IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 24 February 2023, accepted 10 March 2023, date of publication 14 March 2023, date of current version 20 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3257029

SURVEY

Blockchain Meets Metaverse and Digital Asset Management: A Comprehensive Survey

VU TUAN TRUONG[1], LONG BAO LE[1], (Senior Member, IEEE), AND DUSIT NIYATO[2], (Fellow, IEEE)

[1]Institut National De La Recherche Scientifique (INRS), University of Québec, Montréal, QC H5A 1K6, Canada
[2]School of Computer Science and Engineering (SCSE), Nanyang Technological University, Singapore 639798

Corresponding author: Long Bao Le (long.le@inrs.ca)

The work of Vu Tuan Truong and Long Bao Le was supported in part by the Innovation for Defence Excellence and Security (IDEaS) Program from the Department of National Defence (DND) under Grant MN3-005. The work of Dusit Niyato was supported in part by the National Research Foundation (NRF), Singapore, and Infocomm Media Development Authority under the Future Communications Research Development Programme (FCP) under Grant FCP-NTU-RG-2022-010; and in part by the DSO National Laboratories under the AI Singapore Programme (AISG Award No: AISG2-RP-2020-019), under Energy Research Test-Bed and Industry Partnership Funding Initiative, part of the Energy Grid (EG) 2.0 programme, and under DesCartes and the Campus for Research Excellence and Technological Enterprise (CREATE) programme.

ABSTRACT Envisioned to be the next-generation Internet, the metaverse has been attracting enormous attention from both the academia and industry. The metaverse can be viewed as a 3D immersive virtual world, where people use Augmented/Virtual Reality (AR/VR) devices to access and interact with others through digital avatars. While early versions of the metaverse exist in several Massively Multiplayer Online (MMO) games, the full-flesh metaverse is expected to be more complex and enabled by various advanced technologies. Blockchain is one of the crucial technologies that could revolutionize the metaverse to become a decentralized and democratic virtual society with its own economic and governance system. Realizing the importance of blockchain for the metaverse, our goal in this paper is to provide a comprehensive survey that clarifies the role of blockchain in the metaverse including in-depth analysis of digital asset management. To this end, we discuss how blockchain can enable the metaverse from different perspectives, ranging from user applications to virtual services and the blockchain-enabled economic system. Furthermore, we describe how blockchain can shape the metaverse from the system perspective, including various solutions for the decentralized governance system and data management. The potential of blockchain for security and privacy aspects of the metaverse infrastructure is also figured out, while a full flow of blockchain-based digital asset management for the metaverse is investigated. Finally, we discuss a wide range of open challenges of the blockchain-empowered metaverse.

INDEX TERMS Metaverse, blockchain, artificial intelligence, digital asset management, the Internet of Things, digital twin, VR/AR.

I. INTRODUCTION

A. BACKGROUND

The term metaverse was first introduced by Neil Stephenson in his science fiction novel *Snow Crash* written in 1992 [1], where the metaverse was described as a virtual world running parallel to the physical world. In particular, people immerse themselves in the metaverse using VR devices and interact with each other through their digital representation called avatars. Thanks to the rapid development and invention of various advanced technologies, the concept of metaverse is re-emerging and has been envisioned as the next-generation Internet. Specifically, while Digital Twin (DT) enables seamless mapping between the digital and physical worlds, the Augmented/Virtual Reality (AR/VR) technology allows people to explore the 3D virtual world with immersive and

The associate editor coordinating the review of this manuscript and approving it for publication was Mehdi Sookhak.

vivid experience [2]. The advancement of state-of-the-art communication and networking technologies such as 5G-and-beyond wireless networks is also a key driving force for the metaverse as they provide ultra-high speed, low latency and reliable data communications among metaverse devices and between devices and the network [3]. Artificial Intelligence (AI) offers efficient tools to create virtual environment and digital items automatically as well as to extract valuable knowledge from massive data generated in the metaverse [4]. The metaverse is expected to revolutionize various aspects of life such as education [5], healthcare [6], entertainment [7], e-commerce [8], smart manufacturing and other social services [9].

Many giant technology companies and organizations have been investing heavily to make the metaverse a reality. In 2021 alone, Meta poured at least $10 billion into building the metaverse [10]. Similarly, other tech giants like Microsoft, Google, and Nvidia have also taken solid steps to advance the metaverse with huge investments [11]. Existing metaverse projects and platforms such as Fornite,[1] Roblox,[2] and Sandbox[3] have been attracting great attention from the entire society. However, these platforms are still far from realizing the ultimate concept of the metaverse. They could be considered as light versions of the metaverse which evolved from Multiplayer Online (MMO) games.

In MMO games, users playing the games are typically represented as in-game characters, which are similar to the concept of avatar in the metaverse. The players could also interact with each other and participate in various virtual activities held by game publishers or even by the players themselves. Even as these games integrate VR/AR technology offering their players immersive 3D experience, there are still several differences between them and the full-flesh metaverse. Firstly, the games usually lack the interoperability capability. While the metaverse is envisioned to be a global virtual world in which people are not restricted to any particular platform [2], current game-based metaverses operate separately and could not connect to each other. Secondly, to truly imitate and enable a virtual society, the metaverse must not be controlled by any particular organization [3]. The metaverse should be a decentralized environment with its own democratic governance system in which every participant has a voice instead of depending entirely on a centralized party. Thirdly, it must maintain a complete economic system, where the value of digital assets is kept stable regardless of platforms, and they could be traded conveniently within the virtual world via a digital version of real-world fiat currencies [4]. If a particular organization has all rights to generate or delete digital contents and virtual currencies, the platform would lack the desirable fairness and sustainability.

[1]https://www.epicgames.com/fortnite/en-US/home
[2]https://www.roblox.com/
[3]https://www.sandbox.game/en/

From the technical viewpoint, blockchain is a digital distributed ledger that stores transactions and data in a decentralized manner. Specifically, transactions submitted by network nodes are bunched into blocks, then blocks are linked together through a hash function to form a chain. This chain is distributed throughout the network in which each node stores a replica of it. Thanks to this architecture, blockchain possesses outstanding properties such as immutability, transparency, decentralization, and security [12].

Cryptocurrency, an important derivation of blockchain technology, is a potential use case in the metaverse's economic system. Furthermore, major key technologies derived from blockchain such as smart contract, Non-Fungible Token (NFT) [13], Decentralized Autonomous Organization (DAO) [14], Decentralized Finance (DeFi) [15], and Decentralized applications (dApps) [16] can be leveraged to build the economic, financial, and governance systems in the metaverse. Moreover, blockchain can be used as a resilient decentralized data storage method, where various cross-chain communication techniques could be employed to achieve metaverse data interoperability [3].

Most blockchain-based applications in the metaverse are related to certain types of digital assets. While cryptocurrency, NFT, virtual real estate, user avatar and user-generated content (UGC) are obviously digital assets, one could argue that any data generated and stored in the metaverse can be considered as digital asset since they are commercially valuable. Thus, while development of blockchain-based metaverse applications is an important research direction, detailed studies of blockchain-based digital asset management are also necessary when it comes to the next-generation metaverse. To this end, a comprehensive survey covering most up-to-date use cases of blockchain for the metaverse could provide researchers and developers necessary knowledge and facilitate further research in this burgeoning field.

B. EXISTING SURVEYS

There were several recent surveys on metaverse and related enabling technologies, and the list has been growing rapidly over recent years. The authors in [17] conducted a survey of blockchain-enabled networking for the metaverse. The paper mostly focuses on intelligent networking for the metaverse, whereas other use cases of blockchain such as data storage, governance and financial applications are not investigated. Two recent papers [4], [18] both presented the use of blockchain combined with AI in the metaverse. They show the importance of these two technologies and show how they can be leveraged to create the virtual world in certain aspects. However, they did not offer comprehensiveness in terms of blockchain-based applications, while the included use cases are mostly limited to introduction. The contribution of blockchain to the metaverse is also illustrated in [3] as one of edge-enabling technologies. The paper mostly concentrates on use cases related to mobile edge computing and communication networks, while deeper analysis on

blockchain-based applications such as the governance system were not carried out. The authors in [2] discussed the metaverese in terms of security and privacy in which blockchain is used in several use cases to ensure these important properties. For example, blockchain can guarantee security of cross-domain authentication and offer privacy-preserving features. The study in [19] investigates a wide range of applications of blockchain in social media platforms. They found out that existing studies mainly focus on blocking fake news and enhancing data privacy. However, the concept of metaverse is not just limited to social media as it is broader and involves more factors to be discussed. Similarly, other metaverse surveys [6], [20], [21] mentioned blockchain technology as one of metaverse technology enablers, but none of them treats the blockchain technology thoroughly since they focus on other technologies and aspects of the metaverse.

C. MOTIVATIONS AND CONTRIBUTIONS

Aiming to fill the existing gaps in the literature, our paper provides comprehensive discussions on the role of blockchain in the metaverse. Since both blockchain and metaverse are under rapid development, we attempt to include the most up-to-date blockchain-based applications that could be deployed in the future metaverse. By discussing the potential of the blockchain-enabled metaverse deeply and comprehensively, our survey offers necessary guidelines for both developers and researchers in exploring and developing these state-of-the-art technologies. Specifically, the contributions of our survey can be summarized as follows:

- Firstly, we provide readers with necessary background of blockchain technology and the metaverse. Then, we discuss the potential impacts and contributions of blockchain to the metaverse.
- Secondly, we investigate a wide range of blockchain-enabled use cases for the metaverse from the user application perspective, including economic system, entertainment, financial services, and social services.
- Thirdly, we describe the impacts of blockchain on the metaverse from the system perspective, including applications for the governance, reputation, identity system, and data management.
- We discuss security and privacy of the metaverse infrastructure with the corresponding countermeasures based on existing works.
- Next, we conduct an in-depth technical analysis on digital assets in the metaverse, and present a 8-stage digital asset management workflow for the virtual world.
- Finally, we discuss open challenges in integrating blockchain into the metaverse from both technical and social angles.

Table 1 presents the contribution of our work in comparison with previous studies of the blockchain-enabled metaverse in terms of depth and comprehensiveness. The remainder of the paper is organized as follows. Sections II and III present the background of the metaverse, blockchain, and the potential integration of blockchain into the metaverse respectively. Then, various blockchain-based user-side applications in the metaverse are discussed in Section IV. In Section V, we present how blockchain technology empowers the metaverse from system perspective. Section VI surveys security and privacy issues of metaverse infrastructure. Section VII focuses on the roles of blockchain for metaverse digital asset management. Open challenges are discussed in Section VIII, while Section IX concludes the paper. For convenience, the list of abbreviations is given in Table 2, whereas the structure of this survey is illustrated in Fig. 1.

