University Of AL-Qadisiyah
Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Toward a Trustworthy and Interoperable Metaverse: A Systematic Review of Blockchain-Based Enhancements

Muhammed Abdulkhaliq Naseef [a], Ahmed Chalak Shakir [b]

[a]Department of Computer Science, College of Computer Science and Information Technology, University of Kirkuk, Iraq.Email: stcm22012@uokirkuk.edu.iq

[b]Department of Information Technology, College of Computer Science and Information Technology, University of Kirkuk, Iraq.Email: ahmedchalak@uokirkuk.edu.iq

ARTICLE INFO

Article history:
Received: 18 /06/2025
Rrevised form: 10 /07/2025
Accepted : 13/07/2025
Available online: 30/09/2025

Keywords:

Blockchain, metaverse, security, trust, interoperability, decentralized identity, cross chain protocols, Systematic literature review

ABSTRACT

The integration of blockchain technology with the metaverse has the potential to revolutionize online interaction by enabling secure, trustworthy, and interoperable virtual environments. This systematic literature review (SLR) explores how blockchain technologies can address fundamental challenges within the metaverse, particularly concerning security, trust, and interoperability. Eighteen research articles published between 2020 and 2025 were examined from top academic databases and grouped into three main topics: security methods using blockchain, systems for decentralized trust, and protocols for working across different platforms. The results show that blockchain's decentralization, immutability, and cryptographic foundations enable robust authentication, secure data exchange, and trustless identity systems. Additionally, blockchain facilitates seamless integration between diverse metaverse platforms through smart contracts, cross-chain protocols, and tokenized assets. Despite significant promise, challenges such as computational overhead, real-world deployment limitations, and lack of standardization persist. This review offers a consolidated foundation for ongoing research and proposes directions for integrating blockchain into scalable and reliable metaverse ecosystems.

https://doi.org/10.29304/jqcsm.2025.17.32368

∗Corresponding author: Muhammed Abdulkhaliq Naseef

Email addresses: *stcm22012@uokirkuk.edu.iq*

Communicated by ‘sub etitor’

1. Introduction

The advent of the metaverse signifies a pivotal moment in the evolution of digital space, facilitating immersive virtual environments that interact with real-world infrastructure and reality [1].The term "Metaverse" was initially presented in Neal Stephenson's 1992 novel, Snow Crash. [2].The metaverse has transitioned from a mere hypothetical concept to a tangible technical domain, underpinned by advancements in virtual reality (VR), augmented reality (AR), artificial intelligence (AI), Internet of Things (IoT), and, crucially, blockchain technology [3]. Platforms such as Meta's Horizon Worlds, Decentraland, Sandbox, Axie Infinity, Illuvium, and Roblox exemplify first developments in this digital frontier, prompting both industry and academia to acknowledge its potential to transform areas including education, healthcare, entertainment, and commerce [4]. The metaverse, as a digital ecosystem, will demonstrate permanence, immersion, interoperability, and decentralization, enabling individuals to socialize, trade, and collaborate inside 3D virtual worlds that bridge physical and digital realities [2], [5].

Despite its potential, the metaverse faces significant challenges, including centralized control, fragmented identity systems, data privacy concerns, and the lack of secure, interoperable models. These problems constrain the metaverse' s capacity to operate as a truly transparent and reliable environment. The use of blockchain technology, with its characteristics of a distributed nature, transparent tracking, and verifiability, was suggested as a baseline solution to overcome these problems [6]. Nevertheless, sources are limited due to the fact that blockchain and the metaverse are often viewed as separate entities, and existing literature relies on collecting information.

Blockchain technology, defined by decentralization, immutability, transparency, and verifiability, is seen essential for resolving security, trust, and interoperability issues in the Metaverse [7]. It empowers users through mechanisms such as decentralized identity (DID), smart contracts, decentralized finance (DeFi), and non-fungible tokens (NFTs), which provide secure asset ownership, governance, and peer-to-peer interactions devoid of centralized authority.

Although the studies on blockchain and metaverse technologies are available independently, there is no established unique research that specifically explores how blockchain can benefit the metaverse regarding security, trust, and interoperability. The volume of literature is increasing; however, much of it still consists of conceptual discussions, surveys, or general overviews rather than empirical and implementation-based studies. Consequently, existing literature often lacks any coherent or viable context, containing isolated opinions or limited situations without a complete or working context. This fact brings out one of the critical gaps in the literature and reasons why the research should be conducted comprehensively and empirically on how to properly integrate decentralized technologies into the realm of realistic virtual worlds.

This review fills these gaps by analyzing 18 scholarly articles published in 2020–2025.It looks at current blockchain-based methods in three main areas: security, trust, and interoperability. The review then evaluates the advantages and disadvantages of these methods, as well as their readiness for implementation. The goal is to give researchers and developers who want to build trustworthy and interoperable metaverse ecosystems using blockchain technology a clear, organized picture of the state of the art and useful advice on how to do it. the research questions that would guide this systematic literature review include the following:

- RQ1: How can blockchain technology enhance security within metaverse environments?
- RQ2: How can blockchain foster trust among users in the metaverse?
- RQ3: How can blockchain enable metaverse system interoperability?

Table 1: List of abbreviations

Abbreviation	Full term

SLR	Systematic Literature Review
VR	Virtual Reality
AR	Augmented Reality
MR	Mixed Reality
XR	Extended reality
IoT	Inter Of Things
AI	Artificial Intelligence
DID	Decentralized Identity
Defi	Decentralized Finance
NFT	None Fungible Token
CPU	Central Processing Unit
GPU	Graphical User Interface
3D	Three– dimensional
NPCs	Non-Player Characters
DT	Digital Twin
CT	Computed Technology
MRI	Magnetic Resonance Imaging
PoW	Proof of Work
PoS	Proof of Stake
ZKP	Zero-Knowledge Proof
P2P	Peer to Peer
ERC	Ethereum Request for Comment
AXS	Axie Infinity Shards
SLP	Smooth Love Potion
ILV	Illuvium
sILV	Synthetic Illuvium
ZK-rollups	Zero-Knowledge Rollups
AAA	Triple-A Game
PBFT	Practical Byzantine Fault Tolerance
BAN Logic	Burrows–Abadi–Needham Logic
PUF	Physical Unclonable Function
SBAC	Substitution Cipher Access Control
OTCE	On-demand Trusted Computing Environments
SSI	Self-Sovereign Identity
BVM	Blockchain Virtual Machines
TCRA	Trust-Centric Resource Allocation
PoT	Proof-of-Trust
DDoS	Distributed Denial of Service
HTLC	Hash TimeLock Contract
MITM	Man-in-the-Middle
DoS	Denial Of Service
HCNCT	Hash Timelock Contract Combine Notary Mechanisms Cross-chain Transaction
ETH	Ethereum

2. Background
2.1 Metaverse
2.1.1 An Architectural Overview
The architecture of the metaverse expands from people's experiences to the underlying enabling technologies and comprises seven layers [8], [9], [10], as illustrated in Figure 1 and briefly described below.

- The infrastructure layer will provide support for the metaverse by enhancing its network and computing foundations. It involves technologies such as 5G/6G, cloud computing, cloud service data centers, and high-performance processors (CPUs, GPUs, and quantum computers) so that content can be delivered quickly and with minimal latency.
- The interface layer consists of the gadgets and applications that allow people to access and interact with the metaverse, including VR glasses, AR eyewear, and smartphone applications.
- The decentralization layer ensures that no single party controls the metaverse. Applies blockchain to safeguard the autonomy of users, authorize the ownership of digital assets, and foster safe exchanges.
- The spatial computing layer combines technologies such as VR, AR, MR, and haptics to blend the physical and digital worlds, allowing us to experience a 3D world.
- The Creator Economy layer equips users with tools to author, distribute, and monetize their content, fostering a culture of innovation and a healthy digital ecosystem.
- The Discovery layer is a discovery component that enables finding content, experiences, and communities through search, recommendations, and social links.
- The Experiences Layer covers all components in the metaverse, including gaming, socializing, learning, and shopping, making the metaverse an enjoyable and significant experience for users.

