Review

A Review on Blockchain-Based Trust & Reputation Schemes in Metaverse Environments

Firdous Kausar *, Hafiz M. Asif, Sajid Hussain, Shahid Mumtaz

Posted Date: 15 October 2025

doi: 10.20944/preprints202510.1172.v1

Keywords: Metaverse; blockchain; reputation; trust management; gaming; digital real estate; healthcare; education; NFT; challenges

Review

A Review on Blockchain-based Trust & Reputation Schemes in Metaverse Environments

Firdous Kausar [1,*], Hafiz M. Asif [2], Sajid Hussain [1] and Shahid Mumtaz [3]

[1] Department of Computer Science and Data Science, School of Applied Computational Sciences, Meharry Medical College, Nashville, TN 37208, USA
[2] Department of Electrical and Computer Engineering, College of Engineering, Sultan Qaboos University, Muscat 123, Oman
[3] Digital Innovation, Computer Science, Nottingham Trent University (NTU), Nottingham NG1 4FQ, UK
[*] Correspondence: firdous.kausar@mmc.edu

Abstract

The metaverse represents a transformative integration of virtual and physical worlds, bringing unprecedented opportunities for social interaction, commerce, education, healthcare, and entertainment. Establishing trust in these expansive and decentralized environments remains a critical challenge. Blockchain technology, with its decentralized, secure, and immutable nature, is emerging as an essential pillar of trust and digital asset ownership within the metaverse. This paper provides an extensive review of blockchain-enabled trust and reputation frameworks specifically tailored to metaverse ecosystems. We present an in-depth analysis of existing blockchain solutions across diverse metaverse domains, including gaming, virtual real estate, healthcare, and education. Our core contributions include a comprehensive taxonomy that classifies current trust and reputation schemes by their underlying mechanisms, threat models addressed, and their architectural strategies. We provide a comparative benchmark analysis evaluating key performance metrics such as security robustness, scalability, user privacy, and cross-platform interoperability, revealing critical trade-offs inherent in current designs. Our analysis finds that score-based designs trade scalability for nuanced reputation representation, while SSI and SBT-based approaches improve Sybil-resistance but introduce significant privacy governance challenges. Finally, we outline unresolved research challenges, including cross-platform reputation portability, privacy-preserving computation, real-time trust management, and standardized governance structures.

Keywords: Metaverse; blockchain; reputation; trust management, gaming; digital real estate; healthcare; education; NFT; challenges

1. Introduction

The metaverse – a convergence of AR/VR, IoT, AI, and web3 – promises immersive digital worlds, but establishing trust in these decentralized, user-driven environments is a core challenge [1]. Traditional platforms like Roblox and Horizon Worlds rely on centralized moderation and user reports to manage trust, whereas open metaverse platforms e.g. Decentraland [2], The Sandbox [3] aspire to decentralize governance and reputation. Blockchain technology is envisioned as a "pillar of trust" for secure metaverse interactions, offering transparent and tamper-proof records. However, researchers caution that current blockchain solutions face limitations e.g. reliance on centralized name services, lack of data authentication, and scalability issues, when applied to metaverse trust. This survey provides a comprehensive overview of blockchain-based trust and reputation mechanisms in the metaverse context, spanning permissionless public chains and permissioned consortium chains. We cover leading metaverse platforms and academic proposals, developing a taxonomy of approaches and benchmarking their security, scalability, privacy, and interoperability.

Online reputation systems have long been used in e-commerce and gaming, but the metaverse introduces new scale and adversary models. For instance, the Decentraland community has discussed a reputation system to encourage user participation and aid governance, envisioning a multi-dimensional reputation "vector" derived from on-chain activities such as owning assets, DAO voting, content creation, etc. Such proposals emphasize that reputation should empower community trust without becoming an exclusionary "social credit" system . The Metaverse Standards Forum (MSF) has also highlighted the need for "Unified Reputation" that is decentralized, transparent, and portable across platforms [4]. In their 2025 use-case draft, reputation data from user behavior and cross-platform feedback would travel with users' avatars, enhancing trust and informed decision-making in interconnected metaverses. These indicate a strong demand for blockchain-enabled reputation frameworks that can operate across multiple virtual worlds. On the industry side, companies are exploring reputation tokens and soulbound tokens to represent trust e.g. ERC-20 or ERC-721 tokens that quantify user contributions [**?**]. The Web3 community also experiments with decentralized social graphs that include reputation facets, which could extend to metaverse avatars [5].

Blockchain technology is widely regarded as a cornerstone for trust in Web3 and the metaverse [6,7]. Blockchains provide tamper-proof ledgers and self-executing smart contracts that can record reputation scores or issue trust tokens [8,9]. For example, non-fungible tokens (NFTs) have created digital asset economies, but they lack a notion of persistent user reputation. Emerging proposals like soulbound tokens(SBTs) aim to represent personal credentials and reputation as non-transferable tokens bound to a user's identity, establishing provenance and credibility in an anonymous world [**?**]. At the same time, blockchain-based reputation systems face limitations: on-chain operations can be transparent but slow or costly, and current implementations often still rely on centralized components for user identity or content moderation. Ensuring scalability, privacy, and interoperability of trust across diverse virtual platforms remains an open challenge [10–13].

In this survey, we provide a comprehensive review of blockchain-based trust and reputation mechanisms for metaverse environments. We cover both permissionless public blockchains and permissioned or consortium ledgers applied to metaverse use cases. We examine academic proposals, industry whitepapers, and technical reports that introduce trust frameworks tailored to virtual worlds including platforms like Decentraland, The Sandbox, Roblox, Horizon Worlds, Spatial.io, etc. Key contributions of this paper include:

- An integrated overview of all relevant works proposing metaverse trust/reputation mechanisms. We summarize each scheme's design, including token-based vs. score-based approaches, and highlight how they handle threats like Sybil attacks, collusion, whitewashing, etc.
- A taxonomy classifying these schemes along multiple dimensions – the underlying mechanism, the threat models addressed, and the architecture.
- A comparative evaluation of the surveyed schemes on key criteria including security, scalability, user privacy, and interoperability. We include comparative tables and charts that compile quantitative results reported in the literature. This analysis reveals trade-offs between approaches.
- An outlook on unresolved issues and research directions for metaverse trust systems. We identify gaps such as cross-platform reputation portability, privacy-preserving reputation computations, standardizing trust tokens/credentials, decentralized governance of reputation, and real-time trust updates. We illustrate these challenges and link each to potential solutions or ongoing efforts.

By consolidating findings across studies, this survey aims to guide researchers and practitioners in understanding the state-of-the-art and charting the path forward for trustworthy metaverse ecosystems.

2. Blockchain Integration in the Metaverse

At the center of today's metaverse endeavors is blockchain technology. It is what makes the virtual realms real in terms of what we think of as ownership, identity, and value. This section walks through the technical architecture making this possible, scrutinizes the leading real-world deployments, and spells out the solid benefits users and developers are already experiencing.

2.1. Architecture of Blockchain-Enabled Metaverse

Typically, a multi-layer architecture underpins metaverse systems based on blockchain. Figure 1 illustrates a typical layered metaverse architecture: user devices connect to cloud or edge servers, which run the virtual environments and manage the logic, using high-speed networks. These devices include VR/AR headsets, PCs, and smartphones. The platform layer usually contains the blockchain nodes and the relevant APIs; here is where the decentralized ledger and smart contracts safely process transactions and manage the assets. After the platform layer comes the application layer, which is responsible for delivering the interfaces for games, social platforms, marketplaces, or educational services.

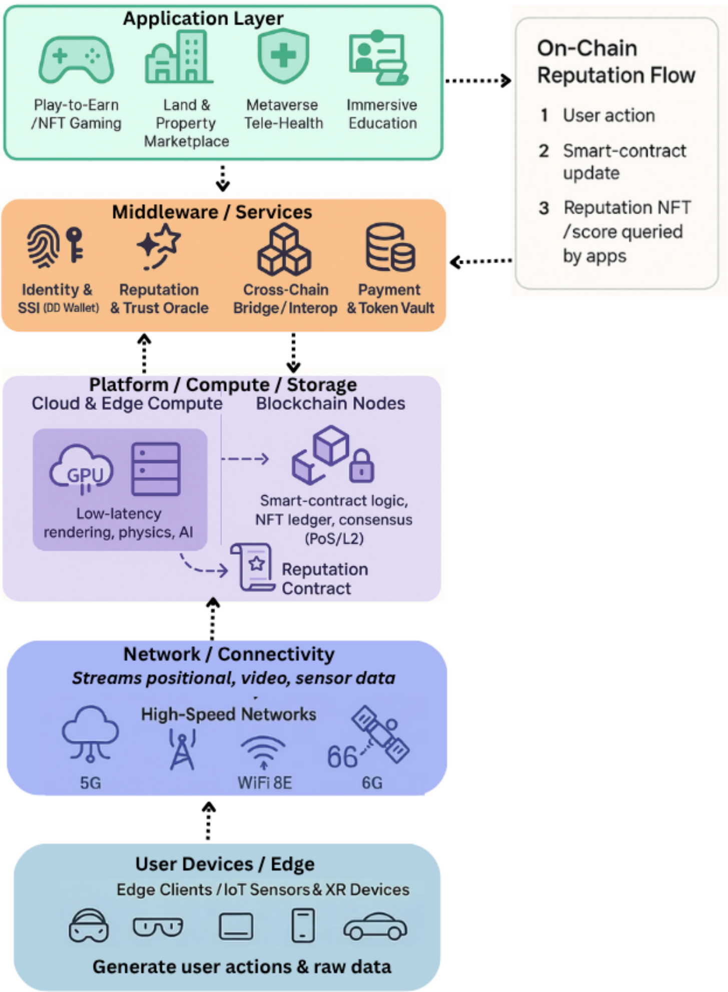
Application Layer
Play-to-Earn /NFT Gaming
Land & Property Marketplace
Metaverse Tele-Health
Immersive Education
On-Chain Reputation Flow
1 User action
2 Smart-contract update
3 Reputation NFT /score queried by apps
Middleware / Services
Identity & SSI (DD Wallet)
Reputation & Trust Oracle
Cross-Chain Bridge/Interop
Payment & Token Vault
Platform / Compute / Storage
Cloud & Edge Compute
Blockchain Nodes
GPU
Low-latency rendering, physics, AI
Smart-contract logic, NFT ledger, consensus (PoS/L2)
Reputation Contract
Network / Connectivity
Streams positional, video, sensor data
High-Speed Networks
5G
WiFi 8E
66
6G
User Devices / Edge
Edge Clients / IoT Sensors & XR Devices
Generate user actions & raw data

Figure 1. Layered Architecture of a Blockchain-Enabled Metaverse.

Edge and cloud components provide scalability, the network layer handles user-device communication, and the blockchain platform layer delivers tamper resistant data storage and contract execution. Xu et al. propose a trustless metaverse architecture using a hypergraph model: groups of users form hyperedges with trust scores, and an On-Demand Trusted Computing Environment (OTCE) allocates sandboxed resources dynamically based on trust [14]. In this model, blockchain maintains transparency of resource use and supports secure on-demand execution. In general, blockchain integration yields immutability and auditability of metaverse state as shown in Figure 1, while smart contracts enable decentralized control over assets and interactions.

Blockchain platforms differ in consensus mechanism, throughput, and security. Early PoW chains (Bitcoin) are robust but slow (7 TPS) and energy-intensive; modern blockchains (Ethereum 2.0, Polkadot, Solana) use PoS or other protocols to increase throughput. Throughput has been improving (some systems aim for tens of thousands of transactions per second), but a recent study notes that even 100k TPS is still accompanied by high deployment costs and complex cross-chain bridges [14]. L2 solutions (sidechains, roll-ups, dedicated game blockchains like Ronin) are emerging to handle gaming/metaverse scale.

For example, Axie Infinity [15] uses the Ronin sidechain [16] to lower costs, and projects like Flow or Immutable X [17,18] adopt novel protocols for NFT-heavy applications. Generally, blockchain consensus must balance decentralization, security, and performance – a known "trilemma" – which is an ongoing research area in metaverse settings [19].

2.2. Current Applications and Case Studies

This section examines real-world metaverse use cases that leverage blockchain.

- **Gaming Metaverses:** Many metaverse games are built on blockchain[20]. Decentraland is a virtual world where land plots are ERC-721 NFTs on Ethereum. Each "LAND" is an NFT minted by burning the MANA token [21]. Ownership is fully on-chain, and a decentralized marketplace allows buying/selling parcels. Sandbox is another voxel-based metaverse on Ethereum: users create 3D objects (via VoxEdit) as NFTs stored on IPFS, and trade them in a marketplace using the SAND ERC-20 token. The Sandbox also uses The Graph (an L2 indexer) for scalability. The Axie Infinity ecosystem (creaturebattling game) uses the Ronin sidechain to reduce Ethereum gas fees; players earn NFTs (Axies) and utility tokens (AXS, SLP) through gameplay. These platforms demonstrate blockchain's value in games: guaranteeing true digital ownership, enabling player-driven economies, and securing scarce virtual goods[22].
- **Virtual Real Estate:** Metaverse worlds often have properties that mirror real estate [23]. Gadekallu et al. note that metaverse virtual land is treated as a scarce asset: "virtual land. . . is offered at auction and traded as NFTs" [21]. Platforms like Decentraland and The Sandbox regularly auction parcels, and secondary sales occur via smart-contract markets [2,3]. This NFT-based ownership provides provenance and transferability of virtual real estate. Companies are exploring commercial use of virtual land (e.g. virtual offices, retail in metaverse malls), all leveraging blockchain for transparent transactions.
- **Healthcare:** Blockchain in metaverse-enabled healthcare can secure patient data and digital health assets. For instance, patient records or VR-based therapy sessions could be anchored on a blockchain to ensure immutability and access control. Surveys by Wang et al. highlight that blockchain "ensures secure, immutable record-keeping" and gives patients control via cryptographic keys [24]. Ali et al. propose a metaverse health platform with Explainable AI where blockchain "provides data security for patients while enabling transparency, traceability, and immutability" of medical information [25]. Use cases include virtual hospitals, telehealth with encrypted records, and medical research data sharing under patient consent. By integrating blockchain, healthcare metaverses can protect privacy through encryption and access logs and comply with data regulations.
- **Education:** The educational metaverse benefits from blockchain by validating credentials and enabling novel learning economies. Karunarathne et al. observe that blockchain-metaverse integration revolutionizes education by "securely storing student records" and enabling immersive, virtual learning experiences [26]. For example, universities could issue diplomas or certificates as verifiable blockchain tokens within an educational VR world. Decentralized IDs on blockchain could manage access to virtual labs or collaborative simulations. Projects like Learning Economy and blockchain-based MOOC platforms already explore these ideas. Overall, blockchain can support trust in academic records and micro-credentialing in virtual campuses.
- **Other Domains:** Blockchain-metaverse applications also appear in industry and commerce. In supply-chain-oriented metaverses, digital twins of factories can be anchored to blockchains for traceability. In retail, brands are opening virtual stores on metaverse platforms, selling blockchain

certified goods (e.g. luxury NFTs) to users. While beyond the four focal domains, these cases underline blockchain's broad metaverse potential.