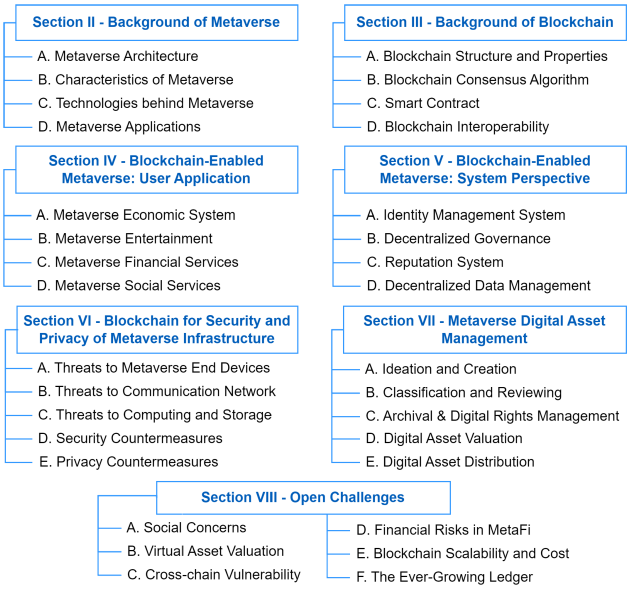

FIGURE 1. The general hierarchical structure of our survey.

II. BACKGROUND OF METAVERSE

The metaverse concept was first coined in the science fiction book Snow Crash in 1992. In 2003, Second Life,[4] which is considered as the first metaverse platform, was introduced and attracted enormous attention from both industry and academia [23]. One of the most important breakthroughs of Second Life compared to previous platforms is that it allows users to create, own, and trade their virtual creations. In the last several years, thanks to the development of AR/VR technology and especially the introduction of blockchain technology, the term metaverse has again emerged and triggered huge attention from the society. While AR/VR enables the immersive and embodied experience in the virtual world, blockchain technology revolutionizes metaverse digital asset management and provides necessary tools to address a wide range of issues in the metaverse [4].

A. METAVERSE ARCHITECTURE

The metaverse is envisioned to be an immersive 3D virtual world that reflects the physical world in various aspects such

[4]https://secondlife.com/

TABLE 1. The contributions of our work compared to other current studies in terms of comprehensiveness.

Content	[17]	[4]	[18]	[6]	[3]	[2]	[21]	[22]	[20]	Ours
The paper provides knowledge of metaverse, including its architecture, properties, components, and applications.	+++	+	+	++	+++	+++	+++	+++	++	+++
The paper presents knowledge of blockchain technology such as its architecture, smart contract, and blockchain interoperability.	+++	+			+	+				+++
The survey illustrates how blockchain enables the metaverse economic system with user-generated content, cryptocurrency, and virtual real estate.		+	+		++	+	+		+	+++
The survey reviews blockchain-based virtual services in the metaverse such as gaming, virtual event, metaverse finance, education, and healthcare.		+		+	++	+		+	+	+++
The survey shows how blockchain empowers the metaverse governance system with identity management, decentralized governance, and reputation systems.						+				+++
The study analyzes the contribution of blockchain to the metaverse infrastructure with data management and blockchain-enabled security and privacy.	++			+	+++	+			+	+++

TABLE 2. List of Abbreviations.

Abbreviation	Definition
ABAC	Attribute-Based Access Control
AI	Artificial Intelligence
AR	Augmented Reality
DAO	Decentralized Autonomous Organization
DApps	Decentralized Applications
DCF	Discounted Cash Flow
DeFi	Decentralized Finance
DFS	Distributed File System
DID	Decentralized Identifier Document
DoS	Denial of Service
DDoS	Distributed Denial of Service
DRM	Digital Right Management
DT	Digital Twin
FL	Federated Learning
IoT	Internet of Things
IPFS	InterPlanetary File System
MetaFi	Metaverse Finance
MITM	Man-in-the-middle
MMO	Massively Multiplayer Online
NFT	Non-Fungible Token
NLP	Natural Language Processing
NPC	Non-Player Character
NVT	Network Value to Transactions
PE	Price to Earnings
PLS	Physical Layer Security
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
SDN	Software Defined Networking
SMRA	Simultaneous Multi-Round Auction
SPOF	Single Point of Failure
SSI	Self-Sovereign Identity
ToS	Terms of Service
UAV	Unmanned Aerial Vehicle
UGC	User-Generated Content
VR	Virtual Reality
XR	Extended Reality
ZKP	Zero-Knowledge Proof
ZKRP	Zero-Knowledge Range Proof

as society, politics, culture, and economy [3]. In this digital world, people can participate in different virtual activities such as working, playing games, shopping, trading assets, and even purchasing virtual lands. To take part in the metaverse, users use wearable AR/VR devices and represent themselves as a real-time digital avatar, reflecting their appearance with a variety of facial expressions and gestures [22].

The general metaverse architecture is presented in Fig. 2, consisting of four main elements which are metaverse infrastructure, metaverse tools, the virtual world and virtual life of participants.

1) METAVERSE INFRASTRUCTURE

The infrastructure of metaverse can be constructed based on a wide range of physical IoT devices and sensors, which help collecting real-world data and reflecting the physical world into the virtual world. The huge amount of collected data is then transmitted seamlessly through advanced communications and networking systems supporting high speed, low latency, and reliable communications [3]. The networking infrastructure can consist of various elements such as satellite, unmanned aerial vehicle (UAV) communications, and especially 5G and beyond wireless networks [2]. To efficiently handle and process the metaverse data, an appropriate combination of computing technologies such as cloud, edge, and end-user computing is crucial. Besides, data storage is an important factor in the metaverse infrastructure, and it could be facilitated by blockchain [4]. This technology provides various options for data storage, including on-chain storage with consortium blockchains, or off-chain storage on distributed database and file systems. Blockchain offers many outstanding characteristics such as immutability, transparency, and interoperability [12].

2) METAVERSE TOOLS

Different metaverse tools are needed for metaverse users to interact with the virtual world. For instance, users participate in and view the metaverse through AR/VR headsets or glasses, while haptic gloves make them feel like they are touching real 3D objects by providing haptic feedback when touching objects in the virtual world [22]. On the other hand, DT technology takes responsibility for mapping and synchronizing between the digital world and physical world, thus offering users immersive and vivid experience [24]. To boost user experience further, AI can be utilized to realize many potential metaverse functions and applications [18]. For example, when users look at an object or place through AR glasses, the AI system could automatically detect and provide information related to it. Besides, blockchain can contribute

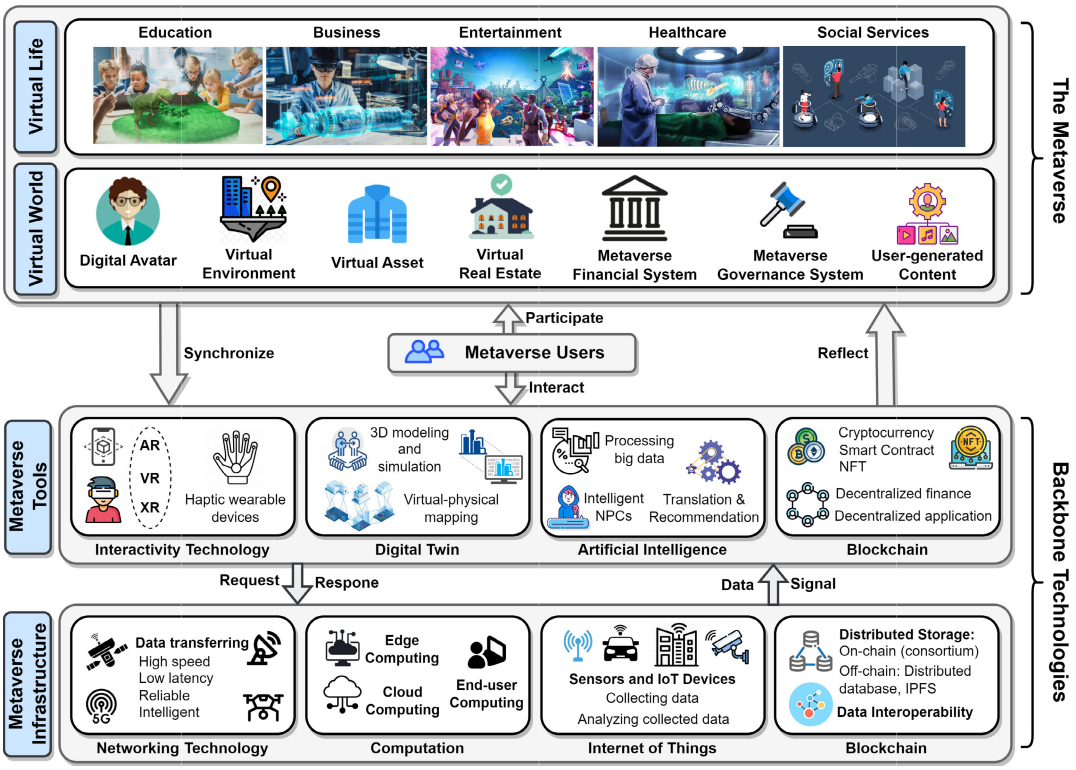

FIGURE 2. General architecture of the metaverse, constructed by various advanced technologies.

to this process with smart contract, cryptocurrency, NFT, and decentralized applications [3].

3) VIRTUAL WORLD AND VIRTUAL LIFE

With all necessary technologies, the digital environment is created with digital assets, real estate, UGCs, and even its own financial and governance systems [25]. Users participate in the platform through their avatars, thereby involving in a variety of activities and services such as education, entertainment, and healthcare [2]. At the highest extent, the metaverse could bring users an entire virtual "second life".

B. CHARACTERISTICS OF METAVERSE

In the following, we describe eight different characteristics of the metaverse:

- **Immersive:** Far beyond the current 2D interaction between users and computers, the metaverse must provide users with vivid and realistic experience so that they could feel psychologically and emotionally immersed in the virtual space [26]. Such immersive experience could be achieved through a blend of visuals, sound, touch, even temperature, and environment effects.
- **Embodied:** Users not merely look at the virtual world and its 3D contents, they are inside of it as a character with a unique and specific role [22]. Specifically, users are represented by their 3D digital avatars and can interact with each other in the metaverse.
- **Global:** The metaverse must be a shared and global environment where everyone can access freely, regardless of their location or nationality.
- **Persistent:** The metaverse must always be available at all times. It continues running in any circumstance, even when users exit the platform.
- **Decentralized:** The metaverse must not be controlled by a particular organization. It should be an open space where users completely own their assets and have a voice in any future direction of the platform.
- **Interoperable:** Each user have a specific identity across platforms and can transfer digital assets across the virtual world. Furthermore, the ultimate version of the metaverse could even interact with the real world [2].
- **Sustainable:** The metaverse must have a complete and stable economic system with its own medium of exchanges and financial activities. All virtual contents in the metaverse must retain their value in comparison with the real world.
- **Synchronized:** The virtual world co-exists and synchronizes with the physical world. Any changes in the physical world can be reflected to the virtual world and vice versa [24].

To achieve the ultimate vision of the metaverse with all of the above characteristics, a wide range of advanced technologies must be employed properly to build the metaverse infrastructure, applications, and services. Most existing metaverse projects still lack certains functions and

characteristics, thus they could be considered as the light versions of the metaverse.