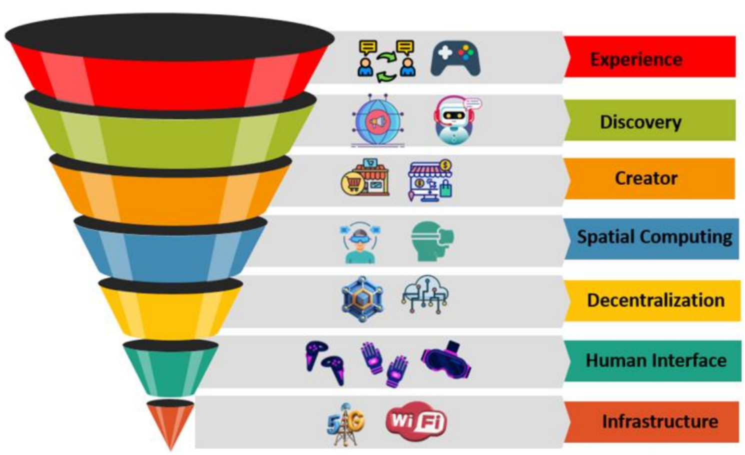

Figure 1: different layers in metaverse.

2.1.2 Key Enabling Technologies for the Metaverse

The metaverse is perceived as the next-generation three-dimensional representation of the Internet, arising from the amalgamation of various advanced technologies, each essential in defining its architecture and operation. Below is a brief description of the main enabling technologies which are depicted in Figure 2.

- Immersive experiences: are facilitated by interactive technologies, including Augmented Reality (AR), Virtual Reality (VR), and Extended Reality (XR). These allow users to engage visually and physically through wearable devices like VR headsets and haptic gloves [5].

- Digital Twin: employs real-world data to generate digital representations of physical entities. It facilitates the synchronized attribute of the metaverse, permitting the coexistence of physical and virtual realities. Real-world things can manifest in the virtual realm, and alterations made to these objects in the digital domain will be mirrored in the actual world [11], [12].

- Artificial Intelligence (AI): enhances the metaverse by providing intelligent services like smart non-player characters (NPCs), automatic translation, and personalized avatars that can mimic users' emotions and expressions.AI supports other technologies, including the Internet of Things (IoT), DT, and blockchain [13].

- The Internet of Things (IoT): consisting of numerous interconnected sensors and cameras, creates significant data for the metaverse. This technology allows for the development of a digital twin, effectively mapping the physical world to the virtual realm and vice versa [14], [15].

- Cloud and Edge Computing: play a crucial role in this context. Although wearable devices often have limited processing power and storage capacity, the servers that run metaverse applications and services can become overwhelmed by the large number of users interacting with the platform. Therefore, it is essential to effectively integrate and utilize modern cloud and edge computing solutions to process the vast amounts of data in the metaverse while ensuring the necessary quality of service [5] [15] .

- Communication and Networking Technologies: The substantial data produced by a vast number of global users and their online activities necessitates a rapid and highly dependable network infrastructure [5]. Moreover, cutting-edge communication technologies can be utilized to ensure low latency and high-speed connections, mitigating motion sickness associated with VR equipment, hence enhancing user experience and fostering greater social acceptance of the metaverse [16].

- Blockchain technology provides a decentralized and secure foundation for the metaverse, facilitating digital economies through NFTs, cryptocurrencies, and decentralized finance (DeFi) while ensuring reliable data management [17].

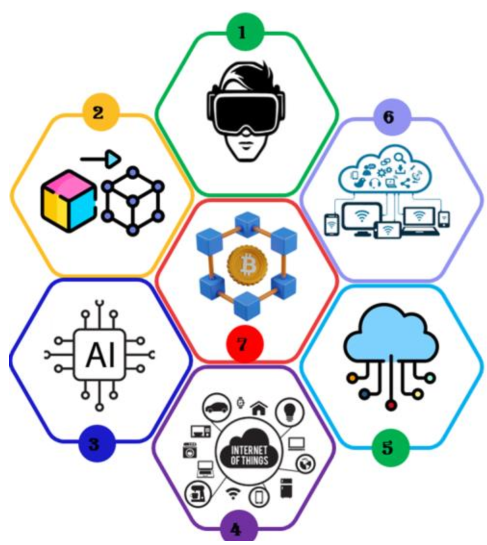

Figure 2. Metaverse technologies.

2.1.3 Metaverse Applications

The list below describes some of the most significant applications of the metaverse, which is shown in Figure 3.

- Entertainment: The most popular metaverse app is entertainment, which lets you have immersive experiences through movies, virtual concerts, games, and online sports. Users can talk to each other in real-time using avatars in shared virtual areas [18]. AI improves these experiences by enabling smart NPCs, realistic animations, lifelike music performances, and high-quality sound and visuals, making the environment more captivating and authentic[19] .

- Education: The metaverse improves online learning by making realistic surroundings that make standard videoconferencing systems work better. It looks like real classrooms, yet there are still problems with teaching hands-on. AI-powered tutors and haptic technologies, on the other hand, can give students individualized and engaging learning experiences. Also, virtual simulations let people practice skills like surgery safely and cheaply, lowering real life's dangers [20].

- Healthcare: Augmented and virtual reality (AR/VR) are changing healthcare by improving medical training, lowering expenses, and making surgery safer. Tools like Microsoft HoloLens let doctors see patient data and images (CT, MRI, and 3D scans) in real-time, which helps with diagnosis and surgery. AR also makes it easier to find veins, especially in tough instances. Research indicates that virtual reality in surgical training can enhance performance by more than 230% [21].

- Real estate: The metaverse improves real estate by enabling clients to take virtual tours of homes with music, lighting, and interactive information. This saves time, cuts down on travel, makes purchasers feel more sure about their decisions, and enables you to tailor experiences to each client's demands [20].

- Tourism: With virtual tourism in the metaverse, people can visit places without leaving their homes by using VR and AR to experience them fully. It has realistic, dynamic worlds you can share with others, making it easier to use and more fun [22].

- Fashion & Shopping: The metaverse is transforming the fashion and retail sector by allowing individuals to make purchases in 3D shopping and purchase virtual fashion pieces. Design houses like Gucci have also begun selling virtual goods (on platforms such as Roblox). The price of some things, such as a digital Gucci bag, can reach up to $4,000. Firms such as Zara and Nike integrate their retail and online stores and give their customers tangible and intangible products. Virtual fashion will also be an essential source of revenue as more people use NFTs. We may soon alter how humans buy online due to such services as Roblox, virtual stores [20]

- Smart cities: The idea of smart cities is to digitalize urban life with the help of progressive technologies. They use VR, AR, IoT, AI, the internet, and blockchain to support urban life as they become "Metaverse Cities." The technologies are compatible with sustainability, economic development, social visions, and quality of life for citizens [6].

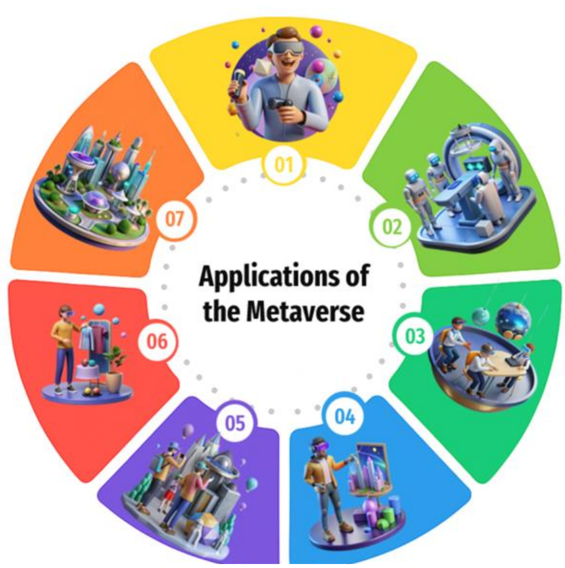

Figure 3. Applications of the metaverse.