2.3. Benefits of Blockchain in Metaverse

Blockchain brings several key advantages to metaverse systems:

- **Data Integrity and Security:** By design, blockchain provides tamper-resistant records. Transactions and asset histories are immutable and replicated across nodes, ensuring that no data can be altered without consensus . For sensitive data (medical records, identity details), blockchain encryption and consensus give users "complete control of their data". Decentralized storage also reduces single points of failure.
- **Trust and Transparency:** In open metaverse economies, trust among participants is crucial. Smart contracts enforce rules transparently (e.g. fair auctions, loot generation) without needing intermediaries. As Ali et al. note, blockchain enables transparency and traceability in healthcare transactions , and more generally assures all stakeholders of system integrity. Public ledgers let anyone audit digital asset provenance.
- **Digital Ownership (NFTs and Tokens):** Blockchain makes digital scarcity possible. Non-fungible tokens (NFTs) represent unique virtual items (land, art, avatars). Users have provable ownership and can trade these assets on-chain . This creates novel economic opportunities: for example, players in The Sandbox truly own and can sell their creations, rather than renting them from a company. Tokenized economies (ERC-20/721 tokens) allow in-world currency (e.g. MANA, SAND) and novel finance (staking, DAOs) as part of the metaverse.
- **Decentralization and Resilience:** Unlike centralized servers, blockchain-based metaverses do not rely on a single authority. This can improve uptime and censorship-resistance; virtual property rights persist even if one company shuts down. Interoperability protocols (cross-chain bridges) can allow users to move assets between different metaverses . Decentralization also means collaborative governance (DAOs) can emerge for virtual communities.
- **Automated Enforcement (Smart Contracts):** Business logic on blockchain via smart contracts automates complex interactions. For example, royalties on NFT resale can be coded so creators always earn a percentage. In education, smart contracts could automatically unlock course content upon payment or credential verification. These programmable agreements reduce overhead and ensure rules are executed as intended.

3. PRISMA Flow of Study Selection

We performed a comprehensive search in IEEE Xplore, ACM Digital Library, ScienceDirect, and Scopus for publications from year 2020–2025. The search keywords were set to "blockchain" AND "metaverse" AND ("trust" OR "reputation"). This yielded approximately 1758 total records. Searches across multiple databases resulted in overlapping results and 828 duplicate entries were removed. This left 930 unique records to screen. We screened 930 unique articles by title and abstract. We excluded 820 articles at this stage for failing to meet inclusion criteria. Common reasons for exclusion included: the work was not actually about blockchain-based trust/reputation in metaverse contexts e.g., it dealt only with blockchain performance or metaverse applications without trust, or it was not a research paper. This rigorous filtering left 110 articles that appeared potentially eligible for full-text review. We retrieved and assessed 110 full-text articles. At this stage, 87 studies were excluded after in-depth evaluation. Reasons for full-text exclusion included: the article did not specifically propose or evaluate a trust/reputation mechanism even if the title/abstract seemed relevant, lack of sufficient technical details or empirical evaluation, or other scope misalignment, e.g., a broad survey that mentioned trust only in passing. In some cases, papers were excluded for quality concerns or incomplete data. In the end 23 studies were included in the core analysis of the review.

Table 1. PRISMA flow of study selection (2020–2025).

PRISMA stage	Records (n)	Notes
Identification: total records from all databases	1,758	IEEE, ACM, ScienceDirect, Scopus (2020–2025); search: *blockchain & metaverse & (trust OR reputation)*
Duplicates removed	828	∼50% overlap across databases
Records after de-duplication (screened)	930	Title/abstract screening pool
Records excluded at title/abstract stage	820	Off-topic, language, or format filters
Full-text articles assessed for eligibility	110	Downloaded and reviewed in full
Full-text articles excluded	87	No trust mechanism; not metaverse-relevant; not blockchain-relevant; insufficient detail; non–peer-reviewed; duplicate concept
Studies included in qualitative synthesis	**23**	**Papers analyzed in Tables 1–4**

4. Related Work

4.1. Blockchain-Enabled Reputation Systems for Metaverse Platforms

Early research on decentralized reputation systems provides the foundation for metaverse trust management. Awan et al.[27] propose a blockchain-based trust management system for metaverse avatars and organizations. Their model assigns each virtual entity a trust score based on observed behaviors and the reputation of associated entities, dynamically weighted and stored on-chain. By leveraging smart contracts as "trust regulators," the system mitigates common reputation attacks – it explicitly counters Sybil attacks, bad-mouthing (false negative feedback), and on–off attacks. Notably, they incorporate a decentralized dispute resolution process: disputes between avatars are arbitrated by other reputable avatars via smart contract, enhancing fairness . They implemented the scheme on a real blockchain platform and compared it to earlier trust frameworks (BTCGS and MSBC-CTrust). The results showed improved malicious entity detection (e.g. 99% Sybil detection vs 80–89% in prior works) and faster threat response . This work exemplifies a scorebased reputation mechanism with a fully on-chain trust computation. Its focus is security against identity centric attacks, assuming an underlying permissionless blockchain to deter tampering.

Awan et al. [28] extend this concept to performance optimization with trust. They introduce a "trust-based resource allocation" framework for metaverse networks. Here, trust scores and a reputation system are used to monitor and penalize nodes causing high latency, thus incentivizing cooperation in sharing computational resources. They even design a novel "Proof-of-Trust" consensus mechanism to integrate these scores into blockchain consensus. Simulation results showed significant latency reduction and scalability improvement by removing untrusted, lag-inducing nodes. This approach highlights a hybrid goal: boosting performance by trust management, not just social trust. It is still score-based and on-chain, addressing malicious or selfish node behavior like denial-of-service or resource hogging in a metaverse's infrastructure layer. Security-wise, it targets Sybil-like abuses and unreliable nodes, but it does not focus on user reputation for content or interactions.

Another notable reputation model is the Blockchain-based Trust and Reputation Model (BTRM) by Tu et al. [29], albeit in an IoT context with ideas transferable to metaverse. BTRM employs a Dynamic Evaluation Mechanism (DEM) to update user reputation efficiently. Users' on-chain behavior is evaluated across multiple aspects, and reputation is adjusted with decay functions that give less weight to old interactions. This dynamic/aging mechanism helps mitigate reputation inflation and Sybil strategies – long-dormant or freshly spawned identities start with low reputation, and any malicious act quickly lowers their trust score. BTRM was prototyped on a Hyperledger Fabric permissioned blockchain, demonstrating that even a private ledger can host decentralized reputation services with some level of security and transparency. The authors report that DEM-BTRM resists multiple attack types and reduces overhead by performing reputation updates only when needed, instead of every transaction. While BTRM is not metaverse-specific, it foreshadows design choices in later metaverse trust proposals: use of trusted blockchain ledgers for sharing reputation data, and selective evaluation to remain scalable.

Applying reputation specifically to metaverse consensus, Xia et al. [30] present a reputation-aided lightweight consensus service for a multi-chain metaverse. They note that conventional blockchain consensus e.g. PoW, PoS can be inefficient for metaverse applications that demand low latency and high throughput. By leveraging participant reputations, their framework prioritizes reputable nodes in the consensus process, effectively creating a Proof-of-Reputation variant. This not only speeds up block confirmation (since well-behaved nodes are less likely to double-sign or fork) but also provides Sybil resistance – a swarm of new fake identities will lack reputation and thus have minimal influence on consensus.They also integrate a cross-chain reputation management so that users active on one chain or shard of the metaverse carry their trust score when interacting on another, addressing interoperability in a multi-chain metaverse. Although detailed performance results are pending publication, this work highlights the trend of building reputation into blockchain infrastructure itself (consensus, not just application layer), thereby establishing trust at the very foundation of metaverse transactions.

Moving to user behavior trust, Rahaman et al. [31] present Meta-Governance, a framework to manage misbehavior e.g. hate speech, harassment in the metaverse using blockchain and AI . They deploy an NLP model to detect toxic chat or actions and then record each offense on a blockchain ledger as an immutable record . A smart contract then updates a "credit score" reputation for the user – a form of on-chain score that lowers with infractions. Accumulating bad behavior can trigger penalties or access restrictions. The prototype uses a permissioned blockchain to maintain privacy and performance while ensuring data integrity. By combining AI detection with on-chain reputation, this scheme addresses trust in social interactions: it provides accountability and access control based on reputation. The threat model here is behavioral (trolling, harassment) rather than identity fraud. It implicitly assumes user identities are somewhat persistent (though on a private chain). Sybil attacks remain a challenge, as the authors note centralized systems alone are vulnerable – integrating this with identity proofs would be needed. Nevertheless, Meta-Governance demonstrates a permissioned-chain reputation system focused on community trust and safety, with promising results in maintaining a secure, inclusive environment.

Dimitriou [32] developed a decentralized reputation token scheme that, while not metaverse-specific, is highly relevant. In this system, each user has a single long-term secret identity, but can have many pseudonymous avatars. All those pseudonyms link to one reputation token on a blockchain via zero-knowledge proofs, preventing anyone from linking the avatars yet ensuring the user's reputation is unified . The reputation token is stored on a public ledger and updated as the user gains feedback . Crucially, whitewashing attacks are prevented: a user cannot discard a bad reputation by switching pseudonyms, since the token ties together all identities. At the same time, the use of zk-SNARKs ensures feedback is anonymous and reputation queries do not reveal which pseudonyms belong to the same user. It also inherently mitigates collusion to some extent (since fake identities are curtailed and feedback is anonymous, collusive rating rings are harder to organize). The trade-off is complexity and reliance on advanced crypto, but it represents a state-of-the-art in decentralized reputation design.

Baccour et al.[33] propose a blockchain-based reliable federated meta-learning framework specifically tailored for metaverse services. Their approach leverages blockchain to securely record and manage participant reputations, using both historical and predicted contributions. The dual-game mechanism incentivizes honest behavior and penalizes unreliable agents, providing a decentralized, tamper-proof foundation for collaborative AI and avatar services. This work exemplifies the potential of blockchain to address trust and incentive challenges in large-scale, decentralized metaverse platforms, combining on-chain transparency with advanced reputation modeling and game-theoretic analysis. Lin et al.[34] put forward a trustworthy AIGC service framework based on blockchain technology for the metaverse, which combines semantic communication, IRM-based extraction, and smart contract verification to guarantee decentralized trust and authenticity of content generated by AI. Their approach not only permits verifiable, human-centric digital content sharing between unknown participants but also puts forth the state-of-the-art in metaverse trust mechanisms enabled by blockchain.

Kharvi [35] introduces a multi-faceted trust score framework that aggregates diverse signals—Web3/DID authentication, NFT ownership verification, behavioral analytics, and contextual information—into a single reputation score . His protocol also defines a Metaverse Trust Score Protocol (MTSP) to enable cross-platform identity persistence, effectively providing a privacy-preserving, AI-driven trust metric for users migrating across virtual worlds . This work exemplifies a sophisticated score-based system, extending blockchain-enabled reputation to interlinked metaverses. Similarly, Truong et al. [36] focus on digital-asset trust: their MetaTrade framework uses blockchain smart contracts to manage AI-generated content (AIGC) trading . MetaTrade removes trusted third parties by escrow-based smart contracts, securing copyright and license exchange in a trustless metaverse marketplace. Simulation results show it achieves higher throughput and lower transaction costs than centralized DAM platforms, while being resilient to content piracy, single-point failures, and fraud. These schemes enrich the class of blockchain reputation systems by handling complex assets (AIGCs) and composite trust scores across domains.

Ud Din et al. [37] proposed a blockchain-enabled zero-trust architecture tailored specifically for the Metaverse. This model emphasizes continuous verification rather than assuming implicit trust, leveraging blockchain's decentralized nature to manage identities and enforce strict authentication. Their results indicate superior threat detection rates, faster security breach responses, and improved scalability compared to traditional perimeter-based security systems.

4.2. Self-Sovereign Identity and Credential-Based Trust

Beyond numeric reputation scores, another branch of research focuses on identity trust: ensuring that metaverse avatars or organizations are tied to verifiable credentials. This is often pursued via Self-Sovereign Identity (SSI) frameworks using decentralized identifiers (DIDs) and verifiable credentials on blockchain. Ghirmai et al. [38] propose a Web3-based trust architecture that leverages SSI to secure interactions across different metaverse platforms. In their system, each user controls a digital wallet (dApp) that stores identity credentials issued as cryptographic tokens. A backend of blockchain smart contracts verifies these credentials whenever two parties interact in a virtual environment. They demonstrate a prototype on Ethereum and report significant improvements in security and scalability: by offloading most verification logic to smart contracts and keeping identity data in user wallets, their system allows secure cross-platform authentication with minimal performance overhead. Notably, this architecture makes the metaverse interoperable – credentials issued in one world can be recognized in another world if both adhere to common SSI standards and trust the issuer. It addresses the fragmentation problem where today each platform is an island of identity. However, one challenge is governance: establishing which authorities can issue reputation credentials and ensuring they are not falsified.

A complementary approach is to use non-transferable tokens as reputational badges. The concept of Soulbound Tokens (SBTs) introduced by Ohlhaver et al.[39] has gained traction as a way to encode trust in Web3 communities . An SBT is essentially a personal token in one's wallet that cannot be transferred, only issued or revoked [**?**]. For example, an MMORPG metaverse could award an SBT to players who attain a high karma or complete certain trustworthy tasks. Because the token is bound to the user's identity, it establishes a persistent reputation that others can verify.

Jalink [**?**] of EY describes SBTs as a means to "encode the trust networks we know and value in the real economy" into the metaverse . Unlike freely tradable reputation points, SBTs ensure reputation is earned and non-fungible – much like real-world diplomas or credit scores . Proposed use cases include proof of skill/experience, community standing, and governance voting weight in DAOs . For metaverse specifically, SBTs can help prevent Sybil attacks and fake personas: each unique user builds a collection of SBT credentials over time, making it costly or impossible to counterfeit a long positive history. If a malicious actor spawns new anonymous avatars, they will lack the SBT-based reputation that established users have, limiting their ability to cause harm. Several pilot implementations of

SBT-like features are underway in the blockchain community. While not a standalone "system" with performance metrics yet, SBTs are increasingly cited in metaverse trust discussions as a token-based reputation mechanism that complements on-chain score systems.