C. TECHNOLOGIES BEHIND METAVERSE

In terms of technology, the metaverse is considered as the next-generation and the 3D model of the Internet. It is a comprehensive fusion of various emerging technologies such as VR/AR, Extended Reality (XR), DT, AI, Blockchain, 5G/6G Wireless Networks, Internet of Things (IoT), cloud and edge computing. These advanced technologies all contribute to the metaverse in different ways, and they complement each other. The general roles of these technologies can be presented as follows:

- **Interactivity Technologies (AR/VR/XR):** These technologies are very crucial in enabling the immersive characteristic of the metaverse. They allow users to experience the metaverse visually through wearable devices such as VR headsets and haptic gloves instead of traditional devices like smart phones and laptops [22].
- **Digital Twin:** DT uses real world data to create digital representations of physical objects [27]. It enables the synchronized property of the metaverse [24], thus allowing the co-existence of physical-virtual reality where real-world objects can appear in the virtual world, and any changes applied to these objects in the digital world will be reflected into the real world [28].
- **Artificial Intelligence:** AI contributes to the metaverse in different ways [4]. Firstly, it could empower other metaverse technologies such as IoT, DT and blockchain, thereby indirectly contributing to the metaverse [4]. Moreover, it can enable the automatic creation process such as creating vivid digital avatars through learning user emotions and facial expressions. AI can also be utilized to develop various virtual smart services such as smart NPCs (non-player character), automatic translation, and recommendation systems in the metaverse.
- **Internet of Things:** IoT with numerous sensors and cameras connecting together provides a massive source of data for the metaverse. It facilitates digital twin in the process of mapping the physical world into the virtual world and vice versa [29], [30].
- **Cloud and Edge Computing:** While wearable devices often have limited processing power and storage capacity, the servers running the metaverse applications and functions could also be overloaded due to the massive number of users participating in the platform. Therefore, proper combination and utilization of advanced cloud and edge computing is crucial in processing the tremendous amount of data in the metaverse while delivering the required quality of service [3].
- **Communication and Networking Technologies:** With massive data generated from an enormous number of users around the world and their virtual activities, a fast and ultra-reliable network infrastructure is crucial [3]. Furthermore, state-of-the-art communication technologies can be leveraged for low latency and high speed communications to prevent motion sickness from using VR devices, thus providing users the highest sense of user experience and improving social acceptance to the metaverse [17].
- **Blockchain:** Blockchain is the key technology which enables the decentralized and sustainable characteristics of the metaverse. It can help creating the economic system of the metaverse with NFT, cryptocurrency and DeFi [25]. In terms of metaverse infrastructure, blockchain offers reliable data management and decentralized systems for various applications.

The development and maturity of aforementioned technologies are the prerequisites for the formation of a complete metaverse in the future. Currently, most metaverse platforms are still incomplete versions of the metaverse [3]. However, these light-version metaverses all seem to point towards the ultimate concept of the metaverse and would gradually converge at some point in the future, when technologies are more mature in both software and hardware.

D. METAVERSE APPLICATIONS

Several prominent applications of the metaverse are described in the following:

- **Education:** The metaverse could provide students immersive learning experience with visual graphics thanks to AR/VR technology. Students can interact efficiently with their teachers through digital avatars. Furthermore, DT enables practically learning with real-time 3D models in the metaverse.
- **Business:** The metaverse could revolutionize sales and marketing sectors with virtual stores built on metaverse real estate. Besides, virtual factories in the metaverse could enhance the productivity for businesses, while digital workplaces offer convenient communication between staff.
- **Entertainment:** The metaverse can be considered as the future of the entertainment industry. It offers immersive play-to-earn games, provides unlimited spaces for virtual concerts, virtual reality theme parks [31] and exhibitions.
- **Healthcare:** The metaverse with virtual reality and DT technologies could revolutionize the surgical practice and medical training for the healthcare sector [6]. Moreover, medical records could be managed by blockchain-based solutions within the metaverse platform to ensure security and integrity.
- **Social Services:** Besides education and healthcare, the metaverse could revolutionize both social and commercial insurance sectors by leveraging the blockchain technology for transparent document storage. It also offers social service management and various types of financial services in a decentralized manner.

There could be more metaverse applications emerging during its development. Within the scope of the paper,

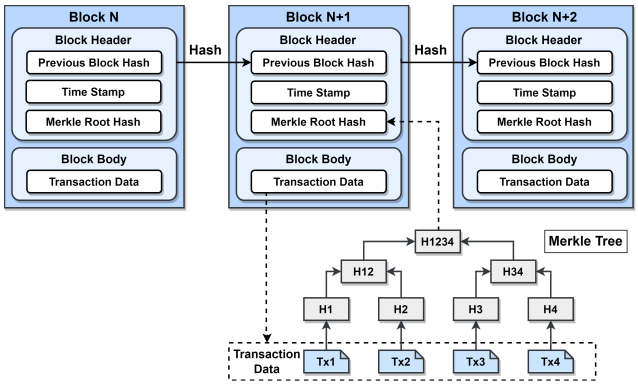

FIGURE 3. The general structure of a blockchain. The Merkle tree allows users to verify payments quickly without having to download the entire transaction history [33]. The block header actually often contains more fields, depending on particular blockchain.

we concentrate more on applications enabled by blockchain technology and its derivative mechanisms.

III. BACKGROUND OF BLOCKCHAIN

A. BLOCKCHAIN STRUCTURE AND PROPERTIES

Blockchain, as its name suggested, is a chain of consecutive blocks linked together. Each block includes two parts, which are block header and block body. In general, the body of a block contains a certain amount of data. If these data are financial transactions (e.g., sending cryptocurrency from one node to another node), the blockchain can be considered as a ledger, while the native currency being traded is called cryptocurrency. That is why blockchain technology sometimes referred to as Distributed Ledger technology. On the other hand, the block header often contains at least three fields. The first one is the Merkle root, which is the root hash of the Merkle tree whose leaves are all transactions in the body of the block [32]. The second field is the hash of the previous block's header, while the third one is the *time stamp*, which estimates the time when a block is created. This general blockchain structure is shown in Fig. 3.

With this structure, if any transaction of a block is modified, the Merkle root of that block will be changed completely due to the collision-free characteristic of the hash function. Therefore, the hash of that block's header is also changed, breaking the link between that block and its next block [32]. This offers the first feature of blockchain technology, tamper-proof, meaning that any tampering on the blockchain can be detected easily by comparing block hashes between every pair of consecutive blocks. Besides, since every block includes a time stamp field indicating its creation time, we could track the creation time of any transactions inside it. This presents the second characteristic, traceability, meaning that we can always keep track of any data in a blockchain over time by accessing the chain's history.

Furthermore, a public blockchain is usually distributed throughout a large peer-to-peer decentralized network with numerous nodes, where each node keeps a replica of the chain. Therefore, it possesses the next characteristic, transparency, meaning that all data on the blockchain is transparent to the public as everyone can download a replica of it at any time. This implies that if a node unilaterally modifies data on her blockchain, the change is only applicable to her local chain and it will not impact on the rest of the network. This upgrades the tamper-proof feature of blockchain to a higher level of security, immutability, meaning that no one can unilaterally make changes to the global blockchain, including adding/removing blocks or modifying data on any block. To add new valid data to the chain, blockchain consensus algorithms are used.

B. BLOCKCHAIN CONSENSUS ALGORITHM

A crucial mechanism is needed to ensure only valid blocks (i.e., blocks containing only valid transactions) can be added onto the blockchain; and this mechanism is called consensus algorithm [34]. In consensus algorithms, a block is considered valid if the majority of participants in the network agree on its validity. Moreover, a transaction is valid if the digital signature of the sender is valid and the amount of tokens sent does not exceed the sender's balance. Currently, there are different consensus algorithms [35] and the popular ones include Proof of Work (PoW) and Proof of Stake (PoS) algorithms [34]. In PoW, nodes in the network compete to solve a complex puzzle and who finds the correct solution first will become the block proposer for the next block (the miner) and earn a reward. Specifically, it requires exhaustively searching for a solution string, nonce, such that cryptographic hash of the concatenation of x, the previous block's header, and the nonce satisfies the following condition:

$$Hash(x, nonce) \leq target,$$

where x is the previous block's header, *target* is a small value determining the hardness of the current block, and *nonce* is the solution that miners search for. Since miners use brute force to find the satisfied nonce, the more computational capacity a node possesses, the higher possibility it wins the race, thus becoming block proposer for the next block.

On the other hand, in PoS, the possibility for a node to become the block proposer is proportional to the amount of financial resource it owns [34]. In a normal case, after a block proposer is chosen, the proposer will validate certain transactions received from other nodes, and then gather the valid ones to form a block [32]. The proposer also attaches a proof into the block, proving that it is the right node to produce the next block (e.g., the proof in PoW is the solution for the mathematical problem). Then, it broadcasts the block to the rest of the network. All other nodes receive the block and validate the transactions. If honest nodes see that all transactions in the block are valid and the attached proof is correct, they must append the block to their own local chain.

If the majority of the network accepts the block, we can say that the network has reached consensus for that block [34].

C. SMART CONTRACT

Blockchains supporting smart contracts usually follows the account-based model, in which each user owns an account with the corresponding account address and the account balance. It operates similar to a state machine which receives transactions as inputs, then changes its state accordingly. The blockchain global state represents all user accounts and some special accounts, which are smart contract accounts [36]. A smart contract account also has an address and its balance. However, it stores a piece of code, similar to a computer program. Anyone can write and deploy smart contracts to the network, but they are not controlled by any user once created. Users can interact with a contract account and trigger its code by submitting transactions that execute a function defined inside the contract. Since smart contract accounts are available on-chain, every participant can verify its source code and make sure of its functionality [36]. Contract functions are executed automatically without any trust assumption and intervention of intermediaries. However, smart contracts are immutable once they are deployed, thus they must be designed and tested carefully before deployment to prevent potential issues [37], [38].

With smart contracts, blockchain technology goes far beyond a mere ledger of financial transactions. One well-known application of smart contract is NFT. NFTs are cryptographic tokens stored on blockchain that prove the ownership of digital assets [13]. NFTs cannot be counterfeited or divided as they are often represented by the ERC-721 standard, in which each of them has a unique identification for recognition. This means that while we can buy, for example, 10 bitcoins or 10 Ethers, there is no sense of ''10 NFTs in general'' because all NFTs are totally different from each other. Smart contract is also the foundation of DeFi and dApps. DApps are applications whose back-end is built by smart contracts, making them fair, transparent, and cannot be dominated by attackers [16]. DeFi [15] is an emerging financial technology which provides users a variety of financial services such as borrowing, lending and investment without third-party authorities like central bank or financial corporations.

D. BLOCKCHAIN INTEROPERABILITY

Blockchain interoperability refers to the ability of different blockchains to communicate with each other to exchange cryptocurrencies, tokens, and any type of digital asset [39]. It can help independent blockchains to connect together to form a large network, which could be considered to be the Internet of blockchains [40]. In general, blockchain interoperability often includes cross-chain bridge and multi-chain platform, which are discussed in the following.

- **Cross-chain Bridge:** This presents a mechanism connecting two arbitrary independent blockchains together. Some current popular bridges include Binance Bridge,[5] Umbria Narni Bridge,[6] and Wormhole.[7]
- **Multi-chain Platform:** Instead of connecting independent blockchains, a multi-chain platform is usually an ecosystem with multiple built-in blockchains. Current prominent multi-chain ecosystems include Polkadot [41] and Cosmos [42].