2.2 Blockchain

2.2.1 Fundamentals of blockchain technology

The blockchain concept was initially conceived in 2008 by a researcher who used it to the digital currency Bitcoin [23] to address Europe's economic challenges [24]. Blockchain is a decentralized database that use encryption to avert manipulation and operates without a central authority, relying instead on the consensus of its network participants. The blockchain database expands with the addition of new blocks, and data removal is contingent upon the approval of the majority or all network participants [25]. A blockchain network consists of blocks that document encrypted transaction data on a distributed, decentralized ledger[26]. The initial "genesis block" has a hash value that connects it to the subsequent block. Each block comprises two primary components: the block header and the block data. The block header contains the version, the Merkle root hash, the hash of the preceding block, the timestamp, the difficulty goal (nBits), and a nonce. The block data contains the transaction particulars. The Merkle tree method secures data by repeatedly hashing transactions in pairs until a singular hash value, known as the Merkle root, is obtained [27], [28]. Figure 4 shows the blockchain structure.

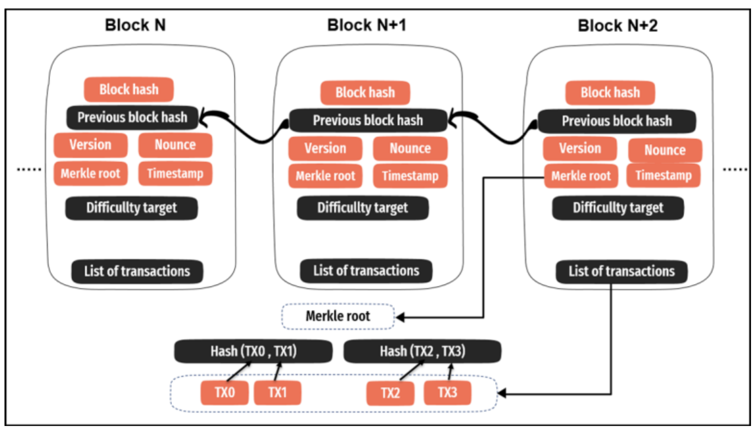

Figure 4: Blockchain Structure

2.2.2 Core blockchain Technologies in Metaverse

Blockchain technology plays a crucial role in developing a safe, decentralized, and effective metaverse, which is constructed based on four key elements: distributed storage, consensus mechanism, smart contracts, and cryptography. Figure 5 illustrates the core blockchain technologies.

- A distributed storage network is based on the distributed ledger. All data is stored across multiple nodes in an immutable and transparent manner, with each node having a copy of the ledger and independently verifying transactions. It does not require central servers and is therefore more fault-tolerant, more secure, and more user-privacy resistant, unlike legacy client-server architecture, which has reduced fault-tolerance and increased maintenance costs due to single points of failure [1], [29].

- The consensus mechanism provides decentralized control, as all nodes in the network accept the validity of the available data. The two most important models are Proof of Work (PoW), which uses high energy to solve cryptographic puzzles, and Proof of Stake (PoS), a more efficient process that uses token possession as its form of validation authority. The mechanisms ensure the integrity of the data being stored and provide remote and decentralized access to the metaverse for any region of the world [3].

- Smart contracts are self-executing pieces of code that run on a blockchain (such as Ethereum) and follow a fixed set of rules. They automate transactions, eliminating the need for intermediaries. They enable self-referencing activities, the management of digital assets, copyright protection, and even the governance of the metaverse and are programmed in languages such as Solidity. Nodes execute transactions, and the blockchain permanently records them [1].

- Blockchain security is based on protocols in cryptography, including asymmetric encryption, hash algorithms, and zero-knowledge proof (ZKP). Asymmetric encryption protects all of this, facilitating everything from the encryption of communication to the digital confirmation of identity through digital signatures and highly efficient, tamper-free data storage via hashing. ZKPs enable users to establish ownership or identity without disclosing any sensitive information, which is a more effective way to improve privacy and scalability. All of these technologies create a robust basis for a decentralized, transparent, secure, and fair Metaverse [1][6].

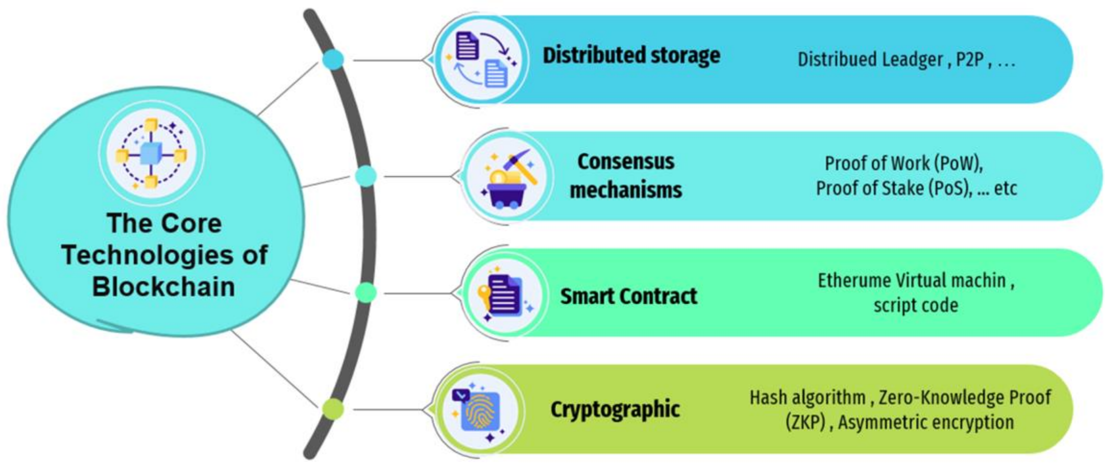

Figure 5: The core technologies of blockchain

2.3 Blockchain Based Metaverse Platform

Numerous metaverse platforms have utilized blockchain technology to establish decentralized virtual real estate, gaming ecosystems, and digital commerce services [4], [7], [30]. These platforms demonstrate how decentralized infrastructures enable individuals to possess assets, engage with one another, and transact value in immersive settings. Table 1 presents a comparative analysis of these initiatives, while Figure 6 displays images of their virtual landscapes.

1. Decentraland is a 3D virtual reality world runs on the Ethereum blockchain, and individuals can purchase, trade, and resell virtual land and in-game items. It uses two tokens: MANA (an ERC-20 token) and LAND (an ERC-721 NFT). It can be used to do many things, including creating content, creating games, advertising, and allowing individuals to trade in digital collectible assets, as well as providing them with a platform where they can have immersive socializing experiences. To avoid slow transactions and high fees on the Ethereum network, Decentraland integrates Polygon as a sidechain.

2. The Sandbox is a game-focused metaverse built on the Ethereum blockchain where users can buy, sell, play, create, and govern. The Sandbox uses three tokens (SAND (ERC-20), ASSETS (ERC-721) and LAND (ERC-1155), etc.) to power its ecosystem. The Sandbox will be integrating with Polygon to support scalability and increase speed and lower costs, reduce delays in transaction times and volume limits.

3. Axie Infinity is a blockchain gaming universe on Ethereum and Binance Smart Chain where players collect, breed and battle creatures called Axies. Players are rewarded with AXS and SLP fungible tokens. For speedier transactions, Axie Infinity has introduced Ronin, it's own Ethereum sidechain, to help improve performance and scalability for its large user base.

4. Illuvium is an AAA blockchain game on the Ethereum blockchain which uses ILV as its native token, and sILV as its in-game currency. It combines elements of immersive gameplay and decentralized governance where players can stake their native ILV tokens to earn rewards and participate in the governance side of game decision-making. Although some elements of game functions use Ethereum, Illuvium will employ layer-2 scaling solutions such as Immutable X and zero-knowledge rollups (ZK-rollups) in order to further improve scalability, lower gas costs, and easily carry-out in-game transactions.