Song et al.[40] blend the SSI approach with algorithmic scoring in their fuzzy AHP-based trust management mechanism for metaverse identities. They argue that trust in the metaverse should account for multiple factors – not only blockchain transaction history, but also social behavior, verified credentials, and context. By using a fuzzy Analytic Hierarchy Process (AHP), their system aggregates various trust indicators into a single trust score for each identity. The fuzzy logic handles uncertainty and subjective inputs in a more nuanced way than simple averaging. Importantly, this scheme is decentralized: trust calculations can be performed on distributed nodes (or oracles) and written to the blockchain as needed. Identities are self-sovereign, meaning users can choose which data to share; the trust algorithm then only uses the consented data. While detailed results of Song et al.'s[40] implementation are pending, their approach aims to resist manipulation by considering arbitrary identity attributes. For instance, an attacker who fakes one attribute might still have others (like transaction history) exposing their low trust. The authors cite that their model "evaluates user reputation from many aspects and can resist multiple malicious attacks". We can infer it tackles whitewashing by including time-based decay and collusion by weighting feedback by the rater's own reputation. Overall, this represents a hybrid trust model – bridging credential-based trust and behavior-based reputation into a composite score.

Patwe et al. [41] propose a blockchain-empowered interoperable authentication scheme using SSI principles . Their architecture comprising a user-controlled wallet dApp, a metaverse environment, and Ethereum smart-contract backend allows avatars to carry verifiable credentials across platforms. This design defends against impersonation, replay, MITM and other attacks (as confirmed by AVISPA/ROR analyses) while preserving user anonymity.

Mebrahtom et al.[42] also build on SSI, implementing a decentralized identity chain for avatars across virtual worlds . Both works place trust in user-managed DIDs and credentials rather than centralized authorities, improving privacy and cross-platform interoperability. In contrast, Kharvi's [35] trust score relies partly on DID-based identity proofs combined with behavior and NFT data, blurring the line between identity-based and reputation-based trust. These contributions highlight an emerging category of blockchain trust schemes that use self-sovereign identity and verifiable credentials to authenticate users and anchor trust without central intermediaries.

Gebre et al. [43] propose a Web 3.0 architecture leveraging self-sovereign identity (SSI) and blockchain to enable secure, interoperable trust across multiple metaverse platforms . A user-controlled digital wallet stores verifiable credentials, which are checked by a blockchain-based back-end to authenticate avatars and assets across worlds. The system is largely hybrid: local SSI credentials and off-chain interactions are anchored by on-chain verification for tamper-proof interoperability. This approach targets cross-platform metaverse applications, such as allowing a user's reputation and identity to carry over between different virtual environments.

Ling et al. [44] develop a trust management framework for digital healthcare in the metaverse. Their approach uses SSI to give patients and providers control over personal data and qualifications in a virtual hospital setting. Each user (patient or doctor avatar) has verifiable credentials (e.g. a medical license, patient ID) managed through an SSI wallet; trust is established by verifying these credentials via smart contracts before any medical interaction. The framework emphasizes privacy and data consent and ensures that only authenticated, credentialed avatars can access sensitive services, thus addressing impersonation and fraud in medical encounters. While primarily conceptual, this scheme highlights how trust frameworks can be tailored to specific domains like healthcare by combining blockchain with real-world identity standards.

4.3. Trust Architectures and Specialized Metaverse Domains

Beyond general frameworks, researchers have proposed tailored trust architectures for specific metaverse scenarios. Xu et al. [14] introduce a "trustless architecture" for blockchain-enabled metaverses that emphasizes secure resource sharing and privacy. They observe that a metaverse is composed of many subsystems, and a one-size-fits-all global trust system is infeasible. Instead, they model the metaverse as a hypergraph of user groups, where each hyper-edge (group) consists of users with a certain relationship or context. They then define a Local Trust Model (LTM) that computes a trust value for each group rather than for the entire network. Essentially, trust is localized: within a gaming guild, for example, the members establish trust amongst themselves, and that trust is used to manage resources or interactions within that group. This design contains the impact of malicious actors: an attacker would have to infiltrate and gain trust in a specific group to do damage, and even then, other groups remain unaffected. The architecture uses blockchain as an underlying layer to connect these groups and enforce On-Demand Trusted Computing Environments (OTCE). For example, if a group of IoT sensors in a metaverse city district has a high trust level, the blockchain can trigger an OTCE with more relaxed security checks for them, improving efficiency. Conversely, a low-trust group might get a locked-down OTCE. By adjusting security policies per trust group, the system is both efficient and secure. While mostly conceptual, this architecture aligns with the metaverse's need to fuse diverse trust contexts without a single point of failure. It's a form of partitioned trust domain approach, using blockchain to coordinate trust evaluations and resource access among domains.

In more specialized domains, trust schemes have emerged to tackle domain-specific threats. One example is Vehicular Metaverses – blending AR/VR with real-time vehicle networks. Lotfi et al. [45] present VMGuard, a security framework to ensure trust in data exchanged within a vehicular metaverse. In this scenario, vehicles and roadside sensors feed data to a virtual world. A critical threat is data poisoning: compromised IoT devices sending false data to disrupt services. VMGuard implements a reputation-based incentive mechanism to discourage and detect poisoning. Each data-producing device (camera, car sensor, drone) earns a reputation score based on feedback from data consumers. A subjective logic model aggregates feedback into trust scores, which are stored and updated. Devices with high reputation get rewards or continued access, while those that provide bad data see their reputation plummet. The authors validate that this mechanism effectively prevents poisoning attacks. While VMGuard does not explicitly detail a blockchain implementation, it aligns with decentralized trust principles. We can envision such a scheme being deployed via smart contracts in a city-wide permissioned blockchain, where each vehicle has a blockchain identity and an associated rep score. This would make the trust assessments transparent and harder to tamper with, increasing drivers' and regulators' confidence in the vehicular metaverse data.

Several new works address trust at the infrastructure or application level. Li et al [46] present DareChain, a blockchain-based trusted collaborative network infrastructure for the metaverse. DareChain uses a novel multi-chain architecture with a "collaborative-worker" system, a subject–object account model, layered smart contracts, and a hyperlinear ledger consensus. This design targets enterprise and public-sector metaverse scenarios e.g. government, healthcare, finance by raising throughput and enforcing privacy [25]. In particular, DareChain's parallel consensus dramatically boosts transaction throughput and reduces latency, and its transaction model includes privacy-preserving obfuscation of sensitive data. These features effectively turn blockchain into a high-performance, privacy-aware backbone for metaverse collaboration.

Liu et al. [47] tackle vehicular edge metaverse trust. They embed a reputation score into a PBFT consensus protocol: vehicles with high trust are selected as validators, improving consensus speed and reliability . Resource allocation is optimized per-vehicle, and communication phases are tuned to reduce delays. Simulation shows this scheme reaches PBFT agreement with significantly lower latency and energy consumption, making vehicular metaverse consensus both faster and more scalable . This introduces a "reputation-weighted consensus" category, where trust values directly influence who participates in consensus for edge domains. In parallel, Awan et al. [48] introduces a quantum-secured trust management framework for vehicular networks, integrating blockchain technology with quantum cryptography and metaverse modules. This hybrid approach is positioned to meet the next-generation demands of secure and reliable trust management in immersive vehicular environments, addressing both classical and quantum threat models.

Other domain-specific studies include Kuru et al.[49], who survey cyber threats in an urban metaverse and propose a decentralized ML-based authentication preserving privacy. Their method uses immersive edge devices to jointly train federated models of user identity/behavior and verifies authenticity via blockchain, thwarting avatar impersonation and credential theft without central authorities. Cao et al.[50] introduces PolyTwin, an edge blockchain-enabled trustworthy digital twin (DT) network for the metaverse. Unlike previous DT systems, PolyTwin was built around the idea of deploying AI-packed edge devices to generate DTs for practical use. Not only that, they also leveraged a new on-chain Proof of Consistency (PoC) mechanism to validate digital twin networks in such a way as to ensure consistency and correctness far beyond any prior DT system. In effect, they created a system that they claimed makes trustworthy DTs from which secure physical-to-virtual interactions can arise. They validated their claims using two practical prototypes, PolyCampus and PolyExchange, of the core functionality needed for a DT to perform in a trustworthy manner. PolyTwin paves the way for a new direction in metaverse trust, achieved by integrating edge AI with a decentralized blockchain consensus to validate digital twins.

In the digital asset commerce domain, Islam [51] analyzes trust perceptions in Web3 metaverse transactions. He finds that institutional/brand trust dominates even in tokenized environments. Traditional trust concepts, performance, reciprocity, etc., remain critical. Islam concludes that reputation mechanisms e.g. SBTs, ratings will need to complement these legacy trust factors to gain user acceptance.

Finally, industry consortia are actively exploring standards for unified reputation in the metaverse. The Metaverse Standards Forum (MSF)[4] in 2025 published a use-case blueprint for “Unified Reputation Management for Metaverse Entities.” This is not a specific algorithm but rather a vision that encapsulates many of the above research insights. The MSF envisions a decentralized, transparent reputation system where both individual avatars and organizations accumulate reputation based on their activities and feedback in any metaverse platform. Reputation data would be portable – e.g. your “Metaverse reputation profile” could move with you from one world to another. Real-life reputation could even be linked (with consent) to metaverse identities (e.g. a LinkedIn job reputation can attach to your professional avatar). The MSF highlights the feasibility of using blockchain and decentralized storage (IPFS) to achieve this portable rep: projects like Civic [52] and Chainlink oracles [53] are mentioned as building blocks. Essentially, one could store reputation credentials or scores on a public blockchain, with each platform reading/writing to that common ledger. However, the forum also acknowledges major challenges such as privacy, data accuracy, and cross-platform interoperability details. The significance of the MSF report is that it aggregates industry requirements and lends momentum to the academic ideas – indicating a convergence on the need for standardized trust metrics in the metaverse. Table 2 summarizes the key blockchain-based trust/reputation schemes covered, highlighting their mechanisms, blockchain platforms, and contexts.

Table 2. Summary of leading bl ockchain-based trust/reputation schemes for the metaverse, classified by mechanism and platform.

Scheme (Year)	Mechanism Type	Blockchain Platform	Architecture	Target Context	Ref.
Trust-based Metaverse Framework (2023)	Score-based reputation (PoT consensus)	Assumed permissionless (Ethereum-like)	Mostly on-chain (smart contracts + monitoring)	General metaverse (resource sharing, VR/AR)	[28]
DEM-BTRM IoT Trust Model (2022)	Score-based reputation + decay	Permissioned (Hyperledger Fabric prototype)	Hybrid (off-chain calc, on-chain storage)	IoT/Metaverse crossover (trust in IoT data)	[29]
Rep-aided Consensus (2024)	Score-based reputation (weighted consensus)	Multi-chain Metaverse (sharded chains)	On-chain integrated (consensus protocol level)	Blockchain infrastructure for metaverse	[30]
SSI Web3 Trust (2024)	Credential-based trust (SSI, DIDs)	Permissionless (Ethereum smart contracts)	Hybrid (off-chain wallet + on-chain verify)	Cross-platform user identity & auth	[38]
Fuzzy AHP Trust (SSI-based) (2025)	Hybrid score (multi-factor fuzzy)	Not specified (conceptual, any chain)	Hybrid (compute off-chain, publish on-chain)	Metaverse digital identity reputation	[40]
Trustless Architecture (2023)	Local trust groups (scores per group)	Not specified (generic blockchain layer)	Hybrid (blockchain + off-chain enclaves)	General metaverse (resource & security mgmt)	[14]
VMGuard Vehicular (2024)	Score-based reputation (feedback loop)	Blockchain not explicitly used; possible extension	Off-chain currently (could use blockchain log)	Vehicular metaverse (IoV data integrity)	[45]
Soulbound Tokens (2022)	Token-based reputation (non-transferable)	Ethereum and others (concept level)	On-chain tokens (issued via smart contract)	Web3 social trust (metaverse credentials)	[39]
DareChain (2023)	Collaborative multi-chain	Permissionless multi-chain	On-chain parallel consensus	Enterprise metaverse (govt, finance)	[46]
Blockchain SSI Auth (2024)	Credential-based (SSI)	Ethereum	Hybrid (wallet + smart contract)	Cross-platform user authentication	[41]
DPPML Authentication (2024)	Privacy-preserving ML-based	Conceptual urban metaverse	Hybrid (FL + blockchain)	Urban metaverse authentication	[49]
Vehicular Trust Consensus (2024)	Score-based PBFT consensus	Permissioned PBFT	Hybrid (off-chain rep/on-chain PBFT)	Vehicular edge metaverse	[47]
DID-Based Metaverse Authentication (2025)	Credential-based (DID + ILWKM-CS crypto)	Not specified (any DID-enabled chain)	Hybrid: DID issuance off-chain, login/auth proofs on-chain	E-learning metaverse – secure avatar login	[54]
Trust Framework for SSI (2024)	Credential-based (medical SSI)	Permissioned/private healthcare chain	Hybrid: patient/doctor credentials off-chain; smart-contract checks on-chain	Secure tele-medicine VR hospital scenarios	[44]
MetaTrade (2024)	Blockchain DAM (escrow-based)	Ethereum (EVM-compatible)	On-chain (smart contracts)	AI-generated content trading	[36]
Decentralized SSI Trust Framework (2024)	Credential-based (SSI wallet + verifiable credentials)	Ethereum smart contracts	Hybrid: mobile SSI wallet & dApp off-chain; auth proofs on-chain	Cross-domain avatar authentication & access control	[43]
QSTMF (2025)	Quantum-secured trust + blockchain reputation	Consortium chain + quantum cryptography	Hybrid (on-chain/off-chain/quantum)	Vehicular metaverse (Web 3.0/VANETs)	[48]
MAP (2024)	Trustless cross-chain interoperability (relay chain + zk-SNARK light clients)	Multi-chain; Ethereum; MAP relay chain	Decentralized, non-custodial, scalable	Web 3.0/metaverse; DeFi; NFTs	[55]
Meta-Learning (2024)	Federated meta-learning with blockchain-based reputation and dual-game incentives	Custom blockchain (smart contract)	Decentralized; transparent; incentive-aligned (Stackelberg/coalition games)	Metaverse (AI service, avatar reputation)	[33]
PolyTwin (2024)	Proof-of-Consistency for DTs using edge AI + blockchain	Private/consortium blockchain among edge clusters	Edge-AI + blockchain; on-chain validation	Digital twins (PolyCampus, PolyExchange)	[50]
AI Generated Content (2024)	Blockchain-trustworthy AIGC with semantic comm + smart contracts	Consortium blockchain	Decentralized; verifiable; incentive-aligned (Stackelberg, IRM)	Metaverse (AIGC, personalized content)	[34]
Trusted Notary Group Cross-Chain (2024)	Fast cross-chain via trusted notary committee protocol	Multi-chain; consortium/permissioned	Notary group–based; semi-decentralized; high-throughput	Asset/data transfer; cross-domain interop	[56]
Blockchain-Enabled Zero-Trust Architecture (2024)	Collaborative infrastructure (zero-trust model)	General (EVM-compatible or similar)	Hybrid (on-chain + off-chain)	General metaverse (virtual environment security)	[37]

5. Taxonomy of Metaverse Trust Schemes

To better understand the landscape, we organize metaverse trust schemes along multiple axes. Figure 2 provides a taxonomy that groups solutions by their mechanism, threat model, and architecture. This holistic view highlights where different approaches stand and how they relate.