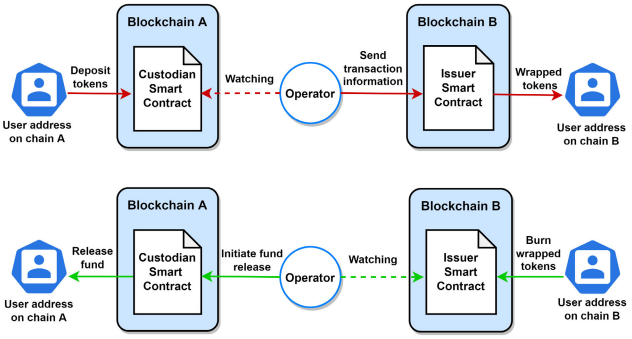

FIGURE 4. The general operation of blockchain cross-chain communication. The process above with red lines is to transfer tokens from one blockchain to another, while the figure below with green lines illustrates how tokens are transferred back to the original chain.

Figure. 4 illustrates a high-level description of cross-chain communication between two blockchains A and B. Specifically, when a node on blockchain A wants to send some tokens to its account on blockchain B, it firstly deposits them to a *custodian smart contract* on the blockchain A, in which the tokens are locked. A third-party service provider called *the operator* takes responsibility for collecting all of these deposit transactions and sending them to an *issuer smart contract* on the blockchain B. This smart contract automatically issues wrapped tokens, which are the representation of the original deposited tokens, to the node's address on the blockchain B. After that, these wrapped tokens could be traded normally on the chain B. Whenever a node wants to transfer its tokens back to the chain A, it sends them to the *issuer smart contract* in which these wrapped tokens are burned, while the deposited tokens are unlocked and send back to the owner on the chain A by the *custodian smart contract*.

IV. BLOCKCHAIN-ENABLED METAVERSE: USER APPLICATIONS

In this section, we present potential contributions of blockchain technology to the metaverse from the user applications perspective, including the metaverse economic system and metaverse virtual services. According to various metaverse features and applications, a summary of some existing metaverse platforms based on these features is provided in Table 3, while Fig. 5 illustrates blockchain-based

[5]https://www.bnbchain.org/en/bridge
[6]https://bridge.umbria.network/
[7]https://www.portalbridge.com/#/transfer

use cases for metaverse user application and potential issues that are discussed in this section.

A. METAVERSE ECONOMIC SYSTEM

The virtual economic system in the decentralized metaverse would be an integration of various types of digital assets such as blockchain native cryptocurrency, fungible token, NFT-based UGCs and virtual real estate. With the decentralized nature of blockchain, the metaverse economic system with its own virtual currency is projected to operate transparently and verifiably without the need for intermediaries [3].

In the metaverse *creator economy*, users can produce content (i.e., UGC) and trade them in the provided marketplace to earn cryptocurrency and tokens. In this use case, NFT can be used to tokenize UGC to ensure its uniqueness and prevent counterfeiting, while the metadata is often stored in off-chain environment to reduce storage cost. Similarly, virtual real estate in the metaverse can be tokenized as NFT to make it scarce and valuable. For instance, creators in Roblox can earn certain Robux (i.e., virtual tokens of the platform) for creating UGCs such as items and game scenes, while Decentraland users can trade virtual real estate ''LANE'', an ERC-721 token in the Ethereum blockchain, through the platform's currency.

However, there are potential security and trust issues of blockchain-based tokens and cryptocurrency [43], [44], especially when it is adopted widely in the metaverse. In terms of cryptocurrency attacks, the authors in [45] formalized cryptocurrencies to find solutions addressing the double spending and secret mining problems. They develop an equilibrium model with a certain confirmation lag that disincentivizes users from double spending. With the proposed model, it is shown that attackers must spend more resource than the monetary benefits obtained from the attack. Besides, selfish mining is another well-known attack, in which the attackers attempt to fork a blockchain by privately maintaining a chain that is longer than the public branch [46]. To prevent this type of attack, the authors in [47] proposed a solution in which there is a ''truth state'' within block data to identify selfish miners. It is computed based on an indication that if the difference between the previous block's average expected height and the current block's height is significant, it is highly likely that the miner withheld the block to conduct selfish mining. In terms of privacy, the authors in [48] discuss anonymity issues of different cryptocurrencies, and possible designs have been pointed out to preserve privacy of cryptocurrency systems. Specifically, ZKP allows users to prove that their transactions are valid under the blockchain consensus rules without revealing any of the computed information [49], whereas mixing protocols make participants anonymous within the platform by permuting ownership of cryptocurrency.

In terms of token-based UGC and virtual real estate, the key challenge is to ensure the integrity of smart contract on which the tokens are deployed, thereby preventing asset counterfeiting. Due to the immutable nature of blockchain, smart contract are unchangeable once they are deployed, thus requiring thorough testing and validation during its development [38]. To this end, the authors in [37] introduced a novel test pattern for reliable smart contract verification. The proposed symmetrical testing method reduces the required number of test cases to just one more than the number of verification rules, leading to a significant decrease in execution time to only a few milliseconds. The authors in [50] analyzed security vulnerabilities of smart contract, including transaction ordering dependence, time stamp dependence, mishandled exceptions, and reentrancy attack. Consequently, they proposed *OYENTE*, a framework detecting security issues of smart contract based on its bytecode. The framework was then evaluated in 19,366 Ethereum smart contracts, showing its practicality and robustness.

B. METAVERSE ENTERTAINMENT

The metaverse has the potential to revolutionize the entertainment industry through a wide range of applications, including gaming and virtual events. An example metaverse game is Roblox, a worldwide platform for user-generated games that enables users to create their own block-based avatars and play a variety of games. When it comes to metaverse virtual event, hundreds of graduating UC Berkeley students attended a virtual commencement ceremony organized in Minecraft, while more than 12 million people participated in the virtual concert of Travis Scott in Fortnite [51].

In terms of metaverse gaming, blockchain and NFT can be utilized to tokenize in-game assets to make them unique and valuable. The authors in [52] proposed a blockchain-based gaming platform that leverages NFT to represent in-game assets, thereby offering effective asset tracking and reward administration. Additionally, blockchain is also utilized for profile management and providing efficient data exchange among players within the game. On the other hand, metaverse gambling games (e.g., the poker game in certain locations of Decentraland) may be designed to give players a disadvantage with a high likelihood of losing their tokens. In this case, blockchain can guarantee the transparency of in-game rules and the fairness of the random generation process. For instance, the authors in [53] proposed a blockchain-based algorithm that generates random number in a decentralized manner. In particular, the final random number is calculated based on the random numbers of both the game provider, players, and an on-chain random number. As multiple participants involve in the generation process, the results are verifiable and cannot be manipulated by any centralized party.

For virtual events in the metaverse, blockchain can be utilized for ticket management, in which tickets are securely linked to their buyers and all associated transactions are transparent on the blockchain, making them resistant to tampering and enabling verification. To this end, Cha et al. proposed a privacy preserving blockchain-based ticketing service [54], using blockchains to store information related to events and tickets, whereas Non-Interactive ZKP are used to

TABLE 3. Summary of existing metaverse platforms and their corresponding features.

Platform	Organization	Main Application	Immersive Experience	Decentralized	Virtual Currency	UGC	MetaFi	DAO	Virtual Real Estate
Decentraland	Decentraland Foundation	NFT-based Game	✓	✓	✓	✓	✓	✓	✓
Roblox	Roblox Corporation	Social Game	✓	✗	✓	✓	✗	✗	✓
Horizon Workroom	Meta	Collaboration	✓	✗	✗	✓	✗	✗	✗
Second Life	Linden Lab	Social Network	✗	✗	✓	✓	✗	✗	✓
Fortnite	Epic Games	MMO Game	✗	✗	✗	✓	✗	✗	✗
Sandbox	Pixowl	NFT-based Game	✓	✓	✓	✓	✓	✓	✓
Cryptovoxels	Nolan Consulting	NFT-based Game	✓	✓	✗	✗	✓	✗	✓
Somnium	Somnium Space	VR Game	✓	✓	✓	✗	✓	✗	✓
Axie Infinity	Sky Mavis	NFT-based Game	✗	✓	✓	✓	✓	✓	✓

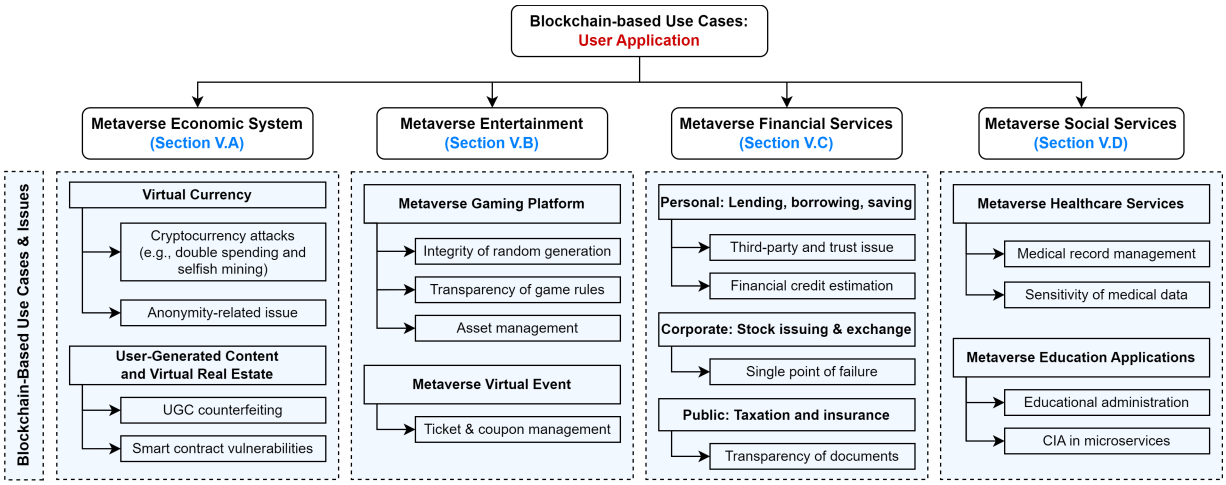

FIGURE 5. Blockchain-based use cases in the metaverse from user application perspective and potential issues.

preserve user privacy. It allows users to prove the ownership to their tickets and ensures the integrity of data, while user privacy is guaranteed as personal information is not required to be provided.

C. METAVERSE FINANCIAL SERVICES

In the physical world, we often participate in a wide range of financial activities such as lending, borrowing, saving, and stock investment. Similarly, the metaverse can also reflect those activities and services, in which blockchain along with the emerging DeFi technologies provide suitable tools to realize them in a decentralized manner. In general, financial activities can be classified into three groups, which are personal, corporate, and public finance.

In terms of personal finance, possible use cases for the metaverse include lending, borrowing, saving and investment in the virtual world. The authors in [55] proposed an architecture using Hyperledger Fabric as a trusted service to enhance the reliability and security of the peer-to-peer lending process. While loan transactions are collected and submitted to the blockchain network by Order nodes, smart contracts regulate the registration process, making it automatic with trust establishment. The authors in [56] proposed a decentralized credit evaluation model based on blockchain and Prospect Theory to minimize the risk of lending. In this system, blockchain takes over the role of third-party organizations in receiving loan funding and determining criteria. Because transactions on the blockchain are verified and permanent, they can be used to assess user's credit using Prospect Theory, which is a reliable method for determining whether to grant a loan to a specific user.

