protocols enable selective information disclosure for trust verification, while advanced indexing optimizes graph operations. Blockchain adoption as a data layer requires research in storage optimization, cost-effective management, and efficient query processing.

B. Implementation Challenges

The practical implementation of DTMS faces several technical challenges related to the adoption of emerging technologies such as blockchain and decentralized identifiers. These challenges require innovative solutions to ensure system efficiency, scalability, and security.

1) Using Blockchain (transactional update): Blockchain technology, while providing immutable audit trails for trust evolution, presents significant challenges in managing dynamic trust relationships. Several architectural approaches address these challenges:

- **State channels**: Facilitate efficient off-chain certificate updates while maintaining on-chain verification integrity, significantly reducing transaction costs and latency (e.g., MASS network implementation [79]);
- **Sharding**: Enhance system throughput through parallel processing of cross-domain authentication tasks, improving scalability in large-scale deployments (e.g., [83] double-layer architectural model);
- **Pruning mechanisms**: Implement data retention policies to manage storage overhead while preserving essential trust history (e.g., certificate revocation);
- **Consensus optimization**: Develop specialized consensus protocols that balance security requirements with performance demands in trust management.

The integration of hybrid architectures, combining blockchain's immutability with traditional distributed databases' performance characteristics, offers promising solutions for optimizing system performance while maintaining trust guarantees.

2) Using DID/VC: Decentralized Identifiers (DID) and Verifiable Credentials (VC) introduce revolutionary approaches to identity and trust management:

- **Cross-system interoperability**: DID's standardized URI format enables seamless entity identification across diverse domains, facilitating unified trust frameworks (cf. [84] IoT naming convention);
- **Selective disclosure**: Advanced ZKP-based VC implementations support granular privacy control in trust verification processes (cf. DART framework [3]);
- **Lifecycle management**: Sophisticated mechanisms for managing dynamic relationships between DIDs and trust anchors, including anchor rotation and credential updates (e.g., BBRM's RCA election [66]);
- **Resolution efficiency**: Optimization of DID solutions to minimize latency in large-scale networks.

Key challenges include optimizing DID document synchronization, developing efficient VC revocation for large-scale deployments, and establishing standardized interoperability across diverse DID systems.

VI. Conclusion

This survey presents a comprehensive review of DTMS, covering fundamental concepts, key components, and emerging applications. We analyzed trust models, consensus mechanisms, and security frameworks that underpin DTMS, emphasizing their significance in modern digital ecosystems.

We demonstrated DTMS's vital role in facilitating trusted decentralized interactions, especially in blockchain and peer-to-peer systems. While identifying challenges like scalability and privacy, we explored potential solutions for advancing decentralized trust management. This work provides researchers and practitioners with a structured reference for developing secure decentralized systems.

REFERENCES

[1] C. A. Ardagna, E. Damiani, S. D. C. D. Vimercati, S. Foresti, and P. Samarati, "Trust management," *Security, Privacy, and Trust in Modern Data Management*, 2007. [Online]. Available: http://www.springerlink.com/content/q1152r71g523np74/fulltext.pdf

[2] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management." IEEE Comput. Soc. Press, 1996, pp. 164–173. [Online]. Available: http://ieeexplore.ieee.org/document/502679/

[3] L. Franceschi, A. Lisi, A. D. Salve, P. Mori, and L. Ricci, "Dart: Towards a role-based trust management system on blockchain." IEEE, 10 2021, pp. 75–80. [Online]. Available: https://ieeexplore.ieee.org/document/9680566/

[4] L. Opiola, L. Dutka, R. G. Slota, and J. Kitowski, "Trust-driven, decentralized data access control for open network of autonomous data providers." IEEE, 8 2018, pp. 1–10.

[5] L. Wei, J. Wu, and C. Long, "Blockchain-enabled trust management in service-oriented internet of things: Opportunities and challenges." ACM, 3 2021, pp. 90–95.

[6] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 485–498, 2017.

[7] "Wave: A decentralized authorization framework with transitive delegation," 2019. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/andersen

[8] J. Lauinger, J. Ernstberger, E. Regnath, M. Hamad, and S. Steinhorst, "A-poa: Anonymous proof of authorization for decentralized identity management." IEEE, 5 2021, pp. 1–9.

[9] G. Zhao, B. Di, and H. He, "A novel decentralized cross-domain identity authentication protocol based on blockchain," *Transactions on Emerging Telecommunications Technologies*, vol. 33, 2022.

[10] S. More, P. Grassberger, F. Hörandner, A. Abraham, and L. D. Klausner, "Trust me if you can: Trusted transformation between (json) schemas to support global authentication of education credentials," 2021, pp. 19–35.

[11] T. Yu, H. Xie, S. Liu, X. Ma, X. Jia, and L. Zhang, "Certrevoke: A certificate revocation framework for named data networking," 2022, pp. 80–90.