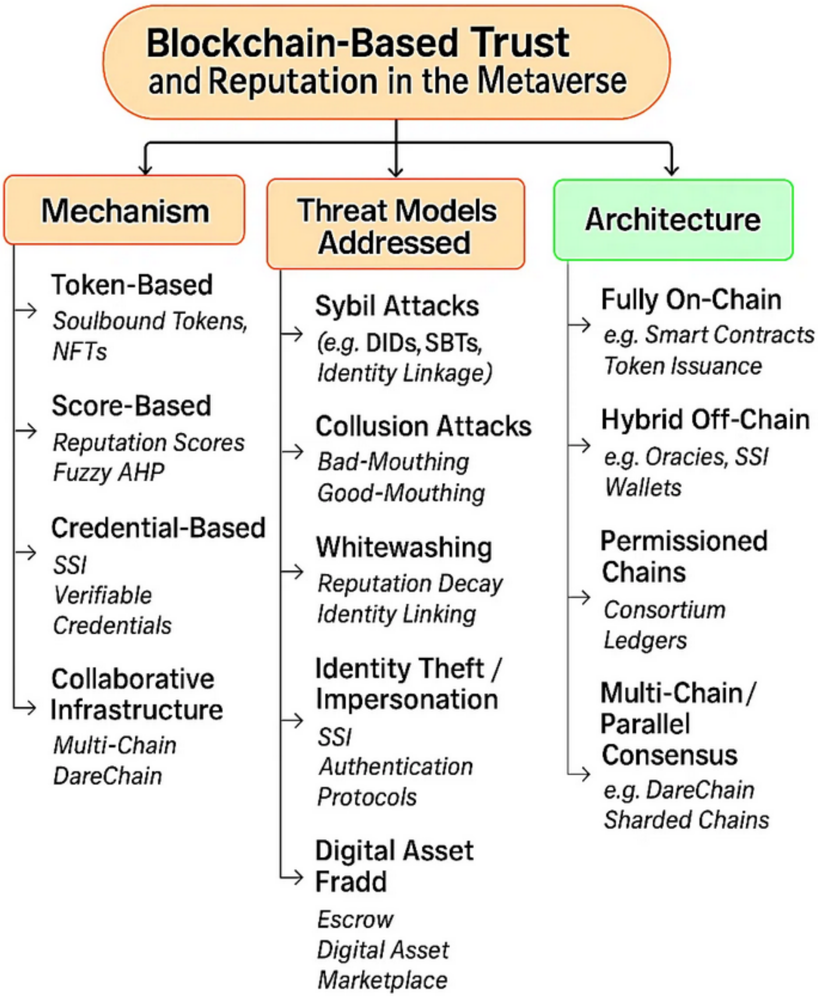

Figure 2. Taxonomy of blockchain-based trust and reputation mechanisms in the metaverse.

As shown in Figure 2, we identify four primary mechanism types:

- **Token-Based Mechanisms:** These use crypto-tokens to represent trust or reputation. Reputation tokens may be fungible or non-fungible. Soulbound Tokens (SBTs) are a prominent example – an SBT is essentially a tokenized credential or badge that signifies some trusted attribute of a user and cannot be transferred [39]. Token-based schemes lean on blockchain's strength in handling assets: trust is embodied as an asset owned by the user. This category typically excels in portability and Sybil-resistance. However, purely token-based approaches may struggle with granularity – a token often represents a coarse achievement rather than a nuanced behavior history – and with privacy, since on-chain tokens are publicly visible. For example, a user's collection of reputation NFTs or SBTs can signal their trust level across the metaverse, but it also means anyone can inspect and correlate those credentials. Token-based designs must balance these trade-offs, and in practice they are often combined with other methods e.g., using on-chain tokens to summarize off-chain scores.
- **Score-Based Mechanisms:** These compute a numerical reputation score for each user or entity, often through algorithms aggregating feedback over time. The score might be stored on-chain or off-chain with secure checkpoints on-chain. Score-based schemes can incorporate complex logic to reflect trust dynamics [28,29]. They offer flexibility and fine-grained updates. Many are designed to address collusion and whitewashing through algorithmic defenses. On the flip side, maintaining scores often requires continuous monitoring and computation, raising scalability concerns in very large systems if every interaction triggers a score update.

- **Credential-Based Mechanisms:** These approaches leverage verifiable identity credentials and attributes as the basis for trust. Rather than (or in addition to) tracking behavior, a user's reputation comes from what they are (their credentials) — for example, possessing a valid ID, a proven skill certificate, or endorsements from trusted parties. Self-Sovereign Identity (SSI) frameworks fall in this category: users have decentralized identifiers (DIDs) and present verifiable credentials to establish trust in anonymity-preserving ways. Credential-based trust is often implemented via tokens that represent credentials (in fact, SBTs can be seen as one form of credential token), or through on-chain registries of verified attributes. Mebrahtom et al. [42] demonstrate this approach by integrating a decentralized identity wallet with an on-chain registry; participants must provide authentic credentials e.g., proof of a verified real-world identity or qualification, which are then tokenized or referenced on-chain. This requirement raises the bar for attackers—Sybil attacks are mitigated because each identity must have unique, verifiable attributes, and impersonation is harder if reputation is tied to cryptographic proofs of identity. Song et al.[40] similarly blend credential-based trust with behavior scoring: in their fuzzy AHP-based reputation mechanism, factors like the presence of certain SBT badges or verified traits of an avatar are weighted alongside that avatar's actions. Credential-based schemes thus anchor trust to confirmed qualities of the user. They can provide strong identity authenticity and initial trust bootstrap, at the cost of requiring robust privacy safeguards and interoperability. Ongoing efforts in standards e.g., decentralized identity and Trust-over-IP models aim to ensure that credential-based trust credentials can be widely accepted across different metaverse platforms without compromising user privacy.
- **Collaborative Infrastructure Approaches:** Some emerging solutions build trust into the infrastructure of the metaverse itself, rather than focusing on a single metric or token. We term these collaborative infrastructure mechanisms: they propose a network architecture where multiple blockchain networks or modules work together to uphold trust. The idea is to support trust and reputation as a cross-platform service, enabling various metaverse domains to collaborate in sharing trust data securely. DareChain [46] is an example of this category – a blockchain-based trusted collaborative network infrastructure for the metaverse. DareChain introduces a collaborative-worker multi-chain system in which a main "collaborative" chain coordinates with multiple specialized side-chains to manage one-to-one mapping of physical entities to digital avatars, record their interactions, and enforce trust rules across different applications. By using a layered smart contract model and a new consensus algorithm, this infrastructure can handle large-scale interactions in parallel while ensuring consistency and security. The collaborative infrastructure approach effectively blurs mechanism and architecture: trust is maintained through the architecture's design. Such designs address challenges like interoperability and scalability of trust – for instance, DareChain enables cross-chain queries and transactions so that reputation or asset data from one virtual world can be trusted in another, creating a unified trust fabric. This approach is still nascent, but it points toward metaverse-scale trust systems where the network of blockchains itself provides core trust services including identity validation, asset provenance, secure transaction processing, for any number of higher-level applications. It complements the other mechanism types by ensuring that trust is holistically supported at the infrastructure level, an approach crucial for an interconnected future metaverse.

Orthogonal to mechanism, we classify schemes by the threat models they tackle. A robust metaverse trust system should ideally counter multiple attack vectors:

- **Sybil Attacks:** A Sybil attack is when one user creates many fake identities to exploit the system e.g., to gain extra rewards or distort reputation scores [57]. Solutions typically aim to limit the ability to spawn endless credible identities. Approaches based on unique identity or proof-of-personhood directly mitigate Sybils. For example, requiring users to register a decentralized identity (DID) backed by some real-world verification, or issuing a non-transferable token per human as in SBTs, makes it hard for one person to manage many identities without detection

[39]. Credential-based schemes naturally help here: if each participant must provide verifiable attributes or undergo an identity attestations process [42] , Sybil nodes are thwarted because an attacker cannot easily fabricate multiple valid credentials. Some score-based systems also indirectly limit Sybils by design—new identities start with neutral or low reputation and must invest time and good behavior to become influential, so a swarm of fresh Sybil bots remains ineffective until they earn trust over many interactions. In Figure 2, approaches like SSI-based identity frameworks and SBT credential systems are grouped under Sybil-resistant solutions, as they raise the cost of obtaining multiple trustworthy identities in an otherwise anonymous metaverse [41].

- **Collusion Attacks:** Collusion involves attackers working together to deceive the reputation system. This can take the form of bad-mouthing where a group of malicious users unfairly low-rating a target to undermine their reputation or ballot-stuffing/good-mouthing where a group conspiring to boost each other's trust with false positive feedback[58]. Decentralized reputation schemes use various techniques to defend against collusion. Many algorithms incorporate statistical detection of anomalous rating patterns, for instance, spotting if a cluster of avatars always rate each other positively or always down-vote a particular victim. Others leverage the web-of-trust concept: they weigh feedback by the rater's own reputation or relationship to the ratee, so a set of low-reputation newcomers colluding will have minimal influence. Some solutions use ground truth anchors by cross-checking ratings against actual outcomes – e.g., if users rate a seller as honest but all of the seller's transactions are disputed, the system can flag those ratings as likely collusive. Blockchain can assist by transparently logging all feedback, making it easier to audit for collusion after the fact. Awan et al.[27] incorporate reputation-driven voting schemes to filter out dishonest feedback and reportedly detect coordinated rating attacks with high accuracy. In Figure 2, we list Awan's trust management framework under collusion defenses, since it explicitly demonstrated the ability to identify both bad-mouthing and ballot-stuffing attacks [27]. Generally, combining algorithmic filters to identify suspicious rating behavior with trust weighting forms the core of collusion resistance in these systems.
- **Whitewashing Attacks:** In a whitewashing attack, a user who has accumulated a bad reputation simply discards that identity and re-enters the system with a brand new identity [59]. This is a classic challenge in reputation systems, exacerbated in open metaverse environments where creating a new avatar can be trivial. Countermeasures focus on making reputation sticky to users or imposing penalties for starting over. One approach is identity linkage: even if a user switches accounts, the system tries to link the new identity to the old so that the negative history follows them [14]. Another common defense is reputation decay and time-based weighting: recent behavior counts more than old behavior, and longdormant identities lose reputation strength. This means an attacker cannot simply shelf an identity until community memory fades; by the time they return, their prior reputation has decayed, and they must prove themselves again. Some systems also issue "age credits" – trust is partly a function of how long an identity has been around and active. Whitewashing is thus discouraged because a fresh identity lacks longevity-based trust and any attempt to rapidly build high reputation will be tempered by cautious algorithms. Awan et al.[27] address whitewashing by tracking entities' history even across join/leave cycles and using dynamic reputation aging; their prototype caught nearly all whitewashing attempts in simulations by detecting when a supposedly "new" node behaved too similarly to a recently departed bad actor. Similarly, Song et al. [40] include a decay factor in their fuzzy reputation model so that users cannot regain full trust instantly after rejoining. In Figure 2, schemes with such features are categorized under the whitewashing mitigation group. By ensuring that reputation cannot be fully reset or quickly rebuilt, these systems maintain accountability over time.
- **Identity Theft/Impersonation:** Beyond fake accounts, a serious threat is when an attacker hijacks or mimics a real user's identity to exploit their established trust. In the metaverse, this might involve stealing private keys to an avatar, or creating a lookalike avatar/profile to fool others [60].

Blockchain-based trust systems tackle impersonation primarily through strong authentication and secure identity management. If trust is tied to cryptographic identities that are controlled by users, an attacker cannot impersonate someone without also compromising their private key. This drives the adoption of SSI authentication protocols in the metaverse. For example, Patwe et al. [41] propose a blockchain-enabled interoperable authentication scheme where each user is uniquely identified in the physical world and linked to their avatars. Their scheme uses cryptographic challenges and blockchain records to ensure that when an avatar tries to interact across platforms, it proves that it has the correct private keys and credentials. This prevents an impostor from masquerading as someone else's avatar because they would fail the authentication checks without the victim's keys. More generally, systems that use verified credentials inherently resist impersonation: an attacker trying to pose as, say, a certified doctor in a metaverse clinic would need that doctor's verifiable credential, which is digitally signed and nearly impossible to forge without issuing authority. Mebrahtom et al. [42] emphasize identity authenticity in their reputation design: By requiring that each participant's identity be validated and bound to their reputation records, they close the door to opportunistic identity theft. In summary, by binding reputation to secure digital identities and requiring cryptographic proof of identity claims, these trust frameworks greatly reduce the risk of impersonation. Users may also be alerted via blockchain logs if an identity key is changed or used in suspicious ways, adding transparency that helps detect account takeovers in a decentralized manner.

- **Digital Asset Fraud:** Metaverse ecosystems feature marketplaces for digital assets that introduce risks of fraud in transactions. Examples include sellers deceiving buyers with counterfeit or non-existent assets, or buyers defaulting after receiving an item. Trust mechanisms have evolved to address these transactional fraud scenarios. A straightforward approach is the use of smart contract escrow services: When two parties trade a digital asset, a blockchain smart contract can hold the buyer's payment in escrow and only release it to the seller once the asset is verifiably transferred to the buyer's ownership. This trustless escrow removes the need to trust the counterparty's promise, as the contract ensures a fair exchange or refunds the buyer if the conditions are not met. Decentralized marketplaces like OpenSea [61] are beginning to use such mechanisms to protect against fraud in NFT trades. Another vital component is provenance tracking. Because blockchain inherently records ownership history, buyers can check the chain of custody of a digital asset to verify its authenticity and that the seller has rightful ownership. This helps prevent the sale of forged or stolen virtual goods. Reputation systems can layer on top of this by assigning trust scores to asset sellers and buyers based on their past transaction behavior. For example, a seller with many successful, dispute-free sales will develop a high reputation, while a seller involved in prior frauds or transaction failures will be flagged with a low score. Future trust frameworks may integrate these reputations directly into marketplace smart contracts—only allowing high-reputation sellers for certain high-value trades, or requiring extra collateral from a low-reputation participant. By linking reputation events with actual on-chain transactions, the system can also filter out false feedback. Initial research indicates that users are more willing to engage in metaverse commerce when they see such protections in place. In fact, a recent study found that trust in the platform or brand remains a decisive factor for users' purchase intentions in the metaverse, despite the presence of "trustless" blockchain tech [51]. This underscores the need for robust anti-fraud measures. In Figure 2, we illustrate digital asset fraud countermeasures as a distinct category of threat response. Together, these measures ensure that digital asset transactions can be conducted with confidence in their fairness and validity [41].

Figure 3 provides a consolidated visual summary of the primary attack vectors faced by metaverse reputation systems and the corresponding blockchain-based defenses highlighted in this survey. Table 3 enumerates which threats each major scheme explicitly addresses.