On the other hand, blockchain technology can facilitate corporate finance in stock issuing and exchange. The authors in [57] proposed a decentralized stock exchange platform operating on top of a consortium blockchain. Unlike traditional platforms regulated by a third-party authority, participants in this scheme interact with a smart contract to place orders. The smart contract is preprogrammed with necessary rules and business logic so that a trade is generated securely whenever the prices are matched between the orders. Blockchain network ensures information transparency, availability and security, while experimental results also prove the performance and efficiency of the system [57].

In terms of public finance, it includes social financial services such as insurance and taxation. For these purposes, blockchain technology can be a game changer by offering transparency and verifiability properties for documents. The authors in [58] introduced *BlockCIS*, a smart contract-based cyber insurance framework using Hyperledger Composer. When a customer node suffers a cyber attack, it submits the logs (e.g., firewall or storage logs) to the BlockCIS system as an evidence of the intrusion. Thus, the insurers can compute the premium and fees based on the analyzed logs, which are transparent, verifiable, and permanently stored on the blockchain network.

D. METAVERSE SOCIAL SERVICES

The metaverse is envisioned to be a complete virtual society, thus it has the potential to revolutionize the delivery of social services and make them more accessible and convenient. In the context of healthcare, the metaverse can provide virtual consultations, remote monitoring, and telemedicine services, thereby reducing the need for physical appearance at hospitals [6]. For education, the metaverse can provide a platform for virtual classrooms and enable immersive learning experiences. This can greatly increase access to education, removing geographic limitations and expanding educational opportunities.

In the metaverse, while many of healthcare applications are based on virtual reality technology, blockchain also offers various benefits for medical management [59]. The authors in [60] proposed *MedRec*, a decentralized permission management scheme for medical record based on Ethereum blockchain. In [60], medical records are managed by three different smart contracts. Firstly, the *Registrar Contract* with embedded policies regulates participants' identity and maps their ID to Ethereum address. The *Relationship Contract* allows healthcare providers to access patient data, while patients can refer to all healthcare providers they have been engaged with thanks to the *Summary Contract*. On the other hand, the linkability between user identification and Ethereum address by the Registrar Contract can threaten data privacy. Liu et al. [61] proposed a medical management framework with enhanced privacy protection. In this scheme, medical data are encrypted by patients' public key and stored on a DPoS-based blockchain, thus ensuring privacy and immutability of medical record. Proxy re-encryption enables medical data sharing between patients and doctors by allowing authorized doctors to decrypt the ciphertext to obtain the medical plain text without knowing the patient's private key.

With respect to metaverse education, blockchain can facilitate educational administration [62] and offer CIA (i.e., confidentiality, integrity, and availability) to education microservices [63]. The authors in [62] proposed *EduCTX*,[8] a blockchain-based credit platform for global education with transparency and verifiability. In this scheme, student's credits are represented by the *ECTX* tokens offered in the DPoS-based blockchain network. While multisignature technique is utilized to guarantee security of token transaction, the blockchain enables a global community between different institutions without national and administrative barriers, which totally fits with the global nature of the metaverse. Besides, the authors in [63] leverage blockchain to offer cyber defense with CIA for education microservices. In [63], different educational organizations join a blockchain network in which education data and microservice transactions are immutable on-chain to offer integrity. Confidentiality is obtained thanks to a dual hybrid cryptosystem consisting of RSA and AES, while an access control model provide availability feature.

[8] http://eductx.org/

V. BLOCKCHAIN-ENABLED METAVERSE: SYSTEM PERSPECTIVE

In this section, we discuss the potentials of blockchain for the metaverse from the system perspective, including identity and authentication management, decentralized governance, reputation system, and decentralized data management. They are summarized in Fig. 7.

A. IDENTITY AND AUTHENTICATION MANAGEMENT

Depending on specific purposes, one may have various identities such as identification, passport, and driver license. In specific circumstances, we must present our identity credentials to access certain services or activities. Similarly, identity also plays a vital role in the virtual world. Firstly, authentication must be established to allow metaverse users with their wearable devices to obtain access to the platform with proper identity. Moreover, IoT devices in metaverse infrastructure (e.g., sensors, UAVs) also need effective mechanisms to authenticate during their operations. To this end, identity management of IoT devices can benefit from blockchain [64] with decentralized solutions for key management [65], cross-domain authentication [66], [67], mutual authentication [68], and privacy preservation [69].

1) SELF-SOVEREIGN IDENTITY

While centralized identity and federated identity [70] are vulnerable to potential third-party risks, Self-sovereign Identity [71] (SSI) could be an appropriate authentication method for the decentralized metaverse. With SSI, users can prove their identity through verifiable credentials or claims [71]. Each user or organization is associated with a unique decentralized identifier document (DID), which can be used across different platforms. To this end, blockchain technology plays the role of storing all DIDs and making them immutable, transparent, and secure thanks to its decentralized property. For instance, the authors in [72] proposed a blockchain-based SSI model for passport-level biometry of Dutch government with advanced security features. The model leverages a personalized blockchain, *TrustChain* [73], to provide portability,

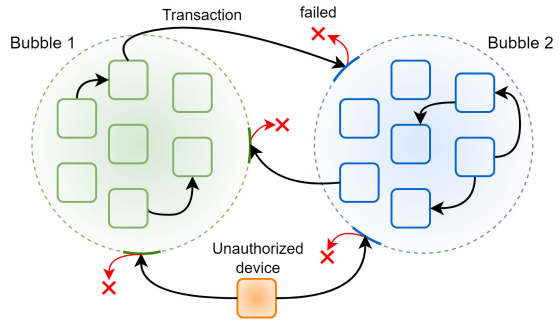

FIGURE 6. Bubbles of trust for IoT authentication presented in [74].

interoperability, minimalization, and protection for the claim format. Both interactive and non-interactive ZKP methods are implemented in four different schemes to minimize disclosure of claims and enhance portability. Performance evaluation of the four schemes also shows the model's efficiency and practicality.

2) THREATS FROM SPOF AND UNAUTHORIZED ENTITIES

Unauthorized users can exploit the vulnerabilities of centralized authentication system to get illegal access to the metaverse. As a result, they can participate in malicious activities such as phishing, scamming, and impersonation. In terms of user-side authenciation management, Esposito et al. [75] presented a distributed authentication framework for smart city applications based on blockchain technology. In particular, they integrate blockchain into FIWARE [76] and OAuth2 [77]. While XACML policies are stored in blockchain, FIWARE identity operations are regulated automatically by chaincode (i.e., smart contract) to provide decentralization. As a result, the framework can protect identity data from malicious and unauthorized users in a large scale scenario by using blockchain to remove Single Point of Failure (SPOF).

3) INTEGRITY OF IDENTITY DATA

If identity data of metaverse users are altered by malicious actors (e.g., during communication and message exchange), it could lead to serious security risks, resulting in financial losses, reputation damage, and privacy violations. The authors in [74] introduced *bubbles of trust*, a blockchain-based authentication system for IoT devices that can protect data integrity and availability. In particular, the system provides "bubble" zones (presented in Fig. 6) that allow devices to identify and trust each other within a same zone, while considering devices in other zones as malicious. Besides, messages exchanged in the platform are all signed by the ECDSA algorithm using the associated blockchain private key. These mechanisms offer secure communication between devices, providing resistance to sybil attack, spoofing attack, non-repudiation, and message substitution [74].

4) RESOURCE CONSTRAINTS OF WEARABLE IoT DEVICES

Wearable IoT devices used by metaverse users often have limited computation and storage capacity, while the capacity also varies among devices. To overcome performance limitations of IoT authentication, the authors in [78] proposed a hybrid blockchain-based scheme for multi-WSN. In the design (Fig. 8), IoT nodes are divided into different types based on their capability, forming a hierarchical structure including base station, cluster head nodes, and ordinary nodes. Base station with highest computing and storage resources is connected to a public blockchain. It manages authentication of its subnet's nodes which are implemented in a local blockchain. While ordinary nodes (with low energy and computing capacity such as camera or sensor) collect data, the data are preprocessed and forwarded to the node manager by cluster head nodes (with certain storage and computing resources). By doing so, the system is optimized based on nodes' capacities, thus achieving higher performance, while it is shown to be resistant to sybil, denial-of-service (DoS), message replay, substitution, and man in the middle (MITM) attack.

While wearable IoT devices are resource-limited, edge nodes can offer computation offloading to facilitate the authentication process. To improve the efficiency of distributed authentication systems, an authentication scheme based on blockchain and edge computing is proposed by the authors in [79]. Specifically, authentication data and logs are stored on a blockchain with optimized PBFT consensus algorithm. A novel caching strategy based on edge computing and belief propagation is proposed to enhance hit ratio. Thus, optimized edge nodes can obtain enough resource to provide efficient authentication service based on smart contracts. According to simulation results in [79], hit ratio is about 8%-14% more efficient than other existing strategies, while the figure for average delay is improved 6%–12%.

5) KEY MANAGEMENT IN AUTHENTICATION

To provide higher flexibility of key management, the authors in [80] proposed a blockchain-based mutual authentication protocol with dynamic key management for edge computing. In this protocol, edge severs participate in a blockchain system, in which a smart contract is designed to manage user keys after registration. It allows flexible key update and revocation without any trusted center, while eliminating the need for computationally expensive cryptographic mechanisms in key management. Therefore, the computational costs for the framework are around 80ms for the end-user and 8ms for the edge server, with a communication cost of 3.4 MB. These results show an improvement of 5-15% compared to existing platforms [81]. Besides, the framework is also shown to resist impersonation, replay, and stolen verifier attacks.

B. METAVERSE DECENTRALIZED GOVERNANCE

Governance plays a crucial role in determining the future of any digital platform. In traditional centralized systems, the

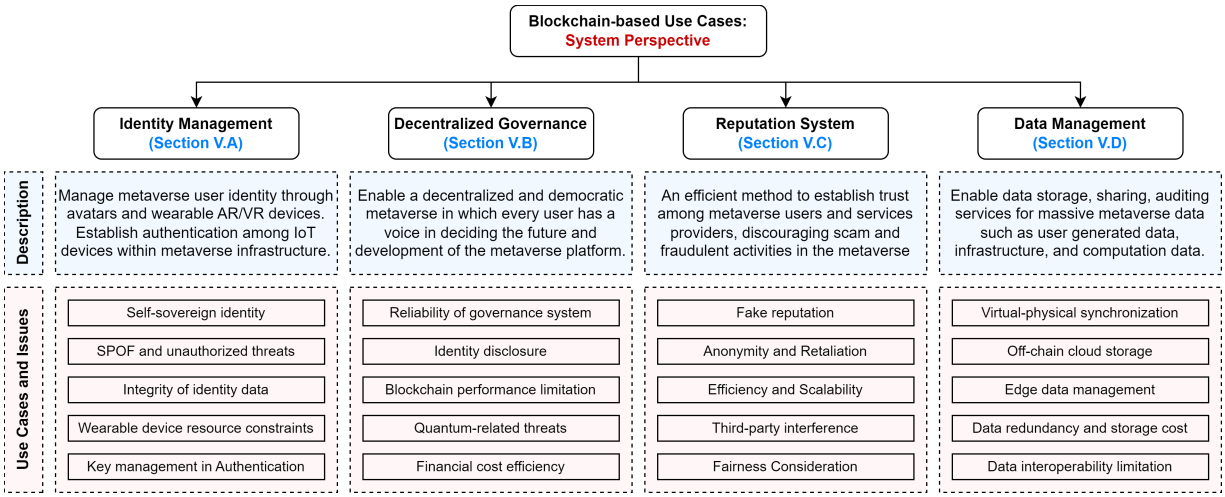

FIGURE 7. Blockchain-based use cases in the metaverse from system perspective.