Table 1: Comparison of blockchain-based metaverse projects

Platform	Blockchain Network	Token Used	Main use cases	Scalability solution
Decentraland	Ethereum + Polygon (sidechain)	MANA (ERC-20), LAND (ERC-721)	Virtual land trading, content creation, social experiences	Polygon sidechain
Sandboxe	Ethereum (Polygon integration planned)	SAND (ERC-20), ASSETS (ERC-721), LAND (ERC-1155)	Game creation, digital asset trading, user governance	Polygon integration planned
Axie Infinity	Ethereum + Binance Smart Chain + Ronin (sidechain)	AXS, SLP (fungible tokens)	Breeding, battling Axies, earning rewards	Ronin sidechain
Illuvium	Ethereum (using Immutable X, ZK-rollups)	ILV (native), sILV (in-game)	AAA gameplay, staking, governance, earning	Immutable X, ZK-rollups

Figure 6: Blockchain based metaverse projects

3. Methodology

3.1 Study Design

This study employs a Systematic Literature Review (SLR) methodology to investigate the potential of blockchain technology to improve security, interoperability, and trust in the metaverse. The assessment emphasizes peer-reviewed journal articles, conference papers, and high-caliber preprints from 2020 to 2025.

3.2 Search Strategy and Data Sources

The literature search was conducted across major academic databases, including IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and arXiv. We searched using the following keywords: Metaverse, Blockchain, Security, trust, Interoperability, Decentralized Identity, Smart Contracts, Virtual Worlds, NFT, and Cross-Chain.

3.3 Inclusion and Exclusion Criteria Inclusion

Papers about blockchain-based security, trusting or interoperability solutions in the metaverse; propositions of articles outlining new solutions.
Exclusion: Papers that do not discuss blockchain; duplicate; papers that are irrelevant to the metaverse context.

3.4 Data Extraction

In each study, data were extracted regarding the publication year, methodology type, the blockchain application domain, blocks and chain tools utilized, key findings, and limitations.

3.5 Analysis Methodology

The articles were categorized according to the main areas of focus: (1) Security Enhancements, (2) Trust Mechanisms, or (3) Interoperability Solutions. A qualitative comparison was then conducted concerning implementation maturity, technological tools, performance indicators, and readiness for the real world. The process of selecting an article was recorded according to the PRISMA guideline.

3.6 PRISMA flow diagram

The technique used in selecting the articles followed the PRISMA process guidelines. A total of 85 articles were identified, with 55 remaining after duplicates were removed. These 55 articles were reviewed based on titles and abstracts, and 25 irrelevant studies were excluded. After assessing their eligibility, we eliminated twelve of the remaining thirty articles because they failed to meet the inclusion requirements. The final synthesis consisted of 18 studies. The PRISMA flow diagram Figure 7 provides the selection process.

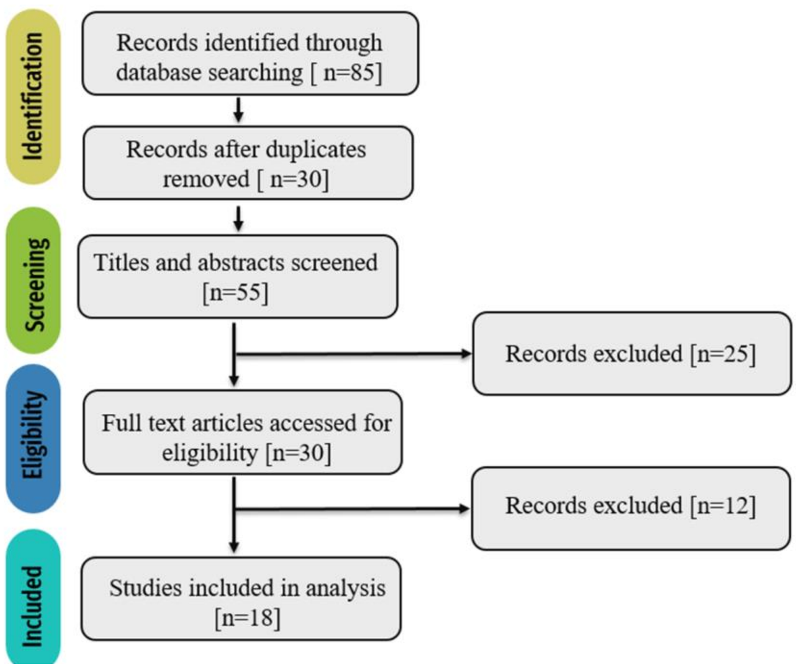

Figure 7. PRISMA Process Diagram

4. Result

4.1 Overview of Selected Studies

This systematic literature review included 18 peer-reviewed articles published between 2020 and 2025. These studies were collected from databases such as IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and arXiv. All selected articles examined the features of blockchain to enhance security, trust, and interoperability in the metaverse context. The selected articles also utilized various methods, including conceptual models, simulation studies, prototypes, and system designs.

4.2 Thematic Categorization of Studies

4.2.1 Blockchain for Metaverse Security

Security enhancements through blockchain imply that secure and decentralized strategies can be used to store users' data, digital assets, identities, and so forth in the metaverse. There is a significant amount of research on how blockchain contributes to the security of the metaverse, particularly in areas such as authentication, identity protection, and secure communication. The following studies detect how blockchain enhances security in virtual environments.

- **Rajawat et al. [31]** explored a consensus algorithm based on blockchain to secure and scale the metaverse by employing PoW, PoS, and PBFT with both simulation and quantitative analysis. The research demonstrates that

PBFT achieves the fastest confirmation (1s) and optimum efficiency, whereas PoS optimizes performance with no security incidents and PoW has resource-intensive/high-energy costs and endured attacks. But it also presents scalability restrictions in PBFT, PoS's risk of centralization, and PoW's inefficiency in power use.

- **Ud Din et al [32]** proposed a blockchain-enabled zero-trust security architecture to augment security and resilience of systems deployed in virtual spaces, such as the metaverse using decentralized authentication, continuous verification, and blockchain-based mechanism, in trust. The analysis demonstrated an improvement in overall effectiveness compared to an establishment's traditional security system, e.g. improved threat discoverability, timely breach response, and improved transaction handling activities under conditions of stress.

- **Yadav et al. [33]** suggested a blockchain-based zero-knowledge proof (ZKP) based authentication protocol to enable secure communications between users and platform servers in the metaverse where public channels leave sensitive information exposed to a range of attacks. Protocols utilize existing ZKP technology and blockchain structure and also formal security checking protocols like BAN logic, scyther and AVISPA, against identify deception and impersonation attacks, privacy attacks, secret leakage attacks and traceability attacks. In this paper, the authors showed the protocol has significantly stronger security protection compared with other protocols and while still showing acceptable performance regarding computational cost, communication, storage size and energy. The authors showed however, that their protocol had slightly more computational cost, and could not handle a situation with a malicious platform server or support avatar-to-avatar authentication, both of which the authors noted are opportunities for future work.

- **Ryu et al. [34]** proposed a mutual authentication scheme to establish secure communication while user identification can be done transparently in metaverse environments utilizing blockchain technology, biometric information, and elliptic curve cryptography. The results indicate improved security and efficiency including protection against public channel vulnerabilities and better computation and communication costs survive existing schemes.

- **Hassan et al. [35**] offered PRIDA-ME, a blockchain authentication scheme for metaverse environments with provisions for privacy, decentralization, and interoperability. PRIDA-ME leverages ECC, biohashing, and PUFs to facilitate secure user–platform authentication, local password updates, and device change. BAN Logic, ProVerif, and Scyther verification prove it resistant against more than 25 attacks with lower computational and communication overhead than current methods. As useful, opportunities for future research such as with threshold cryptography, as well as data share with secrecy preserving, are proposed.