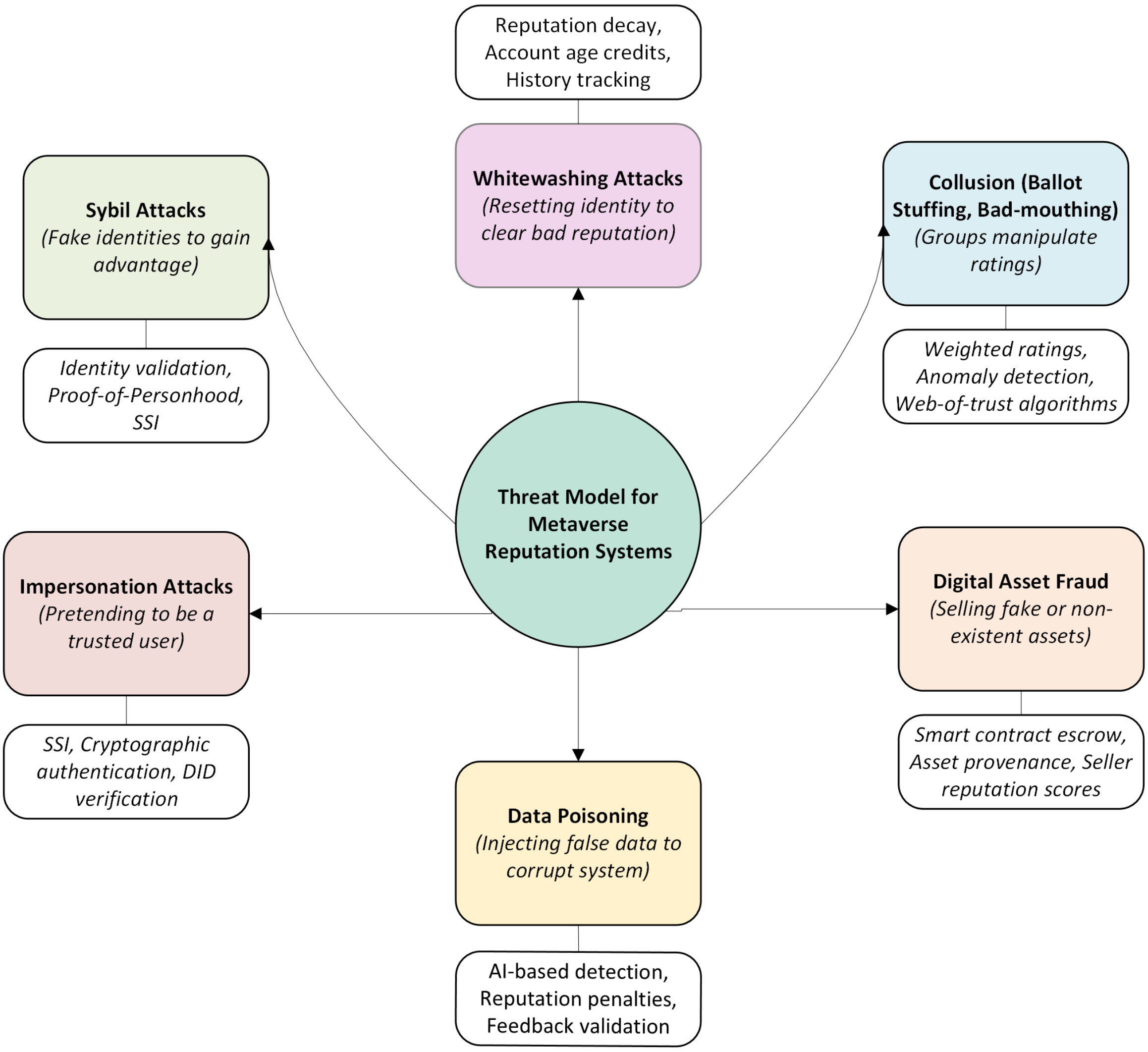
Reputation decay, Account age credits, History tracking
Whitewashing Attacks (Resetting identity to clear bad reputation)
Sybil Attacks (Fake identities to gain advantage)
Identity validation, Proof-of-Personhood, SSI
Collusion (Ballot Stuffing, Bad-mouthing) (Groups manipulate ratings)
Weighted ratings, Anomaly detection, Web-of-trust algorithms
Threat Model for Metaverse Reputation Systems
Impersonation Attacks (Pretending to be a trusted user)
SSI, Cryptographic authentication, DID verification
Digital Asset Fraud (Selling fake or non-existent assets)
Smart contract escrow, Asset provenance, Seller reputation scores
Data Poisoning (Injecting false data to corrupt system)
AI-based detection, Reputation penalties, Feedback validation

Figure 3. Threat Model for Metaverse Reputation Systems

Table 3. Threat-model coverage (✓mitigated; ✗not addressed).

Scheme (Reference)	Sybil	Collusion	White-washing	Impersonation / ID	Asset Fraud	Data Poisoning
SSI-based interoperable authentication [41]	✓	✗	✗	✓	✗	✗
Soulbound-Token (SBT) credential system [39]	✓	✗	✗	✓	✗	✗
Credential-based DID attestation [42]	✓	✗	✗	✓	✗	✗
Reputation-driven voting [27]	✗	✓	✓	✗	✗	✓
Fuzzy reputation with decay [40]	✓	✓	✓	✗	✗	✗
Smart-contract escrow & provenance [61]	✗	✗	✗	✗	✓	✗
DEM-BTRM [29]	✓	✗	✗	✗	✗	✗
Sybil-resistant consensus [30]	✓	✗	✗	✗	✗	✗
Local-trust groups [14]	✓	✓	✗	✗	✗	✗
VMGuard [45]	✓	✗	✓	✗	✗	✓
DareChain [46]	✓	✗	✗	✓	✓	✗
DPPML Auth [49]	✓	✗	✗	✓	✗	✗
ILWKM-CS [54]	✓	✗	✓	✓	✗	✗
SSI (medical) [44]	✓	✗	✗	✓	✗	✗
Trust-aware PBFT [62]	✓	✓	✓	✗	✗	✓
MetaTrade [36]	✓	✓	✓	✗	✓	✗
SSI Trust Framework [43]	✓	✗	✓	✓	✗	✗
Blockchain-Enabled Zero-Trust [37]	✓	✓	✓	✓	✓	✓

Finally, we categorize by architecture:

- **Fully On-Chain:** These systems execute reputation logic entirely on a blockchain. On-chain architectures maximize transparency and tamper-resistance – all actions affecting trust are recorded on the ledger for anyone to audit. For example, a smart contract based rating system might log every feedback and compute trust scores within contract code. The downside is cost and performance: on-chain operations incur gas fees and latency, and complex computations may be impractical on-chain. Nonetheless, some proposals strive for on-chain implementations. Mebrahtom et al.'s [42] cross-platform trust uses Ethereum contracts for verification. If blockchain scalability improves (sharding, Layer-2), on-chain trust management might become more viable.
- **Hybrid Off-Chain:** The majority of practical designs take a hybrid approach, where heavy computation is done off-chain and the blockchain is used as an anchor or arbiter of trust data. In these architectures, intensive tasks happen off-chain — for example, on a set of decentralized oracles, on cloud servers, or within user devices— and only the resulting trust indicators or cryptographic proofs are posted to the blockchain [63]. This offloads work to where it can be done faster and cheaper, while still leveraging blockchain to secure and share the outcomes. Xu et al. [14] exemplify this with their "trustless architecture": they compute trust within local groups and then use a blockchain layer to merely connect groups and enforce decisions. The blockchain in their design triggers On-Demand Trusted Computing Environments and records group trust levels, but the heavy lifting of calculating those trust levels is done off-chain within each group. Similarly, Song et al. [40] envision their fuzzy reputation algorithm running on a network of nodes that periodically write updated scores or proofs to an on-chain registry. The hybrid design aims to achieve scalability while still maintaining verifiability. A risk in hybrid models is the trust one must place in the off-chain components, if those nodes collude or malfunction, they could feed incorrect data on-chain. To mitigate this, many solutions decentralize the off-chain layer too: for instance, use multiple independent oracles and require consensus among them before accepting a trust update, or use cryptographic techniques such as zero-knowledge proofs, secure enclaves, to prove that offchain calculations were done correctly. In our classification, a number of schemes fall under "hybrid": they leverage blockchain for what it's good at without letting it become a bottleneck. This approach is generally the most practical for today's metaverse scale, and indeed most current implementations, even in Web2, like centralized reputation services, have an analogue of off-chain processing with on-chain anchoring now being introduced for added transparency.
- **Permissioned Chains:** While many metaverse trust systems assume a public, permissionless blockchain environment, some are built on permissioned (consortium or private) blockchains. In permissioned architectures, only approved entities can participate in validating transactions and updating the ledger [64]. This model can be attractive for enterprise metaverse applications or specific domains where participants are vetted and the volume of interactions is high. The trust mechanism itself might still be token-based or score-based, but it runs on a closed blockchain network with controlled access. The benefits include higher throughput, lower and more predictable transaction costs, and the ability to enforce organizational governance rules on reputation data. For example, the Blockchain Trust and Reputation Model (BTRM) was prototyped on Hyperledger Fabric, a permissioned ledger [29]. In that system, IoT devices in a controlled environment share a Fabric blockchain to store and update reputations; the permissioned setup ensures only authorized devices and servers partake in consensus, which improves performance and privacy. Similarly, one could imagine a consortium of metaverse platforms forming a permissioned chain to exchange reputation scores among themselves without exposing data on a public network. The trade-off is reduced decentralization and transparency to the wider public – users have to trust the consortium governance. Our taxonomy explicitly includes this dimension now: some solutions operate on consortium ledgers, which we classify under permissioned chain architecture. It's worth noting that permissioned vs. permissionless is often orthogonal to the mechanism; a

token-based or credential-based scheme could be deployed on either type of chain depending on the context. In any case, permissioned chain approaches show that blockchain-based trust can be adapted to closed-world settings where openness is traded for performance or regulatory compliance.

- **Multi-Chain/Parallel Consensus:** As metaverse applications scale, a single blockchain might become a bottleneck for trust management. New architectures therefore explore multi-chain or sharded designs, where the workload is distributed across multiple ledgers running in parallel [62]. In such designs, different aspects of trust might be handled on different chains, or multiple chains might each serve a subset of users and then interoperate. This category overlaps with the earlier "collaborative infrastructure" concept and emphasizes the architectural aspect of using several blockchains together. Xia et al. [30] present a reputation-aided consensus mechanism for a multi-chain metaverse: in their approach, each blockchain shard maintains local reputations and prioritizes reputable nodes for block production, and they introduce a way to carry a user's trust score from one chain to another so that an avatar doesn't have to rebuild trust from scratch on each world. This not only speeds up consensus on each chain but also addresses interoperability by linking trust across platforms. Another example is the aforementioned DareChain architecture [46], which explicitly uses a collaborative multi-chain system: a main chain coordinates global state and identity, while numerous worker chains handle specific domains or regions of the metaverse, all following a unified trust protocol. By running many chains in parallel, DareChain achieves high throughput for trust-related transactions and can isolate certain operations to specific chains. The multi-chain approach inherently requires mechanisms for cross-chain communication and consistency — e.g., relay protocols or bridges that carry reputation information from one chain to another, and consensus algorithms that can scale out. The advantage is scalability and specialization: one chain's congestion or attacks need not bring down the whole system, and each chain can be optimized for a particular trust context while still contributing to an overall trust picture. The challenge is ensuring that these parallel chains maintain a coherent global trust view and that no inconsistencies or exploits arise when moving assets or reputations between chains. As blockchain technology advances, we expect more metaverse trust solutions to adopt multi-chain architectures or layer-2 networks to meet the massive scale of a fully immersive digital universe.

This expanded taxonomy allows us to pinpoint where a given proposal lies in the design space. This framework will aid researchers and practitioners in comparing approaches and identifying complementary strategies for building trustworthy metaverse ecosystems going forward.

6. Benchmark Analysis

We evaluate identified schemes on Security, Scalability, User Privacy, and Interoperability, which are critical in metaverse contexts. Table 4 provides a comparative summary of different schemes on key criteria.

Table 4. Benchmark comparison of schemes on key criteria. Ratings are relative among surveyed schemes.

Scheme	Security (Attack Resilience)	Scalability (Performance)	Privacy (Data Exposure)	Interoperability (Cross-platform)
TrustMgmt [27]	High – multi-attack resistant	Medium – public chain (some optimizations)	Low – on-chain data visible	Low – platform-specific (Ethereum only)
PerfTrust [28]	Medium – specific threat focus	High – custom blockchain consensus (low latency)	Low – no privacy features	Low – platform-specific (private chain)
MetaGov [31]	Medium – stops harassment but Sybils possible	High – permissioned chain real-time AI	Medium – private chain logs identifiable	Low – tied to one platform (not portable)
PrivRep [32]	High – Sybil/whitewash proof	Low – heavy crypto public chain overhead	High – strong anonymity	High – user-centric shareable token
DEM-BTRM [29]	High – multiple attack mitigation via dynamic evaluations	High – permissioned blockchain efficient batching	Medium – partially identifiable transaction data	Medium – potential for multi-chain support
RepConsensus[30]	High – Sybil-resistant via reputation-weighted consensus	High – multi-chain sharded approach	Medium – data visible across shards	High – cross-chain reputation portability
LocalTrust [14]	Medium – local group trust reduces widespread attacks	High – scalable via local computations	High – local trust not globally visible	Medium – dependent on cross-group trust bridges
VMGuard [45]	High – data poisoning protection via reputation	High – regional feedback loops scale efficiently	Medium – vehicle data logs identifiable	Medium – city-wide application interoperability
DareChain [46]	High – attack resistant via parallel consensus	High – parallel chains increase throughput	High – data obfuscation layers	High – designed for enterprise interoperability
DPPML Auth [49]	High – impersonation protection via federated learning	Medium – federated computation scales linearly	High – privacy via federated learning	Medium – urban metaverse focused
Vehicular PBFT[62]	High – Sybil and collusion-resistant via PBFT	Medium – limited by PBFT nodes (<100 nodes)	Medium – data partially identifiable	Medium – edge-specific interoperability
SSI Trust Framework [44]	Medium – strict credential checks in healthcare	Medium – permissioned ledger fits hospital workloads	Very High – patient-driven consent	Medium – domain-specific but standards-compliant
ILWKM-CS [54]	High – ILWKM-CS mutual auth	Medium – lightweight crypto; global scale not yet measured	High – no personal data on-chain	Low – built for one e-learning metaverse
MetaTrade [36]	High – fraud resistance via smart contract escrow	Medium – blockchain dependent transaction speed	Medium – transaction details visible on-chain	High – portable digital asset standards
ZeroTrust-BC Framework [37]	High – multi-vector attack mitigation using blockchain-based zero-trust	High – scalable with fast response and low overhead	Medium – audit trail on-chain with strong access control	Medium – platform-agnostic design, not cross-chain tested

6.1. Privacy and Data Governance

Privacy is of paramount concern in the metaverse, as large amounts of personal data and behavioral traces form the basis of reputation systems. The challenge is to derive trust signals without exposing sensitive information or violating users' rights.