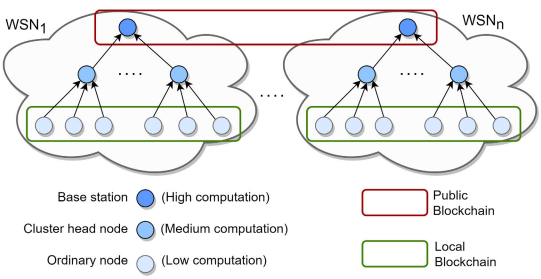

FIGURE 8. Hierarchical architecture of blockchain-based Multi-WSN model in [78].

platform provider has complete control over its development. They could unilaterally release updates that alter the rules and policies of the virtual world, leaving users with no option but to accept all the changes. Inevitably, the decentralized metaverse needs a democratic governance scheme in which users have a voice in deciding the virtual world's future.

To this end, blockchain technology offers DAO, a potential solution for decentralized governance in the metaverse. Unlike traditional centralized systems, DAOs are flat and democratic, with members required to vote for any changes or updates to be approved. For instance, Decentraland is a popular platform adopting DAO, where stakeholders can vote to determine policy update, including a wide range of aspects such as upgrading LAND, specifying dates of LAND auctions, and determining marketplace fees. In addition, blockchain and smart contract can be utilized in various ways to build reliable voting and decentralized governance schemes for the metaverse [82].

1) RELIABILITY OF GOVERNANCE SYSTEM

In decentralized governance schemes, integrity is the first and foremost factor deciding democracy of the platform. The authors in [83] presented BSJC, a proof of completeness algorithm that builds a specific blockchain for electronic voting platforms. In this scheme, votes are represented as transactions on a permissioned blockchain network, in which they are hashed to form a Merkle hash tree. With the recorded on-chain information, the authority can confidently query the voting counts, verify duplication of votes, and ensure the integrity of votes. However, there is still a third-party authority involving in the process, making it vulnerable to data leakage and tallying issues.

2) IDENTITY DISCLOSURE

During the election or voting process, user identity might be leaked, threatening the privacy of participants. To protect the tally and provide higher privacy, the authors in [84] proposed a blockchain-based self-tallying voting system named *Open Vote Network*. In [84], participants represent binary votes as blockchain-based zero-knowledge proofs. The proofs indicate voters' decision (i.e., voting yes or no) and prove voters' identity without revealing such their identity thanks to ZKP algorithm. In addition, smart contracts can compute the tally so that the system does not need a third-party authority counting and verifying the votes. However, the voting size in the proposed framework was limited to just around 60 electors. This scalability and performance limitations could hinder it from being adopted in a large-scale system like the metaverse.

3) BLOCKCHAIN PERFORMANCE LIMITATION

Blockchain often suffers scalability issues due to its decentralized nature, impacting on the performance of the overall system. To fill the gap of performance constraint, Khan et al. [85] investigated a wide range of permissioned and permissionless blockchain settings across different scenarios of their e-voting system. With a specific hardware specification, they adjust blockchain parameters, including block size, block rate, number of miners, difficulty of PoW, and

the number of concurrent clients to determine an optimized architecture with trade-offs between properties. However, there is no mechanism filtering out invalid voters in the proposed scheme, while it is shown to be insecure against quantum attacks [86].

4) QUANTUM THREATS

In the future, quantum computing technology might pose potential threats to blockchain-based systems [87]. To this end, the authors in [88] proposed an anti-quantum voting protocol using blockchain to offer tamper-resistant and decentralization features. They used a modified version of the code-based Niederreiter algorithm, an NP-complete Syndrome Decoding problem which is difficult to solve even with powerful quantum computers. Furthermore, blockchain and Key Generation Center in certificateless cryptosystem provide transparency and auditing functions to the platform.

5) COST EFFICIENCY

In a large-scale scenario, financial cost efficiency is also an important factor in blockchain-based governance schemes. The authors in [89] proposed a framework for e-voting system using smart contracts to enable cost-efficient election. The system utilizes a PoA-based permissioned blockchain with significantly lower cost and traffic compared to public chains of other platforms. Besides, it uses district-based voting to offer coercion resistance, while there are ''bootnodes'' that help district nodes to discover each other more efficiently.

C. REPUTATION SYSTEM

A reputation system allows users and service providers to build trust through feedback, rankings, ratings, and reviews of users for any service they have received. This can be an incentive mechanism which encourages service providers to offer quality services to maintain their reputation. When it comes to the metaverse, a reliable reputation system can provide a powerful trust mechanism to prevent fraud, scam, and improve the quality of service throughout the ecosystem. It allows users to rate each other after receiving the products, services, or any interaction with the others in the virtual world. Regarding this purpose, blockchain technology can be integrated into the reputation system to offer security [90], fairness [91], performance efficiency [92], and privacy perservation [93], [94], [95].

1) FAKE REPUTATION

Fake reputation can be popular in centralized platforms, in which users can create fake accounts to rate for themselves, while the central organization can also modify the rating data to earn financial benefits. The authors in [90] proposed a blockchain-based reputation system which resists fake reviews, sybil and collusion attacks. In this scheme, low reputation users must stake tokens into a triple signed wallet of PoS blockchain. This mechanism, along with the expensive cost of entrance, can discourage malicious reviews and sybil attacks effectively. Besides, an average-scoring mechanism and time interval between reviews are introduced to prevent collusion attacks.

2) ANONYMITY AND RETALIATION

In the metaverse reputation system, users may hesitate to vote low ratings due to the fear of retaliation from the recipients. To prevent bad-mouthing attacks, the authors in [94] proposed a trustless reputation system that offers anominity based on blockchain technology. In this scheme, the service provider must provide a token to the customer just before a purchasing transaction takes place. This token is based on the signature protocol, allowing the customer to prove that she is eligible to submit a review, while the token-based review will be unlinkable to the original blockchain transaction. This not only protects the service provider from bad-mouthing attacks, but also ensures privacy of customers since the reviews are verified without correlating to the reviewers' identity.

Moreover, the authors in [93] further elaborate the privacy requirements of reputation system in which not only the rating provider's identity is protected, but also the privacy of the rating weights and rating aggregation process is guaranteed. In their proposed system, ratings are recorded and managed by a blockchain with hybird consensus algorithm mixed between PoW and PoS. Rating provider's identity and the rating weights (assigned by reputation requesters) are both encrypted to provide anonymity for raters and requesters. In the rating aggregation process, homomorphic encryption is utilized to allow the aggregator to compute the final reputation without decrypting the rating weights.

3) EFFICIENCY AND SCALABILITY

A blockchain-based reputation system might suffer from low efficiency due to scalability issue of blockchain. To overcome this problem, the authors in [96] proposed an anonymous reputation system IIoT-Enabled Retail Marketing, in which the state-of-the-art Ouroboros consensus mechanism is utilized to provide higher efficiency and provable security. In this system, service providers act as stakeholders in Ouroboros PoS protocol, and the reputations are associated with their stake. Operations including review generation, verification, and aggregation are performed on smart contracts to ensure reliability, while registration and rating token generation are performed off-chain to reduce computation overhead of the blockchain and improve scalability. Furthermore, Bulletproof [97] is used as an efficient method to provide unlinkability between reviews and identities. A proof-of-concept prototype on Parity Ethereum has been conducted, showing that computation costs are only around 250-500 ms for rating token generation and registration processes.

4) THIRD-PARTY INTERFERENCE

To truly realize the decentralized metaverse, the intervention of third-party authorities must be minimized or even eliminated. Li et al. [98] presented a blockchain-based reputation

TABLE 4. The trade-offs between different methods of data storage for the metaverse.

	Storage strategy	Decentralization	Transparency	Querying capacity	Cheap storage	Data redundancy	Example
On-chain	Public Blockchain	High	High	Low	Low	High	Ethereum
	Consortium Blockchain	Medium	Medium	Low	Medium	Medium	Hyperledger
Off-chain	Centralized Database	Low	Low	High	High	Low	MongoDB
	Distributed Database	Low	Low	Medium	Medium	Medium	CosmosDB
	Distributed File System	High	Medium	Low	High	High	IPFS

system for e-commerce, *RepChain*, which is publicly verifiable without third-party intervention. Specifically, two-move lind signatures are leveraged to create anonymous credentials for the reviews, thus offering unlinkability of transaction and preventing user identity from being leaked. Zero-Knowledge Range Proof (ZKRP) is used to verify the submitted reviews and detect abnormal reviews. Certificate Authority is the only centralized party in [98], but it only takes responsibility for generating cryptographic keys, and will go offline after finishing the entity registration process. Therefore, the ratings would be more reliable, while the system remains fully decentralized thanks to blockchain.

5) FAIRNESS CONSIDERATION

Fairness is also a major concern of the metaverse reputation system to ensure participant's benefits. The authors in [91] proposed a blockchain-based reputation system emphasizing fairness for peer-to-peer energy trading. In this scheme, the reputation rating is weighted based on a linear combination of all participants' current reputation scores. Intuitively, the vote of a low-reputation user should have less impact than the ones with high reputation score. There are also a set of significance factors to adjust the impact of each role (i.e., the seller, buyer, and consensus node) in the formula based on specific use cases [91]. As a result, it could further improve the fairness and quality of reviews in the system.

D. DECENTRALIZED DATA MANAGEMENT

Data management in the metaverse is a critical task impacting on most aspects of the platform. In general, Metaverse data can consist of various sources such as (i) user-generated data from metaverse service providers and users' activities; (ii) infrastructure data collecting by IoT devices for virtual-physical synchronization; (iii) Computation data from computing processes such as edge and cloud computing. However, if data in the metaverse are all stored in traditional centralized databases, they would be vulnerable to various risks such as SPOF, third-party, and privacy issues.

For data management, blockchain technology can offer a wide range of advantages such as decentralization [99], security [100], [101], and auditability [102]. However, storing data on blockchains is extremely expensive due to its decentralized nature. One approach to address the limitations of blockchain with regards to storage cost and capacity is to use consortium blockchain, in which access is only granted to authorized participants, thus reducing the amount of on-chain data stored, improving the processing speed, and reducing transaction cost. Another solution for data storage in the metaverse is to leverage off-chain mechanisms, in which only the hash and a small part of the data are stored on the blockchain, while the metadata can be stored by traditional storage mechanisms. Illustrated in Table 4, the extent of decentralization, storage cost, and transparency can be adjusted based on different storage strategies.