- **Patwe & Mane [36]** offered a blockchain-enabled authentication scheme to provide secure and interoperable identity authentication across metaverse ecosystems, utilizing decentralized identifiers (Meta-IDs) and a blockchain-based Metaverse Interoperable Identity Framework (MIF). The study shows increased security, efficiency, and decreased communication and computational costs, including protection against impersonation, replay attacks, and server-spoofing attacks, while being able to seamlessly navigate across platforms. The work also discloses limitations, noting that more real-world deployment and evaluation of the MIF mechanism is needed to support different metaverse use cases.

- **Seo & Park [37]** proposed a blockchain-based access control mechanism (SBAC) to protect personal data in the metaverse by removing the requirement for some type of administrative control, combined with using substitution cipher encryption and rule tables collectively generated with smart contracts. The results show several advantages, including greater resistance to brute-force attacks and improved performance as measured by encryption and decryption time, as compared to existing cryptographic algorithms. Nonetheless, the proposed approach has cons to it - primarily the time required to split the data, and the challenge of managing several smart contracts for storage.

4.2.2 Blockchain as a Trust Mechanism

Establishing trust with blockchain involves creating transparent, verifiable, and autonomous systems that reduce the need for centralized authorities in the metaverse. The following is summarized in several articles related to this field, highlighting how various blockchain-based approaches have been proposed to reinforce trust among users and systems in decentralized virtual environments.

- **Xu et al. [38]** suggested a new trustless metaverse architecture that is blockchain-enabled to efficiently integrate and allocate resources in the convergence between virtual and real worlds. The architecture utilizes On-demand Trusted Computing Environments (OTCE), hypergraph-based local trust evaluation, Distributed Identity (DID) attestation, and Blockchain Virtual Machines (BVM) to generate transparent and trustworthy computing environments and flexible and secure application sandboxing with consistently applied context-specific security plans based on trust levels. The authors note important limitations, including the current use of blockchain and the need for future instantiation through a prototype of a metaverse.

- **Ghirmai et al. [39**] proposed a system to enhance trust and interoperability in the metaverse using Self-Sovereign Identity (SSI) integrated with blockchain, verifiable credentials, non-transferable NFTs, and cryptographic techniques. The study shows that SSI can provide decentralized authentication and secure communication, such as identity verification without data disclosure and encrypted messaging using public key attestations. However, it also highlights limitations, including the lack of support for behavior-rich avatar interoperability, challenges in offline and multi-user encryption, and the scalability of blockchain-based identity storage.

- **Mebrahtom et al. [40**] proposed the establishment of a decentralized authentication mechanism within the metaverse to enhance identity management and trust. This would employ self-sovereign identity, smart contracts, and a Unity-based virtual world. The technology enables users to log in securely and regulates access to information while preserving their privacy. Nonetheless, it presents several issues, including gas fees, challenges in mobile deployment, and scalability concerns.

- **Awan et al. [41]** presented a trust-based resource allocation framework to improve performance and security in the metaverse by reducing latency through a decentralized trust and reputation system. The authors propose a platform with Trust-Centric Resource Allocation (TCRA), a latency model based on reputation, and a Proof-of-Trust (PoT) consensus contract, and validate its outcomes using OMNeT++ simulations. They show notable outcomes including 45% latency reduction, resource availability of 96%, and 96% detection rates for some cyberattacks, including DDoS and on–off attacks. They still capture limitations of the work, such as no real-world deployments.

- **Mebrahtom et al. [42]** introduced a decentralized architecture for secure, interoperable interactions among Metaverse platforms based on Self-Sovereign Identity (SSI), blockchain, digital wallet, and secure backend infrastructure. The research shows improved scalability, efficiency, and user control, e.g., secure cross-platform interactions. Though the authors mention real-world implementation difficulties, they also indicate the necessity for methodological adjustments and technological integration.

4.2.3 Blockchain to Enable Interoperability

Interoperability in the metaverse refers to the ability of users, assets, and data to move freely between virtual platforms. Blockchain makes this possible by supporting secure and transparent exchanges—even across different or isolated blockchain networks. In the following section, we review several studies that examine how blockchain solutions contribute to cross-platform compatibility and explore practical methods for connecting distinct digital environments.

- **Li et al. [43]** proposed MetaOpera, a protocol allowing asset and identity transfers across decentralized and centralized metaverse through NFTs, smart contracts, oracles, and a committee-based notary system. It has 8× reduced proofs and 3× reduced transaction times compared to sidechains but has limitations such as object customization and the unavailability of universal standards and offline trust.

- **Ren et al. [44]** implemented a cross-chain interaction framework (HCNCT) that enables secure, decentralized digital asset exchanges between blockchains in metaverse contexts. This framework utilizes an advanced Hash TimeLock Contract (HTLC), a notary group, verifiable secret sharing, and a user credibility evaluation system. The research enhances security and accuracy, offering resilience against malicious delay transaction attacks, reducing centralization risks, expediting transactions, and improving success rates in the presence of malevolent users. Nonetheless, the research indicates that the oversight and participation of the notary group lead to supplementary transaction fees.

- **Li et al. [45]** introduced a cross-metaverse interoperability protocol (CrossMeta) for secure, fast, and low-cost transfers of assets between diverse metaverses, based on smart contracts, a dynamic committee scheme, and blockchain verification. The research illustrates great efficiency and scalability with 76–78% lower transaction latency and gas fees of 7.7× to 9.4× lower than those of current approaches like STYLE and MetaOpera. The research also identifies areas of remaining limitations like the protection of privacy in subsequent research.

- **Jiang et al. [46]** presented a cross-blockchain asset exchange protocol to attain quick and atomic metaverse interoperability by relying on smart contracts and multi-party Diffie-Hellman key exchanges. Constant-time asset exchange efficiency, like time complexity minimization from O(n) to O(1), is illustrated by the study, even in the case of multiple parties. However, the study also points out weaknesses, like limited real-world deployment and asset-level interoperability consideration only.

- **Oh et al. [47]** suggested a secure content trading system to facilitate cross platform interoperability in the metaverse environment using blockchain technology, smart contracts, and searchable encryption. The study shows that security and efficiency can be improved, including protection against impersonation attacks, Man-in-the-Middle (MITM) and denial of service (DoS), enhanced speed performance, and reduced computational costs compared to existing schemes.

- **Zaman et al. [48]** presented a new protocol for on-chain atomic swaps to safely and securely exchange assets in different metaverses, like cryptocurrency and NFTs, between any two users. The synchronous smart contracts—written in Solidity and tested on the simulated networks of Ethereum—now allow for a state-synchronized method of performing atomic swaps. Meanwhile, outcomes from this recent study show a rather promising picture for the protocol's first real-world use case: Users can expect to complete their atomic swaps in roughly 6 minutes at a cost of about 0.013 ETH.

4.3 Summary Table of Included Studies

Table 2: provides an overview of selected studies on blockchain applications in the metaverse. It compares them based on important factors, including methodology, algorithms, blockchain networks, and technology employed. It also shows what each study is about, such as security, trust, or interoperability, and discusses its limitations. This comparison shows how different blockchain-based methods help solve essential problems in a decentralized virtual environment.