Self-Sovereign Identity (SSI) approaches inherently prioritize privacy. Users fully control their credentials and disclose only what is necessary. For example, to prove one's trustworthiness, a user might show a credential that says "reputation score > 80 (verified by X)" through a zero-knowledge proof rather than revealing their entire history. The design of Mebrahtom et al. design exemplifies this by allowing selective disclosure of trust information, enhancing user control over personal data [42]. There is no central database of identities; identity data stays in user wallets, and only cryptographic attestations are anchored on-chain pseudonymously. This greatly limits leakage because outsiders cannot easily profile a user's activities across worlds if interactions are kept off-chain or anonymized.

On-chain score systems are less private by default because every rating and score update may be visible on the public ledger. This can lead to unwanted profiling. For instance, if Alice's reputation score drops on-chain, anyone could observe that and infer she did something unfavorable. Awan's system, being largely on-chain, doesn't hide such information – one could pseudonymize user addresses, but in a metaverse context an address is often directly tied to an avatar, so a drop in that avatar's on-chain rep is effectively public [27]. To mitigate this, researchers suggest using zero-knowledge proofs to prove statements about reputation without revealing raw data. For example, a user might prove "my score > 50" with a ZK proof; the blockchain can verify this without storing the actual score. None of the surveyed implementations fully integrated ZKPs yet, but this is a known technique in blockchain privacy research that could be adopted in future systems.

Hybrid off-chain models can employ privacy-preserving computation. For instance, Xu's Offchain Trust Computation Engine could run inside a trusted execution environment or secure enclave, so that even sensitive behavior data within a group is processed confidentially [14]. This way, raw interaction data or personal details never leave the local node in plaintext. Similarly, a network of reputation oracles could aggregate users' ratings and publish only a hashed reputation value on-chain, keeping individual inputs hidden. This approach combines the benefits of decentralization with data minimization.

Data minimization and consent are increasingly emphasized. Schemes following Metaverse Standards Forum (MSF) guidelines limit what data is collected for reputation [65]. For example, instead of storing full chat logs for content moderation, a system might just store an "abuse flag count" or a hash of an incident report. Several works also stress user consent: linking real-world accounts (LinkedIn, GitHub) to a metaverse identity should only happen with explicit user approval. This not only respects privacy regulations but also ensures users remain in control of how their data is used in reputation calculations.

Encryption and anonymity techniques are suggested for feedback systems. One idea is to send feedback encrypted to a smart contract, which aggregates it and publishes a result, so individual ratings aren't traceable to the rater. This could prevent retaliation and enhance rater privacy. None of the surveyed schemes implemented this directly, but it's a potential improvement on the horizon perhaps using homomorphic encryption or threshold encryption in smart contracts. Overall, SSI-based and localized trust systems score high on privacy, whereas fully transparent on-chain systems score lower. It's evident that if people fear a metaverse reputation system will expose their every action or allow unwanted profiling, they may be reluctant to participate or will try to game the system. Thus, designers must strike a balance where trust is earned and verifiable, but personal data is protected. Some of the new schemes explicitly address this: for example, Mebrahtom et al. mention exploring Differential Privacy and Federated Learning to improve privacy in future iterations [42]. That could mean multiple platforms collaboratively computing reputation models without sharing raw data, or adding noise to data so individuals can't be re-identified, while still getting accurate aggregate scores. Similarly, Kuru et al. use of DPPML is exactly in line with this trend by using advanced privacy-preserving ML to authenticate without exposing data[49].

Techniques like ZK proofs, secure enclaves, MPC, and careful data policy (collect only what's needed, and only with consent) are key to making metaverse reputation systems privacy-friendly. We see early implementations of some of these ideas, but there is room to integrate more sophisticated privacy tech into future trust frameworks.

6.2. Interoperability and Standardization

Interoperability refers to a trust/reputation mechanism's ability to function across different platforms, virtual worlds, or even across different blockchains. This is crucial because users will not want to rebuild separate reputations from scratch in every metaverse application. Ideally, trust earned in one space should carry over to another, at least in a contextualized way.

Token-based approaches naturally lend themselves to technical interoperability. The Metaverse Standards Forum (MSF) scenario explicitly envisions such reputation data portability across platforms [4]. If your avatar has an "Oracle Certified Developer" SBT from a professional metaverse, a game metaverse might at least acknowledge it as proof you're not a bot. The obstacles here are more organizational than technical: platforms must agree on standards for interpreting each other's reputation tokens or scores. Efforts like the Metaverse Standards Forum (MSF) and Trust Over IP are aiming to create such standards [4,66]. For instance, they discuss common schemas for reputation credentials, APIs for querying reputation across worlds, and so on. If successful, these would allow a badge or score issued in one place to be understood in another without custom integration.

Score-based systems can also be interoperable, but typically require either a shared backend or bridging mechanisms. One approach is a consortium of metaverse platforms deploying a shared smart contract or set of contracts where they all write reputation data. This effectively creates a global reputation network on the blockchain. Another approach is through bridges/oracles: one platform can query another's rep service via an API or via a blockchain oracle. Some research specifically looks at cross-chain reputation. For example, Xia et al. [30] and Li et al. [46] consider reputation that travels across multiple blockchains – a user active on one chain carries their trust score to another chain's metaverse. In DareChain's multi-chain system, presumably one chain can vouch for a user on another via a synchronization mechanism, achieving interoperability between blockchains. These kinds of multi-chain or cross-chain setups are an active area, leveraging one chain as primary or periodic state syncing between chains to keep reputations aligned.

We also see proposals for middleware or services that facilitate interoperability. For instance, one could imagine Reputation-as-a-Service (RaaS) providers – essentially "credit bureaus" for the metaverse. These would be independent services or smart contracts that collect inputs from various platforms and produce a unified trust profile for users. Even platforms that weren't originally blockchain-based such as Roblox or Fortnite might integrate with these systems via bridges [67,68]. For example, Roblox could let users link their account to a blockchain wallet, then fetch their SBT credentials or an external rep score to influence in-game trust settings. This kind of Web2–Web3 integration is likely a transitional step toward a more fully interoperable future.

Interoperability remains one of the biggest open challenges. The technology pieces are mostly in place, but governance and standardization are the bigger hurdles. It's encouraging that industry consortia like MSF are explicitly prioritizing this. A likely near-future scenario is a coalition of major Web3 metaverse platforms agreeing on a basic reputation interchange format. That alone would instantly create a portable base reputation across those platforms. Our benchmark impression is that token/credential solutions are inherently more interoperable, whereas score systems need explicit integration or data sharing agreements.

6.3. Scalability and Performance

Scalability refers to how a scheme performs as the metaverse network and user base grows e.g. the latency of trust updates, throughput (transactions per second), and ability to handle many participants or interactions. Table 5 qualitatively compares the scalability strategies of each scheme and any available performance metrics. We list how each scheme handles growth and any known performance metrics or qualitative assessments. Latency, throughput, and computational overhead are noted where reported.

From Table 5, one can see different focuses: some schemes prioritize throughput, others focus on distribution of load, and others on minimizing on-chain operations to reduce bottlenecks. Notably, none of the surveyed schemes reported an insurmountable scalability problem in their tests – with careful design, each approach finds a way to handle growth, whether by scaling out or cutting down work.

One common trade-off is between real-time responsiveness and on-chain finality. Pure on-chain updates for every single interaction would be far too slow and costly in practice. Thus, schemes that need real-time trust decisions often perform those computations off-chain and only periodically sync important results to the blockchain. This leads to eventual consistency – which is acceptable if small delays in global reputation updates are tolerable. For instance, a user's displayed reputation in-world might update every few minutes in a batch, rather than immediately after every interaction, to allow efficient aggregation.

It's clear that no single scheme yet checks all the boxes – each balances the four criteria differently. An ideal metaverse trust system may need to hybridize multiple approaches, for example, using on-chain SBTs for portability, off-chain score computations for scalability, SSI for privacy, and robust consensus weighting for security. Although such a unified system is not yet fully realized, the components reviewed here indicate that it is feasible.

Table 5. Scalability strategies and reported performance across schemes.

Scheme	Scalability Strategy	Reported Performance
Awan et al. [27]	Decentralized trust decisions; trust-weighted consensus reduces agreement steps so reputable nodes drive consensus. Reputation monitoring avoids expensive recovery from misbehavior.	Processes 2000 nodes in 340 ms vs 520 ms baseline (≈ 35% faster). Integrating trust improved latency; near-linear scaling; graceful degradation; better throughput at scale.
Tu et al. [29] **— BTRM**	Dynamic updates and permissioned chain. Not every interaction triggers on-chain tx; reputation updates are batched/periodic. Uses Fabric's high TPS; idle users pruned.	On Fabric, practical runtimes for reputation updates; scaled to large IoT pools without linear cost growth; low latency by limiting heavy computation frequency.
Xu et al. [14]	Metaverse partitioned into trust groups; computations scale per group. Edge compute for local loads; blockchain coordinates groups; minimizes on-chain ops; groups subdividable.	Conceptual (no numerics). Qualitatively scales: new users add load only to their group. Hypergraph trust supports incremental growth; avoids single bottlenecks.
Li et al. [46] **— DareChain**	Collaborative multi-chain: parallel chains (shards) handle different interactions. Consensus scales with chains/nodes; layered contracts distribute load.	High throughput via parallelism; overall TPS grows nearly linearly with added chains; low per-tx latency as each shard handles smaller load; maintains security/privacy.
Mebrahtom et al. [42]	Off-chain interactions with on-chain verification. SSI setup amortized; no redundant re-checks per login; blockchain can be fast layer-2 backend.	Prototype on Ethereum: $authcost \approx signaturecheck(ms) + ledgerupdate$. Qualitatively supports thousands of logins/checks concurrently.
Patwe et al. [41]	SSI-based hybrid. Auth via off-chain wallet interactions, on-chain validation. Heavy compute peer-to-peer/client-side; chain logs events/revocations; no central auth server.	Measured auth ≈ $50.1ms$; comms 1256 bits. Lightweight enough for real-time VR login. Throughput limited by base chain; modern chains handle 100s–1000s TPS.
Kuru et al. [49]	Federated learning on device data; distributes compute across devices/edge. Blockchain stores checkpoints, not every interaction.	Early-stage concept. Scales with device count; per-user $authlatency \approx modelinferencetime$ (tens of ms for light models).
Xia et al. [30]	Lightweight consensus reduces messaging; reputation streamlines leader election. Multi-chain design: shards handle regions/contexts in parallel.	Simulations show higher throughput per chain; filtering low-rep nodes may reduce consensus from O(n) to O(m), $m \ll n$; capacity increases with more shards.
Liu et al. [62]	Permissioned PBFT with trust scores. Offloads reputation off-chain/in parallel; PBFT uses weights; dynamic node set.	Simulations: dozens of vehicles per region with sub-second blocks. PBFT efficient with filtering; large scale via partitioned regional chains.
Lotfi et al. [45]	Localized feedback loops; each region computes trust locally; regions run in parallel; incentive throttling; if on blockchain, use regional permissioned chains or DAG.	Dozens to few hundred vehicles in real time. For millions, hierarchical clusters; near-linear scale by deploying more servers; needs fast/sharded chains.
Truong et al. [36]	On-chain escrow contracts; every trade hits the chain. Batch on high-TPS networks; reputation updated per trade/audit.	Secure trading focus. Typical L1 escrow: few hundred ms. Thousands/sec possible on L2. Reputation writes are small; scales with chain improvements.
Song et al. [40]	Hierarchical fuzzy trust: split factors, compute in parallel off-chain, aggregate; updates periodic or on significant change.	No explicit metrics (prototype). Off-chain heavy lifting; on-chain only final scores/proofs. Supports very large user sets with distributed compute.
Soulbound Tokens [39]	Static reputational credentials; mint/read/store are efficient; updates infrequent; batch issuance supported.	Seen at NFT scale (millions of tokens). L2/sidechains give high throughput/low cost. Internet-scale feasible; per-user data small.

7. Open Challenges and Future Directions

While substantial progress has been made in designing blockchain-based trust and reputation systems for the metaverse, significant challenges remain before these mechanisms can be widely adopted in production platforms. Based on our expanded taxonomy and benchmark findings, we outline several open challenges and research directions. As shown in Table 6, each challenge in metaverse trust is addressed by specific blockchain-based solutions.

Table 6. Metaverse trust challenges and mapped blockchain solutions.

Challenge	Mapped Solutions
Cross-platform portability	• Token and credential standards (VCs, DIDs) • Cross-chain bridges and oracles
Privacy-preserving computation	• Zero-knowledge proofs (SNARKs/STARKs) • Differential privacy for analytics
Governance & fairness	• Token/credential standards for voting eligibility • DAO-based parameter voting and auditability
Real-time updates	• Real-time off-chain caches • Layer-2 rollups (optimistic/ZK)
Sybil resistance vs. openness	• Zero-knowledge proofs for eligibility • Proof-of-personhood options (privacy-preserving)
Data integrity & false inputs	• AI fraud/forgery filters at the edge • On-chain audit trails and provenance
Massive-scale performance	• Cross-chain bridges & oracles for load isolation • Layer-2 rollups; real-time off-chain caches
User experience & transparency	• On-chain audit trails surfaced in UX • Progressive-disclosure interfaces

7.1. Cross-Platform Reputation Portability:

Achieving true interoperability of trust across the multitude of metaverse worlds is non-trivial. Users desire a unified reputation that they can carry with them, yet today's implementations are largely siloed per platform. The MSF 2025 use-case explicitly calls for "Reputation data portable across platforms in the Metaverse," underscoring the demand for standards . The challenge is twofold: technical (different platforms and blockchains need to exchange data seamlessly) and organizational (platforms must agree to trust and interpret each other's reputation metrics). Future work should focus on standardizing reputation representations – for example, developing an open schema or token standard (perhaps an extension of SBTs or Verifiable Credentials) that multiple metaverses agree to use for issuing and accepting reputation data . Initiatives like a "Metaverse Reputation Interchange (MRI) protocol or trust APIs could emerge from industry collaboration. Cross-chain technology (bridges, oracle networks like Chainlink) can be leveraged to sync reputation state between blockchains. For instance, if one metaverse runs on Ethereum and another on Solana, a bridge or oracle could attest Alice's Ethereum-based rep when she joins the Solana world . Research into federated reputation models – where each platform maintains autonomy but contributes to a collective reputation score – may also prove valuable (similar in spirit to federated identity but for reputation).