1) VIRTUAL-PHYSICAL SYNCHRONIZATION

In virtual-physical synchronization process, blockchain-based data management can help to manage data collecting by IoT devices in the physical world [103]. Li et al. [104] proposed a blockchain-based scheme for large-scale IoT data storage, in which a blockchain replaces third party to manage data storage with trust ensuring. In this scheme, massive data from IoT devices are collected by the corresponding edge servers, then forwarded to the blockchain as transactions to authenticate the devices. Besides, certificateless cryptography is implemented to offer an efficient way to identify IoT devices. As a result, the design is proved to be *IND-CCA* secure, while it achieves traceability and accountability thanks to the blockchain's features.

2) OFF-CHAIN CLOUD STORAGE

The massive amount of data generated from the metaverse's operation may exceed the storage capacity of blockchain, thus necessitating the use of cloud storage. In this case, blockchain can provide integrity services for the cloud [105]. Regarding off-chain cloud storage, the authors in [106] proposed a blockchain-based data storage for IoT with data integrity protection. In the proposal, a dynamic data integrity verification protocol is implemented via smart contracts, called DIS smart contracts. Whenever data are uploaded to cloud storage, the data owner can trigger the DIS smart contract to verify the uploaded data. It compares the hash provided by the data owner and the cloud-based hash to determine the validity of data, ensuring data integrity. A prototype of the system has been constructed to prove its high performance and feasibility.

3) EDGE DATA MANAGEMENT

Certain light-weight tasks of wearable devices can be processed in edge environment without committing to cloud servers, providing faster response and computation efficiency. Regarding edge computing, the authors in [101] proposed a framework for edge data management with blockchain-based trust establishment. In this scheme, smart

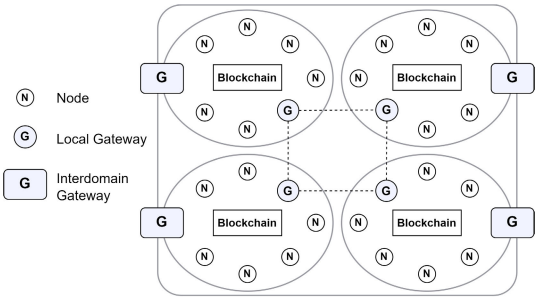

FIGURE 9. Internet-inspired architecture for blockchain data interoperability presented in [110].

contracts in the blockchain network layer take responsibility for edge data management operations (e.g., data invoking and transferring), providing trust and data integrity. Besides, sensitive edge data are protected thanks to a matrix-based multichannel architecture with conditional access, making the data invisible among users in different channels.

In terms of edge data sharing, the authors in [107] developed a reputation-based data sharing framework for edge computing with verifiable credibility of data source. Firstly, edge nodes are incentivized to contribute to storage resource through a *DSSC* smart contract with proof of storage. Secondly, they act as miners in a PoW process of *ISSC* smart contract to provide data sharing, searching, and auditing for data requestors. Besides, a three-weight subjective logic model is designed to estimate reliability of data based on interaction frequency, event timeliness, and trajectory similarity of data source.

4) DATA REDUNDANCY AND STORAGE COST

In blockchain data storage, every consensus node must store a replica of the on-chain data, causing high data redundancy and storage cost. The authors in [108] proposed an algorithm to reduce this resource overhead issue based on regenerative code technology, which allows failed data on a damaged node to be recovered by surviving nodes in the network [109]. For instance, if the original data are extended by certain amount of regenerative code, a proportional number of nodes are allowed to be damaged without impacting on data integrity. Experimental results show that the proposed framework can reconstruct the original files with real-time performance and offers blockchain-enabled security features.

5) DATA INTEROPERABILITY LIMITATION

In blockchain-based data management in the metaverse, the independence among blockchain platforms can be an obstacle to data sharing. Consequently, higher level of decentralized data management requires data interoperability between different blockchains. This can include the communication between public blockchains as well as between both public and permissioned blockchains [39]. To this end, the authors in [110] proposed an internet-inspired blockchain architecture offering data interoperability based on blockchain gateways. As shown in Fig. 9, blockchain networks are modelled as autonomous systems (i.e., routing domains in the Internet architecture). Consensus nodes in blockchain play the role of local gateways within its domain, while there are certain nodes take responsibility for global communications (i.e., inter-domain gateways). Due to the isolation and independence among domains, inter-domain gateways must establish technical trust based on hardware devices, including TPM [111] and SGX [112]. By doing so, blockchain systems can inherit fundamental properties of the Internet such as interoperability, survivability, and manageability.

However, blockchain gateways could suffer from crashing due to external attacks. Belchior et al. [113] proposed *Hermes*, a middleware framework for blockchain interoperability that offers crash-recovery features for gateways based on ODAP protocol [114]. Whenever a blockchain gateway is crashed, based on a rollback timeout, the protocol either (i) recovers the gateway operations using its logs within the timeout, or (ii) rollbacks the gateway to its previous state on the affected blockchains. The proposed framework makes gateway-based data interoperability more reliable and able to withstand various attacks.

VI. BLOCKCHAIN FOR SECURITY AND PRIVACY OF METAVERSE INFRASTRUCTURE

The metaverse is envisioned to exceed far beyond the entertainment purpose, including a variety of activities related to economy, finance, and business [3]. Therefore, security and privacy are obviously critical factors that impacts on most components of the virtual world [2]. While Sections IV and V have illustrated the potentials of blockchain in providing security and privacy of metaverse applications, this section focuses on security and privacy for metaverse infrastructure divided into three layers, namely metaverse end devices, communication network, computing and storage. In particular, the security and privacy threats are discussed for the three layers of the metaverse infrastructure, as illustrated in Fig. 10. While many traditional approaches have been developed to tackle these threats, blockchain-based solutions also show the potential in solving many of the mentioned issues. Due to the scope of our paper, we will only discuss blockchain-based countermeasures for metaverse security and privacy threats in the following.

A. THREATS TO METAVERSE END DEVICES

In the metaverse, users are often equipped with wearable virtual-reality devices (e.g., AR/VR headsets, haptic gloves) to participate in the virtual world. Besides, metaverse end devices also include numerous IoT and mobile devices that collect real-world data to reflect into the virtual environment through DT. Regarding end devices, various attacks can be launched.

1) ACCESS CONTROL ATTACK

Attackers can exploit the vulnerability of access control process to allow unauthorized devices to get access to the metaverse system, while preventing eligible devices from

TABLE 5. Literature reviews on various issues in the blockchain-enabled metaverse and possible solutions based on existing works.

Application	Ref.	Issue	Proposed Solutions	Main Technology
Identity and Authentication System	[72]	Practicality of SSI system	Leverage personalized blockchain for protection of claims. ZKP helps minimizing the disclosure of claims.	Blockchain, SSI, ZKP
	[74]	Data integrity and availability issue	Divide nodes in the IoT system into different bubble zones. Nodes within a zone can identify and trust each other.	Blockchain
	[78]	Performance limitations	Construct a hierarchical network based on node's capability to optimize performance and provide mutual authentication.	Local, public blockchain
	[79]	Limited resource and computation	Design an edge-based caching strategy to enhance efficiency. Authentication data are stored on an optimized blockchain.	Smart contract, blockchain
	[80]	Flexibility of key management	Edge servers join a blockchain network for authentication. Smart contracts provide dynamic key update and revocation.	Smart contract, blockchain
	[75]	Threats from unauthorized users	XACML access-control policies are stored in blockchain. FIWARE identity operations are regulated by chaincode.	FIWARE, OAuth2
Metaverse Decentralized Governance	[83]	Transparency and verifiability	Store votes on-chain as transactions in a Merkle hash tree, thus offering transparency and verifiable voting.	Blockchain
	[84]	Third-party risks in tallying process	Eliminate the role of third partites by ZKP to ensure privacy. Tally can be computed automatically by smart contracts.	Blockchain, ZKP
	[85]	Performance and scalability limitation	Investigate the trade-offs of blockchain-based voting system in various scenarios to optimize performance and scalability.	Blockchain
	[89]	Cost efficiency in large-scale scenario	PoA-based permissoned blockchain for higher efficiency. District-based scheme provides coercion resistance.	Blockchain
	[88]	Quantum attacks	Utilize code-based Niederreiter to prevent quantum attacks. Blockchain provides transparency and auditing functions.	Niederreiter code
Metaverse Reputation System	[90]	Fake reputation and collusion attacks	Stake tokes into a triple signed wallet to prevent malicious transactions. Adopt a time interval to offer adaptability.	Blockchain
	[94]	Bad-mouthing attacks & retaliation	Leverage ZK proofs to hide user identity when rating. Utilize blockchain to provide decentralization and trust.	Blockchain, ZKP
	[93]	Privacy leakage of participants	Encrypt the rating weights by requestor's private key. Homomorphic allows the aggregating without decryption.	Blockchain, homomorphic encryption
	[96]	Low efficiency and scalability	Improve efficiency by utilizing Ouroboros consensus protocol. Provide anonymity thanks to Bullletproof algorithm.	Blockchain, Bullletproof
	[98]	Third-party issue and biased decisions	Create anonymous credentials to prevent identity leakage. ZKRP are used to verify reviews, instead of third party.	Blind signature, ZKRP, blockchain
	[91]	Fairness of rating	Calculating reputation score based on a weighted formula, which depends on current reputation of all participants.	Blockchain
Decentralized Data Management	[104]	Trust issues of centralized storage	Large-scale data storage is managed by blockchain storage. Certificateless cryptography enables device authentication.	Certificateless cryptography
	[108]	Data redundancy, resource overhead	Allow failed data on damaged nodes to be recovered by surviving nodes using regenerative code.	Regenerative code, blockchain
	[106]	Data integrity issue	A dynamic data verification smart contract is deployed to compare hash of the cloud-based data and original hash.	Blockchain, DFS, cloud storage
	[101]	Management of edge data	Smart contracts offer trusted edge management operations. Sensitive data are hiden by conditional access scheme.	Blockchain, edge computing
	[107]	Credibility of data source	A three-weight subjective logic model helps estimating data reliability and source credibility based on smart contracts.	Blockchain, edge computing
	[110]	Lack of data interoperability	Design a blockchain architecture offering interoperability based on Internet architecture with blockchain gateways.	Blockchain gateways
	[113]	Gateways crashing in interoperable scheme	Design blockchain gateways with crash-recovery strategy and define a threshold to rollback blockchain state.	ODAP protocol

participating in the platform [115]. Once obtaining illegal access to the system, unauthorized avatars can impersonate legitimate users or devices, thereby conducting phishing scam, digital footprint tracking [116], and deceiving the victim's friends in the metaverse.

2) MALWARE ATTACK

One major source of security and privacy issues is the ability to inject malicious third-party applications (i.e., malware) into metaverse end devices [117]. Through these applications, attackers can dominate the devices, stealing sensitive data and disrupting their operation [118]. Currently, malware is mainly spread through traditional methods such as email attachments and malicious websites. When it comes to the metaverse, interaction between users are significantly enhanced with virtual reality technology, thus it would be more potential for attackers to convince and trick victims into accessing malicious sources through their devices.