[12] U. Javaid, M. N. Aman, and B. Sikdar, "A scalable protocol for driving trust management in internet of vehicles with blockchain," *IEEE Internet of Things Journal*, vol. 7, pp. 11 815–11 829, 12 2020.

[13] C. Boudagdigue, A. Benslimane, and A. Kobbane, "Cluster-based certificate revocation in industrial iot networks using signaling game." Institute of Electrical and Electronics Engineers Inc., 12 2020.

[14] A. Baudet, O.-E.-K. Aktouf, A. Mercier, and P. Elbaz-Vincent, "Decentralized public key infrastructure for autonomous embedded systems," 2022. [Online]. Available: http://ceur-ws.org

[15] K. Nichols, "Trust schemas and icn: Key to secure home iot." Association for Computing Machinery, Inc, 9 2021, pp. 95–106.

[16] Y. Wang, P. Chen, B. Wu, C. Wan, and Z. Yang, "A trustable architecture over blockchain to facilitate maritime administration for mass systems," *Reliability Engineering and System Safety*, vol. 219, 2022.

[17] W. Li, W. Meng, and L. F. Kwok, "Surveying trust-based collaborative intrusion detection: State-of-the-art, challenges and future directions," *IEEE Communications Surveys & Tutorials*, vol. 24, pp. 280–305, 2022.

[18] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1200–1210, 2014.

[19] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "Sectrust-rpl: A secure trust-aware rpl routing protocol for internet of things," *Future Generation Computer Systems*, vol. 93, pp. 860–876, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X17306581

[20] E. J. Chang, F. K. Hussain, and T. S. Dillon, "Fuzzy nature of trust and dynamic trust modeling in service oriented environments." ACM, 11 2005, pp. 75–83.

[21] K. A. Awan, I. U. Din, M. Zareei, M. Talha, M. Guizani, and S. U. Jadoon, "Holitrust-a holistic cross-domain trust management mechanism for service-centric internet of things," *IEEE Access*, vol. 7, pp. 52 191–52 201, 2019.

[22] T. Wang, L. Qiu, A. K. Sangaiah, G. Xu, and A. Liu, "Energy-efficient and trustworthy data collection protocol based on mobile fog computing in internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3531–3539, 2020.

[23] Q. Cui, Z. Zhu, W. Ni, X. Tao, and P. Zhang, "Edge-intelligence-empowered, unified authentication and trust evaluation for heterogeneous beyond 5g systems," *IEEE Wireless Communications*, vol. 28, no. 2, pp. 78–85, 2021.

[24] J. . Cho, A. Swami, and I. . Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 562–583, 2011, cited By :494. [Online]. Available: www.scopus.com

[25] M. Bampatsikos, I. Politis, C. Xenakis, and S. C. A. Thomopoulos, "Solving the cold start problem in trust management in iot," in *ACM International Conference Proceeding Series*, 2021. [Online]. Available: www.scopus.com

[26] X. Fan, L. Liu, R. Zhang, Q. Jing, and J. Bi, "Decentralized trust management," *ACM Computing Surveys*, vol. 53, pp. 1–33, 1 2021.

[27] V. Thummala and J. S. Chase, "SAFE: A declarative trust management system with linked credentials," *CoRR*, vol. abs/1510.04629, 2015. [Online]. Available: http://arxiv.org/abs/1510.04629

[28] I. . Chen, J. Guo, D. . Wang, J. J. P. Tsai, H. Al-Hamadi, and I. You, "Trust-based service management for mobile cloud iot systems," *IEEE Transactions on Network and Service Management*, vol. 16, no. 1, pp. 246–263, 2019, cited By :54. [Online]. Available: www.scopus.com

[29] J. Wang, Z. Yan, H. Wang, T. Li, and W. Pedrycz, "A survey on trust models in heterogeneous networks," *IEEE Communications Surveys & Tutorials*, vol. 24, pp. 2127–2162, 2022.

[30] B. Cao, Z. Wang, L. Zhang, D. Feng, M. Peng, L. Zhang, and Z. Han, "Blockchain systems, technologies, and applications: A methodology perspective," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 353–385, 2022.

[31] W. Liu, B. Cao, M. Peng, and B. Li, "Distributed and parallel blockchain: Towards a multi-chain system with enhanced security," *IEEE Transactions on Dependable and Secure Computing*, 2024.

[32] Q. Wang, R. Li, Q. Wang, S. Chen, M. Ryan, and T. Hardjono, "Exploring Web3 from the view of blockchain," *arXiv preprint arXiv:2206.08821*, 2022.

[33] W. Liu, B. Cao, and M. Peng, "Web3 technologies: Challenges and opportunities," *IEEE Network*, vol. 38, no. 3, pp. 187–193, 2023.