7.2. Privacy-Preserving Reputation:

More privacy-enhancing techniques need to be integrated so that gaining trust doesn't mean losing anonymity or exposing personal data. As discussed, Zero-Knowledge Proofs (ZKPs) offer a promising avenue – users could prove they have a high reputation or certain credential without revealing details [69]. For example, one could prove "I have at least 3 SBT trust badges" or "My trust score is above 80" to a smart contract, which then simply outputs yes/no to the application without ever revealing which badges or the exact score . Similarly, applying Differential Privacy when aggregating feedback could allow global reputation stats to be computed without leaking individual user inputs (e.g. adding slight noise to large datasets of ratings to mask any single user's data). This is still an emerging area – using ZK-SNARKs or STARKs to prove complex reputation claims is computationally intensive today, but rapid advances in blockchain ZK tech could make it feasible . Another angle is Secure Multi-Party Computation (MPC): multiple nodes could jointly compute a reputation score from private inputs (ratings) such that no node sees all the inputs. Ensuring privacy also involves policy and UX: obtaining user consent for any linking of realworld data, providing opt-outs, and aligning with regulations (GDPR, CCPA, etc.) . Future research should explore privacy-preserving incentives – e.g., how to reward users for sharing certain data for reputation without compromising them. The concept of zero-knowledge credentials (where attributes are hidden but verifiable) will likely play a big role in metaverse identity and trust going forward.

7.3. Reputation Governance and Trust Constitution:

Decentralizing trust management raises the question of who defines and oversees the reputation algorithms and policies. In a centralized platform, the company sets the rules (e.g. how user reports translate to bans). In a decentralized metaverse, the community may need to govern this. We foresee DAO-based governance of reputation systems – where token holders or community members vote on parameters (how quickly does rep decay? what behaviors warrant penalties? etc.). However, governance itself can be attacked or captured (e.g. "reputation whales" with high standing might manipulate settings to favor themselves). It's an open challenge to ensure governance is balanced and not dominated by the rich-get-richer effect . Research could examine approaches like quadratic voting or soulbound governance tokens to give a more equitable voice (one idea: weight votes by something other than raw reputation to prevent the most reputed from having all the power) . Additionally, establishing an "Ethics Board" or Trust Council could help audit and guide these systems. The MSF discussions hint at some form of digital ethics oversight for reputation usage. Future reputation systems might include elected moderators or even AI watchdogs to ensure the algorithms are fair, not biased, and not being gamed. Embedding dispute resolution mechanisms is also key – users should have recourse if they feel their reputation was unfairly damaged. Decentralized arbitration (similar to Kleros or community juries) could be employed to handle reputation disputes in a transparent way.

7.4. Dynamic and Real-Time Reputation:

The metaverse is a live environment – think fast-paced games or live social hubs. Reputation systems need to keep up with real-time behavior. If someone starts griefing or cheating, others should know or the system should react almost immediately (e.g. to kick a bad actor out of an ongoing event). Yet, blockchains are not known for low-latency updates. There's a tension between the immediacy of trust decisions and the lag of on-chain finality. Future research can explore off-chain real-time reputation streams that later settle on-chain. One idea is a pubsub (publish/subscribe) model: user actions update a local reputation score instantly for the session, and these ephemeral scores are published to nearby users or moderators. Periodically, these could be anchored to the blockchain (e.g. a summary of the session's reputation deltas) for permanence. Also, leveraging faster consensus mechanisms – as Xia et al.'s lightweight consensus or other Layer-2 solutions aim to – can bring down the latency for on-chain parts. Another intriguing idea is predictive trust: using AI to predict who is likely to misbehave before they actually do, to preemptively adjust trust or trigger warnings . This is risky but could be useful for moderation (think of it as trust score meets anomaly detection). The "trust but verify" approach of Mebrahtom et al. captures a bit of this ethos: allow interactions freely but have the logs andverification ready to punish after the fact if needed. Ultimately, a hybrid approach might prevail: off-chain immediate reactions combined with on-chain eventual consistency. For example, an event server might maintain a live reputation scoreboard and use it for on-the-fly decisions, then submit the final reputations to the blockchain at the end of the event. The open challenge is reconciling blockchain's guarantees with the metaverse's real-time demands – perhaps dedicated sidechains for trust data or ultra-fast finality chains could be part of the solution.

7.5. Sybil Resistance vs. Openness:

There is a fine balance between clamping down on Sybils (fake identities) and keeping the metaverse open to new, pseudonymous users. Many Sybil defenses require verification (KYC, government IDs, etc.), but these measures can exclude users who value privacy or lack access to credentials. This is as much a social challenge as a technical one. A future direction is to develop Web of Trust models on blockchain – letting users vouch for new users in a decentralized way. For example, a new avatar could gradually earn trust through endorsements from already trusted users (similar to how PGP web-of-trust worked, or how certain forums require established members to sponsor newcomers) . Over time, a new user can become trusted without ever revealing a government ID, purely through on-chain history and community vouching. Some early crypto projects (e.g. BrightID) attempt this: creating Sybil-resistant identity via social graph analysis rather than formal IDs . Applying these in metaverse contexts will be important to maintain inclusivity. Another concept is Proof-of-Personhood protocols – essentially "unique human" proofs that don't reveal who the human is, just that they are unique. Examples include uniqueness via device key attestation, face recognition with privacy, or community verification parties. Integrating such protocols (e.g. POH, Idena, etc.) could prevent Sybils while keeping users anonymous. In short, research should continue on better human verification methods that avoid centralization and protect privacy, so that we don't force a heavily permissioned metaverse nor allow it to be overrun by bots. Handling False or Malicious Inputs: Reputation systems themselves can become targets. Malicious actors might spam fake positive or negative feedback, or hackers might compromise accounts to make a good user suddenly look bad (or vice versa). Mechanisms to ensure data integrity are crucial. Blockchain helps by making records immutable (nobody can retroactively fake history easily), but the old adage "garbage in, garbage out" still applies – if the inputs (ratings or claims) are false, the blockchain will faithfully record falsehoods. Future trust frameworks could use AI/ML to filter out implausible feedback, similar to fraud detection in finance. For instance, if a brand-new avatar suddenly receives 100 glowing reviews in an hour, the system can flag that as likely spam. Additionally, tying reputation events to verifiable on-chain actions increases veracity. One idea mentioned in our survey: only count a trade review if an actual trade NFT (escrow transaction) occurred on-chain . This prevents random users from bad-mouthing someone they never interacted with – the system would ignore feedback not linked to a real event. The general challenge is to harden the inputs to the reputation system: ensuring that what's being fed into the trust calculations is authentic and relevant. This could involve multi-factor reputation (cross-verifying user behavior with other data, like time spent, assets at risk, etc.), community validation (having certain feedback vetted by moderators or witnesses), or algorithmic outlier detection (automatically down-weighting feedback that looks suspicious or adversarial). Decentralized identity can help here too: if all feedback providers have skin in the game (reputation or stake), they're less likely to spam. Ongoing research into robust reputation algorithms (resistant to noise or attack) will continue to be important.

7.6. Scalability to Massive Scale:

While the works surveyed tested up to thousands or maybe millions of entities in simulations, a full-fledged global metaverse could involve hundreds of millions of users. At that scale, even storing everyone's reputation on-chain might become a big-data problem. Future systems might need to use off-chain storage with on-chain anchors (similar to how NFT metadata is stored on IPFS and only a hash on-chain). For example, detailed reputation histories could be kept in decentralized storage networks, and only summary hashes or scores are periodically anchored to the blockchain. This would keep on-chain data manageable while still being verifiable. Also, ensuring the algorithms themselves remain efficient is vital – ideally sub-linear complexity (not O(n) per update if n is huge). Techniques from graph processing and network science might be leveraged; for instance, algorithms like PageRank (essentially a kind of trust score computation on graphs) have been scaled to web-sized graphs. Adapting such algorithms for metaverse social graphs could allow reputation to be computed in a distributed way for millions of users. Some Web3 social projects (e.g. Lens Protocol) are indeed experimenting with using social graph metrics as reputational signals. The open issue is integrating those at scale with blockchain finality. We might see layer-2 networks or sharded networks dedicated to reputation data emerge if main chains can't handle the load. In summary, scaling trust to Internet scale will require both architectural solutions (sharding, layer-2, off-chain storage) and algorithmic improvements (efficient computation on large graphs, perhaps approximate reputation scores that can be refined progressively).

7.7. User Experience and Transparency:

An often overlooked challenge is making these trust systems understandable and acceptable to users. How do we present someone's reputation in the metaverse UI in a meaningful way? If it's just a number or badge, does that oversimplify things (cue the Black Mirror concerns about reducing people to a score). Users need context for why someone has a certain trust level – but providing that context must be done without violating privacy. Designing intuitive UIs that maybe show categories of trust (e.g. "great trader, verified identity, new to platform, no violations") instead of a single score could help. Also, users should have ways to appeal or contest their reputation if they believe it's unfair. This ties back to governance: perhaps there should be a dispute resolution mechanism as part of the system (for example, a user can flag their reputation as wrongly lowered, triggering a review by moderators or a community jury). Some proposals have considered decentralized arbitration for reputation – for instance, smart contracts that allow submitting evidence and a jury of peers (or an AI) to vote on restoring a reputation point if it was lost due to, say, a misunderstanding. Transparency of the algorithms is also important: the blockchain's openness can help (anyone can inspect the events that led to a score), but only if the system clearly links those events to the score. Users should be able to see "what did I do to earn this badge or lose those points?" in a clear manner, and have the tools to correct errors (maybe via the appeals process). Ensuring explainability of trust scores (akin to explainable AI, but for reputation) will build user trust in the system itself. Ultimately, a trust system will only be effective if users buy into it – and that requires they understand it, feel it's fair, and have agency in it.

7.8. Unified Evaluation and Collaboration:

As a meta-challenge, the research community needs to establish common benchmarks and testbeds for metaverse trust systems. Our survey found that different works use different assumptions and metrics, which makes direct comparison difficult. One promising direction is for researchers to collaborate on open simulation environments or datasets that can be used to evaluate new reputation mechanisms under standardized conditions. For example, a simulated metaverse city where a certain number of Sybil attackers, colluders, honest users, etc., are present, and new algorithms can be tested and compared on metrics like detection rate, false positives, latency, throughput, and privacy leakage. Defining these benchmarks would greatly accelerate progress – it would be easier to see which ideas truly perform better, and to combine the best features. Additionally, collaboration between academia, industry, and standards bodies is important so that solutions are not developed in isolation. An open-source reference implementation of a metaverse trust framework could allow contributors worldwide to plug in their consensus algorithm, their scoring logic, their credential scheme, and see how it all works together. This kind of interoperability at the research level will help ensure that when standards emerge, they are informed by a broad base of experiments and data. In short, the community should strive to "compare apples-to-apples" and work together on pilots in actual metaverse platforms to identify practical issues. Only through such unified efforts will the broader vision of a trust worthy metaverse come to fruition.

8. Conclusions

Trust and reputation systems will be foundational to the metaverse's success, enabling users to navigate virtual economies and communities with confidence. Blockchain technology provides powerful tools - decentralization, transparency, and immutability – to build these systems. We reviewed both permissionless and permissioned blockchain-based schemes: from on-chain trust scores that bolster security, to hybrid AI-blockchain models for moderating behavior, to cryptographic reputation tokens preserving privacy. We classified them by design choices and evaluated their strengths and weaknesses in security, scalability, privacy, and interoperability.

Our analysis shows that blockchain-based trust systems hold great promise. They introduce transparency, tamper-resistance, and decentralization to reputation management, solving many problems of legacy centralized systems. At the same time, our study makes clear that no single solution is sufficient in isolation. The metaverse is a complex and diverse ecosystem – a trust system for it must be equally nuanced and multifaceted. We highlighted key open challenges that must be addressed for widespread adoption: achieving interoperability through common standards, enhancing privacy via cryptography and careful design, building robust governance mechanisms, and ensuring scalability to millions of users in real time. In summary, blockchain-based trust and reputation mechanisms will be indispensable for a thriving decentralized metaverse. They provide a means to identify trustworthy individuals when traditional gatekeepers are absent, by combining the security of blockchain with the nuance of social trust metrics.

Supplementary Materials: The following supporting information can be downloaded at the website of this paper posted on Preprints.org.

Author Contributions: Conceptualization, F.K. and S.H.; literature search and screening, F.K. and H.M.A.; data curation , F.K.; validation, H.M.A. and S.M.; visualization , F.K.; writing—original draft preparation, F.K.; writing—review and editing, H.M.A., S.H., and S.M.; supervision, S.H. and S.M.; project administration, F.K.; resources, S.H.; funding acquisition, S.M. All authors have read and agreed to the published version of the manuscript.

References

1. Aygun, R.C.; Vural, T.; Zhang, L. Blockchain's Role in Metaverse Trust and Transactions. In Proceedings of the 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), 2023, pp. 786–792. https://doi.org/10.1109/MetaCom57706.2023.00148.