Table 2: A Comparative Analysis of Selected Research on Blockchain-Powered Metaverse Solutions

References	Publication year	System Design and Evaluation Type	Application Domain	Algorithm Used	Blockchain network	Tools/Technologies Used	Focus Area(s)			Limitations
							Security Enhancements	Trust Mechanisms	Interoperability	
[31]	2023	Simulation & Comparative Analysis	Metaverse infrastructure	PoW, PoS, PBFT	General	Consensus mechanism	✓	✗	✗	Limit scalability
[32]	2024	Theoretical framework + Simulation	Metaverse Security	Zero Trust model	general	Graph theory, cryptographic hash functions	✓	✓	✗	Lacks real-time metrics and broader deployment analysis
[33]	2023	theoretical + simulation	Metaverse Authentication	ZKP	Public	BAN, Scyther, AVISPA	✓	✗	✗	functional and performance
[34]	2022	theoretical + simulation	Metaverse security	ECC + bio hashing	Public	AVISPA, BAN, ROR	✓	✗	✗	no real-world deployment
[35]	2025	System proposal + simulation	Metaverse authentication	ECC, biohashing, PUF	Public and private	BAN, ProVerif, Scyther	✓	✓	✓	No DoS prevention, limited local verification
[36]	2024	System proposal +	Metaverse identity	ECC, Hashing, PKI	Hyperledger Fabric	AVISPA, BAN, ROR	✓	✗	✓	Needs real-world

		simulation	management							deployment and testing
[37]	2024	Encryption & Access Control Design	Metaverse access control	Substitution cipher	General	Smart contract	✓	✓	✗	Smart contract complexity
[38]	2022	Architectural Proposal	Blockchain-enabled Metaverse	Local Trust Model(Hypergraph)	General	OTCE, BVM, Graph Analytics	✓	✓	✗	No prototype, high resource use
[39]	2023	Conceptual Framework + Initial Design	Identity management	SSI + Verifiable Credentials	General	SSI, NFTs, Cryptography, Public Key	✓	✓	✓	Scalability/Performance
[40]	2023	Prototype Implementation	Authentication in Metaverse	SSI + ECC	Ethereum	Smart contract , Flutter, Unity	✓	✓	✗	high transaction costs, scalability
[41]	2023	Simulation + Conceptual	Metaverse performance	TCRA, PoT	general	OMNeT++ simulator	✓	✓	✗	Simulation only, no deployment
[42]	2024	Prototype + Use Case	Decentralized Metaverse	ECC + AES	Ethereum	Flutter, Unity, Nethereum Web3, Solidity	✓	✓	✗	Scalability
[43]	2023	Protocol Design & Simulation	Cross-metaverse asset & identity transfer	Committee-based notary system	Cardano + Ethereum	NFT,Notary, Oracles, PoC	✗	✗	✓	establishing global standards
[44]	2024	Prototype and simulation	Cross-chain transaction for digital assets	HTLC, ECC	Ethereum	Notary Group, Solidity-based Smart Contracts,	✗	✗	✓	High cost due to notary monitoring
[45]	2025	Prototype Implementation	Cross-metaverse asset exchange	Committee Selection, Game Theory	Ronin , Ethereum	Smart Contracts, Solidity	✗	✗	✓	Limited privacy preservation
[46]	2023	Protocol Design & Evaluation	Cross-chain asset exchange	Multi-party Diffie-Hellman + Smart Contracts	General	Smart contract	✗	✗	✓	Limited deployment, asset-level only
[47]	2023	Security Protocol Design	Cross-platform content trading	Searchable Encryption	General	Smart Contracts, BAN, Scyther	✗	✗	✓	No real-world deployment
[48]	2023	Protocol Design & Simulation	On-chain atomic asset swaps	Atomic Swap Protocol (Solidity)	Ethereum	Solidity, Ganache	✗	✗	✓	Early stage, lacks scalability validation

5. Discussion

5.1 Answers to Research Questions

- **RQ1: How can blockchain technology enhance security within metaverse environments?**

Blockchain technology enhances security in the metaverse by providing individuals with decentralized and cryptographically robust methods of proving their identity, securing their data, and communicating with one another. The analyzed research articles emphasize the employment of the consensus algorithms (including PBFT and PoS) and building zero-trust systems as well as the application of advanced cryptographic techniques, including zero-knowledge proofs (ZKPs), the elliptic curve cryptography (ECC), and hashing. All these techniques combine to reduce the threats of spoofing, controlled altering of information, and manipulation by unapproved users. It is possible to add support to privacy-protective and cross-platform applied security procedures to blockchain: examples are security models such as PRIDA-ME and interoperable self-administering identifications such as MIF.

These systems also become more resilient and trustworthy; at the same time, current research concerns computational complexity, scalability, and the necessity of empirical verification in real-life applications.

- **RQ2: How can blockchain foster trust among users in the metaverse?**

Blockchain technology builds trust among users in the metaverse by enabling decentralized, transparent, and secure systems for identity, interactions, and resource management. Using Self-Sovereign Identity (SSI), users can control their digital identities and authenticate securely without relying on centralized platforms. Blockchain also supports trust evaluation mechanisms that verify user behavior and enforce context-based security policies. Additionally, reputation-based resource allocation ensures fair access and improves platform performance. Lastly, blockchain facilitates secure, cross-platform interactions, allowing trusted engagement across virtual environments. Despite these strengths, challenges remain—scalability, real-world implementation, and integration complexity. Still, blockchain provides a strong foundation for building a more trustworthy and user-centric metaverse.

- **RQ3: How can blockchain enable metaverse system interoperability?**

The primary function of blockchain is to facilitate interoperability among various metaverse platforms by providing a secure, efficient, and decentralized exchange of digital assets, identities, and content. Various proposed systems, including MetaOpera, HCNCT, CrossMeta, and the mechanism of atomic swap, demonstrate that blockchain-based systems can considerably speed up transaction time in cross-platform transfer, decrease gas transfer costs, and ensure data validity. Those will be based on the use of such instruments as the smart contract, notary systems, verifiable secret sharing, and cryptographic approaches, guarantee flawless communication between otherwise disconnected virtual worlds. Moreover, solutions such as safe content trading and on-chain atomic swaps demonstrate how real-time user-to-user interoperability is possible without centralized third parties. Nevertheless, scalability, transaction cost, the lack of universal standards, and real-life implementation remain common. Despite these challenges, existing studies show clearly that blockchain offers an effective technical basis for creating a more interconnected and interoperable metaverse ecosystem.

5.2 Comparative Synthesis of Blockchain Techniques in the Metaverse

Our analysis of the 18 papers shows that blockchain technology has many applications that enhance the metaverse ecosystem. Commonly used technologies include zero-knowledge proofs (ZKPs), self-sovereign identity (SSI), cross-chain protocols and smart contracts. However, significant trade-offs and inconsistencies also arise.

- Various studies examine privacy, performance, and interoperability in blockchain-based Metaverse systems from diverse perspectives. Some studies, like [33] and [34], focus on strong privacy and user verification using advanced methods like zero-knowledge proofs (ZKPs) and elliptic curve cryptography (ECC). Additional research, such as [36] and [37], concentrates on more straightforward access control techniques to enhance efficiency and streamline the system. Zero-Knowledge Proofs (ZKPs) offer significant privacy, although they require greater computational resources for implementation. Conversely, simpler approaches may exhibit reduced security yet enhanced efficiency.
- Self-Sovereign Identity (SSI) frameworks such as [39] and [40] help to build decentralized trust, but they have problems with scalability and on-chain storage. Hybrid models, such as Proof-of-Trust (PoT) [41], attempt to find a balance between security and performance by judging things based on their reputation.
- Interoperability strategies are also very different from each other. Protocols based on notaries, such as MetaOpera [43] and CrossMeta [45], make it easier for different chains to work together; however, they also make it harder to coordinate and cost more to run. Atomic swap protocols [48], on the other hand, allow assets to be transferred without middlemen, but they are not used as much because assets do not always work together, and there are no standard ways to implement them.

In the table 3 below, we compare the main blockchain technologies that have been mentioned throughout the paper in detail. We also show important trade-offs that need to be thought about when designing secure and scalable metaverse systems, such as those between privacy and performance or interoperability and price.

Table 3 The comparative analysis of core technologies is summarized.