[34] H. Li and M. Singhal, "Trust management in distributed systems," *Computer*, vol. 40, pp. 45–53, 2 2007.

[35] S. Sagar, A. Mahmood, J. Kumar, and Q. Z. Sheng, "A time-aware similarity-based trust computational model for social internet of things." IEEE, 12 2020, pp. 1–6.

[36] M. Ebrahimi, M. H. Tadayon, M. S. Haghighi, and A. Jolfaei, "A quantitative comparative study of data-oriented trust management schemes in internet of things," *ACM Transactions on Management Information Systems*, vol. 13, pp. 1–30, 9 2022.

[37] I. Pranata, G. Skinner, and R. I. Athauda, "A holistic review on trust and reputation management systems for digital environments," 2012.

[38] C. D. Jensen, "The importance of trust in computer security," 2014, pp. 1–12.

[39] R. Rivest and B. Lampson, "Sdsi – a simple distributed security infrastructure," *See the SDSI web page at http://theory.lcs.mit.edu/ cis/sdsi.html*, 08 1996.

[40] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen, "Spki certificate theory," *RFC*, vol. 2693, 09 1999.

[41] Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the internet of things: A context-aware and multi-service approach," *Computers & Security*, vol. 39, pp. 351–365, 11 2013.

[42] S. E. A. Rafey, A. Abdel-Hamid, and M. A. El-Nasr, "Cbstm-iot: Context-based social trust model for the internet of things." IEEE, 4 2016, pp. 1–8.

[43] Z. Lin and L. Dong, "Clarifying trust in social internet of things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, pp. 234–248, 2 2018.

[44] J.-H. Cho, K. Chan, and S. Adali, "A survey on trust modeling," *ACM Computing Surveys*, vol. 48, pp. 1–40, 11 2015.

[45] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X. 509 internet public key infrastructure online certificate status protocol-ocsp," Tech. Rep., 1999.

[46] S. Huang, Z. Zeng, K. Ota, M. Dong, T. Wang, and N. N. Xiong, "An intelligent collaboration trust interconnections system for mobile information control in ubiquitous 5g networks," *IEEE Transactions on Network Science and Engineering*, vol. 8, pp. 347–365, 1 2021.

[47] I.-R. Chen, F. Bao, and J. Guo, "Trust-based service management for social internet of things systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, pp. 684–696, 11 2016.

[48] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, pp. 618–644, 3 2007.

[49] A. I. A. Ahmed, S. H. A. Hamid, A. Gani, S. khan, and M. K. Khan, "Trust and reputation for internet of things: Fundamentals, taxonomy, and open research challenges," *Journal of Network and Computer Applications*, vol. 145, p. 102409, 11 2019.

[50] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "Trm-iot: A trust management model based on fuzzy reputation for internet of things," *Comput. Sci. Inf. Syst.*, vol. 8, pp. 1207–1228, 2011.

[51] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007, emerging Issues in Collaborative Commerce. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167923605000849

[52] S. Ayed, A. Hbaieb, and L. Chaari, "Blockchain and trust-based clustering scheme for the iov," *Ad Hoc Networks*, vol. 142, p. 103093, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870523000136

[53] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, 2004.

[54] Y. Lu, X. Fan, and Q. Jing, "Taeffect: Quantifying interaction risks in trust-enabled communication systems," *International Journal of Communication Systems*, 2022.

[55] X. Fan, L. Liu, M. Li, and Z. Su, "Grouptrust: Dependable trust management," *IEEE Transactions on Parallel and Distributed Systems*, vol. PP, pp. 1–1, 09 2016.

[56] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th International Conference on World Wide Web*, ser. WWW '03. New York, NY, USA: Association for Computing Machinery, 2003, p. 640–651. [Online]. Available: https://doi.org/10.1145/775152.775242

[57] N. Li, B. N. Grosof, and J. Feigenbaum, "Delegation logic: A logic-based approach to distributed authorization," *ACM Trans. Inf. Syst. Secur.*, vol. 6, no. 1, p. 128–171, feb 2003. [Online]. Available: https://doi.org/10.1145/605434.605438

[58] P. Podder and A. Afanasyev, "On improving versatility of versec trust schema," in *Proceedings of the 9th ACM Conference on Information-Centric Networking*, 2022.

[59] A. D. Salve, L. Franceschi, A. Lisi, P. Mori, and L. Ricci, "L2dart: A trust management system integrating blockchain and off-chain computation," *ACM Transactions on Internet Technology*, 2 2022.

[60] I. Jeyakumar, D. Chadwick, and M. Kubach, "A novel approach to establish trust in verifiable credential issuers in self-sovereign identity ecosystems using train," vol. P-325, 2022, pp. 27–38.

[61] M. Davie, D. Gisolfi, D. Hardman, J. Jordan, D. O'Donnell, and D. Reed, "The trust over ip stack," *IEEE Communications Standards Magazine*, vol. 3, pp. 46–51, 12 2019.