2. Decentraland Foundation. Decentraland Official Website, 2025. Accessed: 2025-06-17.
3. The Sandbox Team. The Sandbox Official Website, 2025. Accessed: 2025-06-17.
4. Metaverse Standards Forum. Unified Reputation Management for Metaverse Entities. Technical Report Version 1.0, Metaverse Standards Forum, 2025. Approved for Public Distribution; Last update: May 12, 2025.
5. Ghosh, A.; Hassija, V.; Chamola, V.; El Saddik, A.; et al. A Survey on Decentralized Metaverse using Blockchain and Web 3.0 technologies, Applications, and more. *IEEE Access* **2024**.
6. Gadekallu, T.R.; Huynh-The, T.; Wang, W.; Yenduri, G.; Ranaweera, P.; Pham, Q.V.; da Costa, D.B.; Liyanage, M. Blockchain for the metaverse: A review. *arXiv preprint arXiv:2203.09738* **2022**.
7. Qayyum, A.; Butt, M.A.; Ali, H.; Usman, M.; Halabi, O.; Al-Fuqaha, A.; Abbasi, Q.H.; Imran, M.A.; Qadir, J. Secure and Trustworthy Artificial Intelligence-extended Reality (AI-XR) for Metaverses **2024**. *56*. https://doi.org/10.1145/3614426.
8. Sathya, A.R. Blockchain: The Foundation of Trust in Metaverse; Springer International Publishing: Cham, 2023; pp. 117–129. https://doi.org/10.1007/978-3-031-22835-3_5.
9. Jim, J.R.; Hosain, M.T.; Mridha, M.F.; Kabir, M.M.; Shin, J. Toward Trustworthy Metaverse: Advancements and Challenges. *IEEE Access* **2023**, *11*, 118318–118347. https://doi.org/10.1109/ACCESS.2023.3326258.
10. Truong, V.T.; Le, L.; Niyato, D. Blockchain meets metaverse and digital asset management: A comprehensive survey. *Ieee Access* **2023**, *11*, 26258–26288.
11. Pattanayak, S.; Ramkumar, M.; Gupta, S. Blockchain Empowered Metaverse: Enhancing User Engagement through Trust, Collaboration, Authenticity, And Governance. *Information Systems Frontiers* **2025**. https://doi.org/10.1007/s10796-025-10622-1.
12. Perey, C. Interoperability is a Fundamental Requirement for the Open Metaverse. In Proceedings of the 2024 IEEE International Symposium on Emerging Metaverse (ISEMV). IEEE, 2024, pp. 21–24.
13. Al-kfairy, M.; Alomari, A.; Al-Bashayreh, M.; Alfandi, O.; Altaee, M.; Tubishat, M. A Review of the Factors Influencing Users' Perception of Metaverse Security and Trust. In Proceedings of the 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS), 2023, pp. 1–6. https://doi.org/10.1109/SNAMS60348.2023.10375478.
14. Xu, M.; Guo, Y.; Hu, Q.; Xiong, Z.; Yu, D.; Cheng, X. A trustless architecture of blockchain-enabled metaverse. *High-Confidence Computing* **2023**, *3*, 100088. https://doi.org/https://doi.org/10.1016/j.hcc.2022.100088.
15. Sky Mavis. Axie Infinity, 2024. Accessed: 2024-07-03.
16. Sky Mavis. Ronin Blockchain, 2024. Accessed: 2024-07-03.
17. Dapper Labs. Flow Blockchain. https://flow.com/, 2024. Accessed: 2025-07-03.
18. Immutable. What is Immutable X? https://docs.immutable.com/x/what-is-immutablex/, 2024. Accessed: 2025-07-03.
19. Mourtzis, D.; Angelopoulos, J.; Panopoulos, N. Blockchain integration in the era of industrial metaverse. *Applied Sciences* **2023**, *13*, 1353.
20. Gil, R.M.; Gutiérrez-Ujaque, D.; Teixidó, M. Analyzing the metaverse: Computer games, blockchain, and 21st-century challenge. *International Journal of Human–Computer Interaction* **2024**, *40*, 6758–6775.
21. Huynh-The, T.; Gadekallu, T.R.; Wang, W.; Yenduri, G.; Ranaweera, P.; Pham, Q.V.; da Costa, D.B.; Liyanage, M. Blockchain for the metaverse: A Review. *Future Generation Computer Systems* **2023**, *143*, 401–419. https://doi.org/https://doi.org/10.1016/j.future.2023.02.008.
22. Nguyen, C.T.; Hoang, D.T.; Nguyen, D.N.; Dutkiewicz, E. Metachain: A novel blockchain-based framework for metaverse applications. In Proceedings of the 2022 IEEE 95th Vehicular Technology Conference:(VTC2022-Spring). IEEE, 2022, pp. 1–5.
23. Duan, H.; Li, J.; Fan, S.; Lin, Z.; Wu, X.; Cai, W. Metaverse for Social Good: A University Campus Prototype. In Proceedings of the Proceedings of the 29th ACM International Conference on Multimedia (MM '21), New York, NY, USA, 2021; pp. 153–161. https://doi.org/10.1145/3474085.3479238.
24. Wang, Y.; Zhu, M.; Chen, X.; Liu, R.; Ge, J.; Song, Y.; Yu, G. The application of metaverse in healthcare. *Frontiers in Public Health* **2024**, *12*. Section: Digital Public Health, https://doi.org/10.3389/fpubh.2024.1420367.
25. Ali, S.; Abdullah.; Armand, T.P.T.; Athar, A.; Hussain, A.; Ali, M.; Yaseen, M.; Joo, M.I.; Kim, H.C. Metaverse in healthcare integrated with explainable AI and blockchain: enabling immersiveness, ensuring trust, and providing patient data security. *Sensors* **2023**, *23*, 565.
26. Karunarathne, L.; Ganesan, S.; Somasiri, N.; Pokhrel, S. Navigating the Future: Blockchain-based Metaverse in Education. *Journal of Information Technology and Digital World* **2024**, *6*, 373–387.

27. Awan, K.A.; Din, I.U.; Almogren, A.S.; Seo-Kim, B. Blockchain-Based Trust Management for Virtual Entities in the Metaverse: A Model for Avatar and Virtual Organization Interactions. *IEEE Access* **2023**, pp. 1–1. Published January 2023, https://doi.org/10.1109/ACCESS.2023.3337806.
28. Awan, K.A.; Ud Din, I.; Almogren, A.; Kim, B.S. Enhancing Performance and Security in the Metaverse: Latency Reduction Using Trust and Reputation Management. *Electronics* **2023**, *12*. https://doi.org/10.3390/electronics12153362.
29. Tu, Z.; Zhou, H.; Li, K.; Song, H.; Yang, Y. A Blockchain-based Trust and Reputation Model with Dynamic Evaluation Mechanism for IoT. *Computer Networks* **2022**, *218*, 109404. https://doi.org/https://doi.org/10.1016/j.comnet.2022.109404.
30. Xia, P.; Li, J.; Shi, L.; Cao, B.; Tan, W.; Weng, J.; Liu, Y.; Han, Z. A Reputation-Aided Lightweight Consensus Service Framework for Multi-Chain Metaverse. *IEEE Network* **2024**, *38*, 201–210. https://doi.org/10.1109/MNET.2024.3382346.
31. Rahaman, M.F.; Mohtasin, G.; Subhan, M.; Tuli, E.; Kim, D.S.; Lee, J.M. Meta-Governance: Blockchain-Driven Metaverse Platform for Mitigating Misbehavior Using Smart Contract and AI. *IEEE Transactions on Network and Service Management* **2024**, *PP*, 1–1. https://doi.org/10.1109/TNSM.2024.3419151.
32. Dimitriou, T. Decentralized reputation. Cryptology ePrint Archive, Paper 2020/761, 2020.
33. Baccour, E.; Erbad, A.; Mohamed, A.; Hamdi, M.; Guizani, M. A Blockchain-Based Reliable Federated Meta-Learning for Metaverse: A Dual Game Framework. *IEEE Internet of Things Journal* **2024**, *11*, 22697–22715. https://doi.org/10.1109/JIOT.2024.3383096.
34. Lin, Y.; Gao, Z.; Du, H.; Niyato, D.; Kang, J.; Xiong, Z.; Zheng, Z. Blockchain-Based Efficient and Trustworthy AIGC Services in Metaverse. *IEEE Transactions on Services Computing* **2024**, *17*, 2067–2079. https://doi.org/10.1109/TSC.2024.3382958.
35. Kharvi, P.L. A Design Science Framework for Measuring Trust and Security in the Metaverse Space: A Holistic Approach to Digital Trustworthiness. Doctor of science in cybersecurity dissertation, Marymount University, College of Business, Innovation, Leadership, and Technology, 2025. Committee: Andrew Hall (Chair), Nathan Green, Susan Conrad, Glenn Robertson (External Reviewer). Dean: Anne Magro.
36. Truong, V.T.; Le, H.D.; Le, L.B. Trust-Free Blockchain Framework for AI-Generated Content Trading and Management in Metaverse. *IEEE Access* **2024**, *12*, 41815–41828. Received 15 February 2024, accepted 8 March 2024, published 18 March 2024, current version 22 March 2024, https://doi.org/10.1109/ACCESS.2024.3376509.
37. Ud Din, I.; Habib Khan, K.; Almogren, A.; Zareei, M.; Arturo Pérez Díaz, J. Securing the Metaverse: A Blockchain-Enabled Zero-Trust Architecture for Virtual Environments. *IEEE Access* **2024**, *12*, 92337–92347. https://doi.org/10.1109/ACCESS.2024.3423400.
38. Ghirmai, S.; Mebrahtom, D.; Aloqaily, M.; Guizani, M.; Debbah, M. Self-Sovereign Identity for Trust and Interoperability in the Metaverse, 2023, [arXiv:cs.CR/2303.00422].
39. Ohlhaver, P.; Weyl, E.G.; Buterin, V. Decentralized Society: Finding Web3's Soul. Technical Report 4105763, SSRN Electronic Journal, 2022. Posted: 11 May 2022; Last revised: 6 Feb 2024.
40. Song, X.; Xu, G.; Huang, Y. A Fuzzy AHP-based trust management mechanism for self-sovereign identity in the metaverse. *Applied Soft Computing* **2025**, *174*, 112994. https://doi.org/https://doi.org/10.1016/j.asoc.2025.112994.
41. Patwe, S.; Mane, S.B. Blockchain-enabled secure and interoperable authentication scheme for metaverse environments. *Future Internet* **2024**, *16*, 166.
42. Mebrahtom, D.; Hadish, S.; Sbhatu, A.; Aloqaily, M.; Guizani, M. Trust But Verify - Blockchain-Empowered Decentralized Authentication Schema on the Metaverse: A Self-Sovereign Identity Approach. In Proceedings of the 2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA), 2023, pp. 1–8. https://doi.org/10.1109/iMETA59369.2023.10294349.
43. Gebre, D.; Hadish, S.; Sbhatu, A.; Aloqaily, M.; Guizani, M. Establishing Trust and Security in Decentralized Metaverse: A Web 3.0 Approach. *ACM Transactions on Multimedia Computing, Communications, and Applications* **2024**, *20*, 1–17. https://doi.org/10.1145/3696454.
44. Ling, A.; Butakov, S. Trust framework for self-sovereign identity in metaverse healthcare applications. *Data Science and Management* **2024**, *7*, 304–313. Open Access; retrieved via DOAJ.
45. Lotfi, I.; Qaraqe, M.; Ghrayeb, A.; Niyato, D. VMGuard: Reputation-Based Incentive Mechanism for Poisoning Attack Detection in Vehicular Metaverse. *IEEE Transactions on Vehicular Technology* **2025**, *74*, 10255–10267. https://doi.org/10.1109/TVT.2025.3543650.

46. Li, Q.; Kong, L.; Min, X.; Zhang, B. DareChain: A Blockchain-Based Trusted Collaborative Network Infrastructure for Metaverse. *International Journal of Crowd Science* **2023**. https://doi.org/10.26599/IJCS.2023.9100025.
47. Liu, L.; Feng, J.; Wu, C.; Chen, C.; Pei, Q. Reputation management for consensus mechanism in vehicular edge metaverse. *IEEE Journal on Selected Areas in Communications* **2023**, *42*, 919–932.
48. Awan, K.A.; Ud Din, I.; Almogren, A.; Rodrigues, J.J.P.C. QSTMF: Quantum-Secured Trust Management Framework for VANETs in Web 3.0 and Metaverse. *ACM Trans. Auton. Adapt. Syst.* **2025**. https://doi.org/10.1145/3735672.
49. Kuru, K.; Kuru, K. Blockchain-Based Decentralised Privacy-Preserving Machine Learning Authentication and Verification With Immersive Devices in the Urban Metaverse Ecosystem. *Preprints. https://doi.org/10.20944/preprints202402* **2024**, *317*, v1.
50. Cao, Y.; Cao, J.; Cui, Z.; Bai, D.; Zhang, M.; Wen, L. PolyTwin: Edge Blockchain-empowered Trustworthy Digital Twin Network for Metaverse. In Proceedings of the 2024 IEEE International Conference on Metaverse Computing, Networking, and Applications (MetaCom), 2024, pp. 81–88. https://doi.org/10.1109/MetaCom62920.2024.00026.
51. Islam, S. Trust in digital asset transactions in a web 3 based metaverse. Master's thesis, OULU Business School, University of OULU, 2023.
52. Civic Technologies, Inc.. Civic Whitepaper: A Secure Identity Ecosystem. https://www.civic.com/, 2021. Accessed: 2025-06-17.
53. Chainlink Labs. Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks. https://research.chain.link/whitepaper-v2.pdf, 2021. Accessed: 2025-06-17.
54. Vijitha, S.; Anandan, R. Blockchain-based decentralized identifier in metaverse environment for secure and privacy-preserving authentication with improved key management and cryptosystem. *Peer-to-Peer Networking and Applications* **2025**, *18*. Received: 05 April 2024; Accepted: 13 May 2025; Published: 12 June 2025, https://doi.org/10.1007/s12083-025-02020-w.
55. Cao, Y.; Cao, J.; Bai, D.; Wen, L.; Liu, Y.; Li, R. MAP the Blockchain World: A Trustless and Scalable Blockchain Interoperability Protocol for Cross-chain Applications, 2024, [arXiv:cs.CR/2411.00422].
56. Ding, Y.; Huang, W.; Liang, H.; Wang, Y.; Yang, C.; Wang, H. A Fast Cross-Chain Protocol Based on Trusted Notary Group for Metaverse. *International Journal of Network Management* **2025**, *35*, e2302, [https://onlinelibrary.wiley.com/doi/pdf/10.1002/nem.2302]. e2302 nem.2302, https://doi.org/https://doi.org/10.1002/nem.2302.
57. Kausar, F.; Senan, F.M.; Asif, H.M.; Raahemifar, K. 6G technology and taxonomy of attacks on blockchain technology. *Alexandria Engineering Journal* **2022**, *61*, 4295–4306.
58. Hameed, K.; Barika, M.; Garg, S.; Amin, M.B.; Kang, B. A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues. *Journal of Industrial Information Integration* **2022**, *26*, 100312.
59. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal* **2018**, *6*, 2188–2204.
60. Garg, K. Digital identities in the metaverse: Privacy, security, and user authentication in virtual financial systems. *International Journal of Financial Engineering* **2024**, *11*, 2442009.
61. OpenSea: NFT Marketplace. https://opensea.io/. Accessed: 2025-06-23.
62. Liu, W.; Cao, B.; Peng, M.; Li, B. Distributed and parallel blockchain: Towards a multi-chain system with enhanced security. *IEEE Transactions on Dependable and Secure Computing* **2024**.
63. Lin, Q.; Gu, B.; Nawab, F. RollStore: Hybrid Onchain-Offchain Data Indexing for Blockchain Applications. *IEEE Transactions on Knowledge and Data Engineering* **2024**.
64. Kausar, F.; Sadiq, M.A.K.; Asif, H.M., Convergence of Blockchain in IoT Applications for Heterogeneous Networks. In *Real-Time Intelligence for Heterogeneous Networks: Applications, Challenges, and Scenarios in IoT HetNets*; Al-Turjman, F., Ed.; Springer International Publishing: Cham, 2021; pp. 71–86. https://doi.org/10.1007/978-3-030-75614-7_5.
65. Hemphill, T.A. The 'metaverse'and the challenge of responsible standards development. *Journal of Responsible Innovation* **2023**, *10*, 2243121.
66. Trust Over IP Foundation. Trust Over IP Foundation, 2025. Accessed: 2025-06-30.
67. Roblox Corporation. Roblox, 2025. Accessed: 2025-06-30.
68. Epic Games. Fortnite, 2025. Accessed: 2025-06-30.

doi:10.20944/preprints202510.1172.v1

69. Fiege, U.; Fiat, A.; Shamir, A. Zero knowledge proofs of identity. In Proceedings of the Proceedings of the nineteenth annual ACM symposium on Theory of computing, 1987, pp. 210–217.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.