Technology	Strengths	Limitations	Trade-Offs
ZKP	Strong privacy, no data leakage	High computational cost, limited avatar support	Privacy vs. Performance
SSI/DID	User control, decentralized,	Scalability, gas costs,	Control vs. Usability

	verifiable identity	integration complexity	
Smart Contracts	Automated execution, decentralized logic	Immutable errors, potential code vulnerabilities	Trust vs. Flexibility
Cross-Chain	Seamless interoperability between platforms	Standardization gaps, notary fees, latency issues	Interoperability vs. Cost
PoS & PBFT	Efficient consensus, improved decentralization	Centralization risk (PoS), scalability limits (PBFT)	Efficiency vs. Trust

5.3 Limitations of the Review

This systematic review gives valuable information about how blockchain can be used to improve the Metaverse, but it also has some problems that should be noted:

- Scarcity of Peer-Reviewed Literature

Since blockchain-based metaverse systems are still very new, there are not many academic studies that focus directly on this specific combination. Most available papers discuss blockchain or metaverse technologies separately, or only in theory. Many of them present conceptual ideas or early-stage experiments rather than tested, real-world systems. As a result, it is difficult to compare mature solutions or draw strong conclusions. This lack of focused, high-quality research reduces the amount of evidence available for this review.

- High development costs and limited access

Building a fully functional metaverse environment is difficult, takes many resources, and costs a lot of money. To build these kinds of platforms, you usually need a lot of money, infrastructure, and technical know-how—things that only well-funded companies or institutions typically have. Because of this, academic researchers may have trouble getting to or testing blockchain solutions in real Metaverse settings, which makes it harder to get real-world data and proof.

6. Conclusion and Future Work

This review illustrates that blockchain technology is an essential instrument for tackling the principal challenges of the metaverse, especially regarding security, trust, and interoperability. Decentralized identity, smart contracts, and consensus algorithms enhance user data protection, facilitate verifiable interactions, and promote decentralized asset exchange. Even with these improvements, significant problems remain, including the inability to be easily scaled, the high computational requirements, and the lack of universal standards for interoperability.
In the future, research should focus on utilizing blockchain-based Metaverse solutions in the real world, developing lightweight and scalable security protocols, and collaborating to establish cross-platform standards. These steps are necessary to create a metaverse ecosystem that is safe, interoperable with other systems, and prioritizes user needs.

Reference

[1] H. Meng, J. Ding, H. Wang, Z. Zhang, X. Yao, and H. Ning, “Blockchain Enabled Metaverse: Development and Applications,” Tsinghua Sci. Technol., vol. 30, no. 4, pp. 1552–1582, Aug. 2025, doi: 10.26599/TST.2024.9010054.

[2] H. Wang et al., “A Survey on the Metaverse: The State-of-the-Art, Technologies, Applications, and Challenges,” IEEE Internet Things J., vol. 10, no. 16, pp. 14671–14688, Aug. 2023, doi: 10.1109/JIOT.2023.3278329.

[3] B. Jin, H. Kuang, and X. Li, “Blockchain Application in Metaverse: A Review,” Apr. 16, 2025, arXiv: arXiv:2504.11730. doi: 10.48550/arXiv.2504.11730.

[4] T. Huynh-The et al., “Blockchain for the metaverse: A Review,” Future Generation Computer Systems, vol. 143, pp. 401–419, Jun. 2023, doi: 10.1016/j.future.2023.02.008.

[5] S.-M. Park and Y.-G. Kim, “A Metaverse: Taxonomy, Components, Applications, and Open Challenges,” IEEE Access, vol. 10, pp. 4209–4251, 2022, doi: 10.1109/ACCESS.2021.3140175.

[6] M. Elsadig, M. A. Alohali, A. O. Ibrahim, and A. W. Abulfaraj, “Roles of Blockchain in the Metaverse: Concepts, Taxonomy, Recent Advances, Enabling Technologies, and Open Research Issues,” IEEE Access, vol. 12, pp. 38410–38435, 2024, doi: 10.1109/ACCESS.2024.3367014.

[7] V. T. Truong, L. Le, and D. Niyato, “Blockchain Meets Metaverse and Digital Asset Management: A Comprehensive Survey,” IEEE Access, vol. 11, pp. 26258–26288, 2023, doi: 10.1109/ACCESS.2023.3257029.

[8] M. Hatami, Q. Qu, Y. Chen, H. Kholidy, E. Blasch, and E. Ardiles-Cruz, “A Survey of the Real-Time Metaverse: Challenges and Opportunities,” Future Internet, vol. 16, no. 10, p. 379, Oct. 2024, doi: 10.3390/fi16100379.

[9] A. Qayyum et al., “Secure and Trustworthy Artificial Intelligence-Extended Reality (AI-XR) for Metaverses,” 2022, doi: 10.48550/ARXIV.2210.13289.

[10] A. D. Samala et al., “Metaverse Technologies in Education: A Systematic Literature Review Using PRISMA,” Int. J. Emerg. Technol. Learn., vol. 18, no. 05, pp. 231–252, Mar. 2023, doi: 10.3991/ijet.v18i05.35501.

[11] “Applying Digital Twins in Metaverse- User Interface, Security and Privacy Challenges[#1072189]-2248394.”

[12] S. Mihai et al., “Digital Twins: A Survey on Enabling Technologies, Challenges, Trends and Future Prospects,” IEEE Commun. Surv. Tutorials, vol. 24, no. 4, pp. 2255–2291, 2022, doi: 10.1109/COMST.2022.3208773.

[13] H. Jeon, H. Youn, S. Ko, and T. Kim, “Blockchain and AI Meet in the Metaverse,” in Blockchain Potential in AI, T. M. Fernández-Caramés and P. Fraga-Lamas, Eds., IntechOpen, 2022. doi: 10.5772/intechopen.99114.

[14] K. Li et al., “When Internet of Things Meets Metaverse: Convergence of Physical and Cyber Worlds,” IEEE Internet Things J., vol. 10, no. 5, pp. 4148–4173, Mar. 2023, doi: 10.1109/JIOT.2022.3232845.

[15] A. Patra, A. Pandey, V. Hassija, V. Chamola, and R. P. Mishra, “A Survey on Edge Enabled Metaverse: Applications, Technological Innovations, and Prospective Trajectories Within the Industry,” IEEE Access, vol. 12, pp. 125125–125144, 2024, doi: 10.1109/ACCESS.2024.3452184.

[16] Y. Fu, C. Li, F. R. Yu, T. H. Luan, P. Zhao, and S. Liu, “A Survey of Blockchain and Intelligent Networking for the Metaverse,” IEEE Internet Things J., vol. 10, no. 4, pp. 3587–3610, Feb. 2023, doi: 10.1109/JIOT.2022.3222521.

[17] S. Banaeian Far, A. Imani Rad, and M. Rajabzadeh Asaar, “Blockchain and its derived technologies shape the future generation of digital businesses: a focus on decentralized finance and the Metaverse,” Data Science and Management, vol. 6, no. 3, pp. 183–197, Sep. 2023, doi: 10.1016/j.dsm.2023.06.002.

[18] T. Hennig-Thurau, D. N. Aliman, A. M. Herting, G. P. Cziehso, M. Linder, and R. V. Kübler, “Social interactions in the metaverse: Framework, initial evidence, and research roadmap,” J. of the Acad. Mark. Sci., vol. 51, no. 4, pp. 889–913, Jul. 2023, doi: 10.1007/s11747-022-00908-0.

[19] Y. Wu, A. Yi, C. Ma, and L. Chen, “Artificial intelligence for video game visualization, advancements, benefits and challenges,” MBE, vol. 20, no. 8, pp. 15345–15373, 2023, doi: 10.3934/mbe.2023686.

[20] H. Raad and F. K. M. Rashid, “The Metaverse: Applications, Concerns, Technical Challenges, Future Directions and Recommendations,” IEEE Access, vol. 11, pp. 110850–110861, 2023, doi: 10.1109/ACCESS.2023.3321650.

[21] G. Bansal, K. Rajgopal, V. Chamola, Z. Xiong, and D. Niyato, “Healthcare in Metaverse: A Survey on Current Metaverse Applications in Healthcare,” IEEE Access, vol. 10, pp. 119914–119946, 2022, doi: 10.1109/ACCESS.2022.3219845.