[62] J. Guo, I. R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in internet of things systems," *Computer Communications*, vol. 97, pp. 1–14, 1 2017.

[63] T. L. Nguyen, L. Nguyen, T. Hoang, D. Bandara, Q. Wang, Q. Lu, X. Xu, L. Zhu, and S. Chen, "Blockchain-empowered trustworthy data sharing: Fundamentals, applications, and challenges," *ACM Computing Surveys*, vol. 57, no. 8, pp. 1–36, 2025.

[64] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng, and J. Yu, "Direct acyclic graph-based ledger for internet of things: Performance and security analysis," *IEEE/ACM Transactions on Networking*, vol. 28, no. 4, pp. 1643–1656, 2020.

[65] Q. Wang, J. Yu, S. Chen, and Y. Xiang, "Sok: DAG-based blockchain systems," *ACM Computing Surveys*, vol. 55, no. 12, pp. 1–38, 2023.

[66] A. Sarker, S. Byun, W. Fan, and S.-Y. Chang, "Blockchain-based root of trust management in security credential management system for vehicular communications." ACM, 3 2021, pp. 223–231.

[67] C. Gu, B. Ma, and D. Hu, "A dependable and efficient decentralized trust management system based on consortium blockchain for intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 12, pp. 19 430–19 443, 2024.

[68] X. Xiang, J. Cao, W. Fan, S. Xiang, and G. Wang, "Blockchain enabled dynamic trust management method for the internet of medical things," *Decision Support Systems*, vol. 180, p. 114184, 2024.

[69] J. Yin, Y. Xiao, J. Feng, M. Yang, Q. Pei, and X. Yi, "Didtrust: Privacy-preserving trust management for decentralized identity," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–16, 2024.

[70] L. Shi, T. Wang, Z. Xiong, Z. Wang, Y. Liu, and J. Li, "Blockchain-aided decentralized trust management of edge computing: Toward reliable off-chain and on-chain trust," *IEEE Network*, vol. 38, no. 5, pp. 182–188, 2024.

[71] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, and W. Shi, "Cecoin: A decentralized pki mitigating mitm attacks," *Future Generation Computer Systems*, vol. 107, pp. 805–815, 2020.

[72] M. AlMarshoud, M. Sabir Kiraz, and A. H. Al-Bayatti, "Security, privacy, and decentralized trust management in vanets: A review of current research and future directions," *ACM Comput. Surv.*, vol. 56, no. 10, Jun. 2024. [Online]. Available: https://doi-org.ezproxy.lib.uts.edu.au/10.1145/3656166

[73] C. Allen, "The path to self-sovereign identity," Apr 2016, accessed: 2023-03-16. [Online]. Available: https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md

[74] G. Wang, Q. Wang, and S. Chen, "Exploring blockchains interoperability: A systematic survey," *ACM Computing Surveys*, vol. 55, no. 13s, pp. 1–38, 2023.

[75] N. Li, J. C. Mitchell, and W. H. Winsborough, "Design of a role-based trust-management framework," vol. 2002-January. Institute of Electrical and Electronics Engineers Inc., 2002, pp. 114–130.

[76] S. Yu, "Acid properties in distributed databases," *Advanced eBusiness Transactions for B2B-Collaborations*, 2009.

[77] A. Cavoukian, "Privacy by design," 2011, accessed: 2023-03-26. [Online]. Available: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

[78] "Spectrum of privacy," 3 2022, accessed: 2023-03-26. [Online]. Available: https://www.w3.org/TR/vc-data-model/#spectrum-of-privacy

[79] M. Issa, A. Ilinca, H. Ibrahim, and P. Rizk, "Maritime autonomous surface ships: Problems and challenges facing the regulatory process," *Sustainability*, vol. 14, no. 23, p. 15630, 2022.

[80] Q. Wang, G. Yu, Y. Sai, C. Sun, L. D. Nguyen, and S. Chen, "Understanding DAOs: An empirical study on governance dynamics," *IEEE Transactions on Computational Social Systems*, 2025.

[81] G. Yu, Q. Wang, T. Bi, S. Chen, and X. Xu, "Leveraging architectural approaches in web3 applications-a dao perspective focused," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2023, pp. 1–6.

[82] C. Tang, Q. Cai, C. Dong, Q. Wang, and S. Chen, "Decentralised autonomous organizations (DAOs): An exploratory survey," *Distributed Ledger Technologies: Research and Practice*, 2025.

[83] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu, "Survey: Sharding in blockchains," *IEEE Access*, vol. 8, pp. 14 155–14 181, 2020.

[84] G. Yu, X. Wang, and R. P. Liu, "Cross-chain between a parent chain and multiple side chains," 2023. [Online]. Available: https://arxiv.org/abs/2208.05125