[22] D. Buhalis, D. Leung, and M. Lin, “Metaverse as a disruptive technology revolutionising tourism management and marketing,” Tourism Management, vol. 97, p. 104724, Aug. 2023, doi: 10.1016/j.tourman.2023.104724.

[23] M. H. Jumaa and A. C. Shakir, “Review Study of E-Voting System Based on Smart Contracts Using Blockchain Technology,” Iraqi Journal of Science, pp. 2001–2022, Apr. 2023, doi: 10.24996/ijs.2023.64.4.36.

[24] A. I. Sanka, M. Irfan, I. Huang, and R. C. C. Cheung, “A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research,” Computer Communications, vol. 169, pp. 179–201, Mar. 2021, doi: 10.1016/j.comcom.2020.12.028.

[25] M. Uddin et al., “Exploring the convergence of Metaverse, Blockchain, and AI : A comprehensive survey of enabling technologies, applications, challenges, and future directions,” WIREs Data Min & Knowl, vol. 14, no. 6, p. e1556, Nov. 2024, doi: 10.1002/widm.1556.

[26] M. M. Ahmed and A. C. Shakir, “Review Study: Blockchain Application in Payroll System,” Al-Kitab J. Pure Sci., vol. 7, no. 1, pp. 83–99, Aug. 2023, doi: 10.32441/kjps.07.01.p8.

[27] N. Moosavi, H. Taherdoost, N. Mohamed, M. Madanchian, Y. Farhaoui, and I. U. Khan, “Blockchain Technology, Structure, and Applications: A Survey,” Procedia Computer Science, vol. 237, pp. 645–658, 2024, doi: 10.1016/j.procs.2024.05.150.

[28] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, “A comprehensive survey on blockchain technology,” Sustainable Energy Technologies and Assessments, vol. 52, p. 102039, Aug. 2022, doi: 10.1016/j.seta.2022.102039.

[29] A. P. Singh, “Blockchain Technology: Core Mechanisms, Evolution, and Future Implementation Challenges,” May 13, 2025, arXiv: arXiv:2505.08772. doi: 10.48550/arXiv.2505.08772.

[30] A. Ghosh, Lavanya, V. Hassija, V. Chamola, and A. El Saddik, “A Survey on Decentralized Metaverse Using Blockchain and Web 3.0 Technologies, Applications, and More,” IEEE Access, vol. 12, pp. 146915–146948, 2024, doi: 10.1109/ACCESS.2024.3469193.

[31] A. S. Rajawat et al., “Enhancing Security and Scalability of Metaverse with Blockchain-based Consensus Mechanisms,” in 2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, Romania: IEEE, Jun. 2023, pp. 01–06. doi: 10.1109/ECAI58194.2023.10194035.

[32] I. Ud Din, K. Habib Khan, A. Almogren, M. Zareei, and J. Arturo Pérez Díaz, “Securing the Metaverse: A Blockchain-Enabled Zero-Trust Architecture for Virtual Environments,” IEEE Access, vol. 12, pp. 92337–92347, 2024, doi: 10.1109/ACCESS.2024.3423400.

[33] A. K. Yadav, A. Braeken, M. Ylianttila, and M. Liyanage, “A Blockchain-based Authentication Protocol for Metaverse Environments using a Zero Knowledge Proof,” in 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), Kyoto, Japan: IEEE, Jun. 2023, pp. 242–249. doi: 10.1109/MetaCom57706.2023.00053.

[34] J. Ryu, S. Son, J. Lee, Y. Park, and Y. Park, “Design of Secure Mutual Authentication Scheme for Metaverse Environments Using Blockchain,” IEEE Access, vol. 10, pp. 98944–98958, 2022, doi: 10.1109/ACCESS.2022.3206457.

[35] M. U. Hassan, Y. Abbas Bangash, W. Iqbal, A. Chehri, and J. Iqbal, "PRIDA-ME: A Privacy-Preserving, Interoperable and Decentralized Authentication Scheme for Metaverse Environment," IEEE Open J. Commun. Soc., vol. 6, pp. 493–515, 2025, doi: 10.1109/OJCOMS.2024.3523518.

[36] S. Patwe and S. B. Mane, "Blockchain-Enabled Secure and Interoperable Authentication Scheme for Metaverse Environments," Future Internet, vol. 16, no. 5, p. 166, May 2024, doi: 10.3390/fi16050166.

[37] J. Seo and S. Park, "SBAC: Substitution cipher access control based on blockchain for protecting personal data in metaverse," Future Generation Computer Systems, vol. 151, pp. 85–97, Feb. 2024, doi: 10.1016/j.future.2023.09.022.

[38] M. Xu, Y. Guo, Q. Hu, Z. Xiong, D. Yu, and X. Cheng, "A Trustless Architecture of Blockchain-enabled Metaverse," Dec. 16, 2022, arXiv: arXiv:2210.12655. doi: 10.48550/arXiv.2210.12655.

[39] S. Ghirmai, D. Mebrahtom, M. Aloqaily, M. Guizani, and M. Debbah, "Self-Sovereign Identity for Trust and Interoperability in the Metaverse," Mar. 01, 2023, arXiv: arXiv:2303.00422. doi: 10.48550/arXiv.2303.00422.

[40] D. Mebrahtom, S. Hadish, A. Sbhatu, M. Aloqaily, and M. Guizani, "Trust But Verify - Blockchain-Empowered Decentralized Authentication Schema on the Metaverse: A Self-Sovereign Identity Approach," in 2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA), Tartu, Estonia: IEEE, Sep. 2023, pp. 1–8. doi: 10.1109/iMETA59369.2023.10294349.

[41] K. A. Awan, I. Ud Din, A. Almogren, and B.-S. Kim, "Enhancing Performance and Security in the Metaverse: Latency Reduction Using Trust and Reputation Management," Electronics, vol. 12, no. 15, p. 3362, Aug. 2023, doi: 10.3390/electronics12153362.

[42] D. Gebre, S. Hadish, A. Sbhatu, M. Aloqaily, and M. Guizani, "Establishing Trust and Security in Decentralized Metaverse: A Web 3.0 Approach," ACM Trans. Multimedia Comput. Commun. Appl., vol. 20, no. 12, pp. 1–17, Dec. 2024, doi: 10.1145/3696454.

[43] T. Li, C. Yang, Q. Yang, S. Zhou, H. Huang, and Z. Zheng, "MetaOpera: A Cross-Metaverse Interoperability Protocol," Feb. 03, 2023, arXiv: arXiv:2302.01600. doi: 10.48550/arXiv.2302.01600.

[44] Y. Ren, Z. Lv, N. N. Xiong, and J. Wang, "HCNCT: A Cross-chain Interaction Scheme for the Blockchain-based Metaverse," ACM Trans. Multimedia Comput. Commun. Appl., vol. 20, no. 7, pp. 1–23, Jul. 2024, doi: 10.1145/3594542.

[45] T. Li et al., "CrossMeta: A Fast and Cheap Cross-Metaverse Interoperability Protocol," IEEE Trans. Serv. Comput., pp. 1–14, 2025, doi: 10.1109/TSC.2025.3556613.

[46] S. Jiang, J. Cao, and H. Wu, "Fast and Atomic Cross-blockchain Asset Exchange for Metaverse Interoperability," in 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), Kyoto, Japan: IEEE, Jun. 2023, pp. 177–184. doi: 10.1109/MetaCom57706.2023.00044.

[47] J. Oh, M. Kim, Y. Park, and Y. Park, "A Secure Content Trading for Cross-Platform in the Metaverse With Blockchain and Searchable Encryption," IEEE Access, vol. 11, pp. 120680–120693, 2023, doi: 10.1109/ACCESS.2023.3328232.

[48] S. Zaman, R. Dantu, S. Badruddoja, S. Talapuru, and K. Upadhyay, "Seamless Asset Exchange in Interconnected Metaverses: Unraveling On-Chain Atomic Swap," in 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Atlanta, GA, USA: IEEE, Nov. 2023, pp. 146–155. doi: 10.1109/TPS-ISA58951.2023.00026.