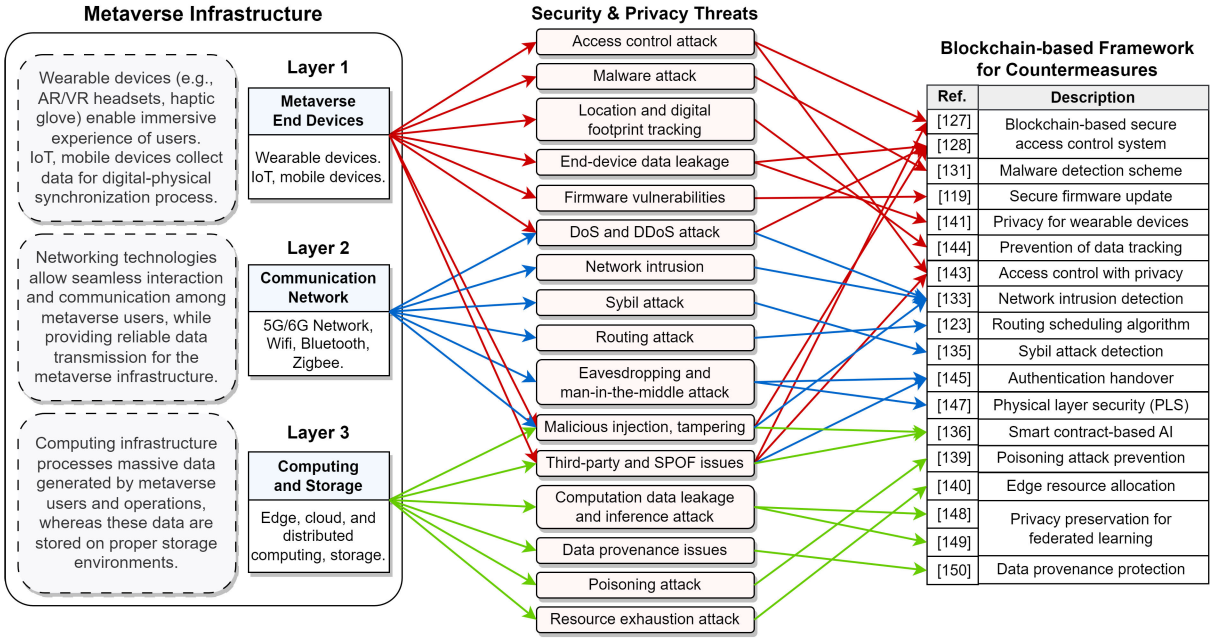

FIGURE 10. Security and privacy threats in the metaverse infrastructure.

3) LOCATION AND DIGITAL FOOTPRINT TRACKING

If physical location of metaverse users is tracked through their wearable devices, metaverse-related crimes may no longer limited to the virtual world, but also in the real world. Besides, hackers can collect avatar's digital footprints to link the avatars to the corresponding real-world identities based on the recorded behavior pattern and habits from their devices [2].

4) END-DEVICE DATA LEAKAGE

Wearable AR/VR devices would collect far more sensitive data from metaverse users compared to traditional platforms. For example, the devices would scan user's appearance to construct avatars in the virtual world, while user's voice and activities are also recorded to be reflected into the avatars. Thus, end devices can be a powerful source of personal data leakage, which can be used for further social engineering attacks such as impersonation and phishing scam.

5) FIRMWARE VULNERABILITIES

Firmware is another vulnerable target with low-level control of devices. While malicious firmware can be embedded into the devices by attackers or such the device producers, certain firmware processes (e.g., firmware update) are prone to security and privacy risks [119]. For instance, since the metaverse is a real-time environment, the delay for firmware update might disrupt the operation and interaction of metaverse devices, causing security vulnerability in specific time intervals.

6) DoS AND DDoS ATTACK

Metaverse end devices often have limited resource and energy, thus being prone to DoS attacks such as battery draining, sleep deprivation, and outage attack [120]. Furthermore, when attackers obtain access to a large number of IoT devices, they can collude to conduct distributed denial-of-service (DDoS) attack to overwhelm and disrupt the metaverse decentralized infrastructure.

7) MALICIOUS INJECTION AND TAMPERING

Due to the immersive experience of metaverse, attackers can inject harmful content in front of user avatar, harassing or even committing crime to users who suffer mental issues [2]. Besides, IoT data from the corresponding devices could be tampered to provide false information to the metaverse system, impacting on other process such as computing.

8) THIRD-PARTY AND SPOF ISSUES

These issues often take place when the management system of devices is centralized. If the centralized system is attacked, this can impact to the entire management scheme. Furthermore, third-party authorities can obtain sensitive information from user devices, while it is challenging to ensure that they always their activities in an honest manner.

B. THREATS TO COMMUNICATION NETWORK

As a paradigm of the next-generation Internet, the metaverse can take advantages of current communication and networking technologies such as 5G/6G, Wifi, Bluetooth, and Zigbee. Thus, it is also vulnerable to a wide range of network-related threats.

1) EAVESDROPPING AND MAN-IN-THE-MIDDLE ATTACK

Eavesdropping is a dangerous privacy threat in which attackers can listen to private conversation between metaverse

nodes. Consequently, the eavesdropper can further conduct MITM attack to impersonate one of the parties in the conversation. For example, the eavesdropper inserts itself in a private communication between a metaverse user and a metaverse application. Then, the attacker secretly relays and alters the messages from the application to persuade the user to give away login credentials, thus obtaining illegal access to the user's avatar.

2) NETWORK INTRUSION

Similar to access control attack at end-device layer, network intrusion allow attackers to gain unauthorized access to the metaverse network. Consequently, the intruders can carry out further attacks on the network such as collusion, DoS, eavesdropping, and MITM attacks. In general, network intrusion can be organized through the use of phishing scams or spreading malware such as viruses and trojans [121].

3) SYBIL ATTACK

In a decentralized peer-to-peer network, attackers can add sybil nodes with many fake identities to gain the majority of influence in the network, thus manipulating the network [122]. This type of attack is often effective in reputable system such as the metaverse reputation system presented in Section V-C.

4) DoS AND DDoS ATTACK

At networking layer, DoS attack floods the metaverse network with traffic and requests, overwhelming its capacity and causing downtime. This can disrupt metaverse services and prevent legitimate users from accessing the network or services in the virtual world.

5) ROUTING ATTACK

Routing attacks such as BGP hijacking can be arranged to redirect traffic to a different destination than intended [123], thus stealing sensitive information of metaverse users (e.g., authorization, identity data) or causing communication interruption (e.g., through routing loops).

6) MALICIOUS INJECTION AND TAMPERING

From networking and communication layer, the attackers can capture, alter, replay packets and inject fraudulent packets into communication links [120]. This can threaten severely to the integrity of metaverse data.

C. THREATS TO COMPUTING AND STORAGE

With massive data needed to be processed, metaverse computation must be a proper combination of different techniques, including both edge and cloud computing, storage. Although end devices often have limited resource, their capacity would be improved significantly along with the mature of the metaverse overtime. Therefore, distributed computing based on end-user nodes is also a potential technique for the metaverse. However, there are a wide variety of threats related to metaverse computing and storage that must be overcome.

1) POISONING ATTACK

This attack often takes place in decentralized computation schemes in which multiple nodes contribute computation resource to a specific task. In this case, malicious actors can intentionally submit wrong or random results to the computing system, thus poisoning the computation outputs. For example, random gradients submitted by malicious nodes in a federated learning scheme can make the final model less accurate, while the dishonest actors can still receive reward if their action is not detected.

2) COMPUTATION DATA LEAKAGE AND INFERENCE ATTACK

On the one hand, input data for the computation process can be leaked at storage and computation layer. On the other hand, hackers can also attempt to infer valuable or sensitive information from the computation outputs (i.e., inference attack). For example, an attacker can steal the training data of Deep Learning models in the metaverse, while he can also collect the parameters trained on the model. Then he uses specific mechanisms to obtain the data on which the models have been trained. If the data contains sensitive information (e.g., medical data), it would threaten the privacy of metaverse users severely.

3) RESOURCE EXHAUSTION ATTACK

In centralized edge or cloud servers under the metaverse infrastructure, attackers can organize resource exhaustion attack in which consecutive resource requests are submitted to consume the system's computation resource, making it slow or even unresponsive. Thus, it is crucial to construct a reliable resource allocation scheme which can detect malicious nodes and their abnormal resource requests.

4) DATA PROVENANCE ISSUES

Data provenance is the history of the origin, ownership, custody, and processing of a piece of data, from its creation to its current state. In a metaverse application that collects user data, data provenance can help ensure that the data is collected and processed in compliance with applicable privacy regulations and user consent. However, the critical issue in data provenance is to ensure the integrity of the provenance, making it traceable and resistant to tampering.

5) MALICIOUS INJECTION AND TAMPERING

At storage level, if attackers can obtain illegitimate access into storage environment (e.g., cloud storage), they could tamper the data or inject fraudulent data into the system. For example, the attacker can modify identity data of metaverse avatars, preventing honest users from accessing their avatars.

6) THIRD-PARTY AND SPOF ISSUES

In centralized computation and storage systems, if the central authority is hacked or they simply act dishonestly, SPOF

might occur and impact on the entire ecosystem instead of certain specific failed nodes. Furthermore, trust management in these schemes often rely on third-party entities, making the computation system vulnerable when these parties stop operating or provide malicious services.

D. SECURITY COUNTERMEASURES

1) BLOCKCHAIN-BASED SECURITY FOR METAVERSE END DEVICES

Blockchain and smart contract can enable decentralized access control schemes for IoT devices with enhanced security [124], [125] and efficiency [126]. To this end, Ding et al. [127] presented a blockchain-enabled access control scheme for IoT devices, in which distribution of attributes is recorded on blockchain to prevent SPOF and data tampering. Access management is regulated by multiple attribute authorities, who (i) play the role of consensus nodes in blockchain network to distribute attributes to IoT devices, and (ii) act as the key generation center to manage registration of devices. The attribute authorities grant requested attributes to devices via blockchain transactions, while only devices with satisfied attributes can obtain access. According to the performance analysis, when the number of attributes reach 30, computation overhead for the requester and the verifier is about 100 ms and 250 ms respectively, which are acceptable in access control systems. Security analysis shows that the system can resist SPOF, collusion, and impersonation [127].

To make the access control system more decentralized and automatic, the authors in [128] presented another scheme for IoT devices in which access control is managed by a single smart contract with configurable access control policies (illustrated in Fig. 11). Communication between devices is enabled by DTLS [129] to prevent spoofing and tampering. Due to the resource constraint of IoT devices, the devices do not join the blockchain network directly, but instead request access from the smart contract through different *management hubs*. Signed certificates is utilized to ensure the integrity of these *management hubs*. A prototype is developed on an Ethereum-based blockchain, while its security is analyzed by STRIDE model [130], showing that the system is resistant to DoS, tamper, and information leakage.

Besides access control, malware is also a potential security threats to metaverse devices. The authors in [131] proposed a blockchain-based malware detection system for Android mobile devices using statistical analysis method. In [131], a multi-feature model with fuzzy comparison method is designed to analyze various malware families. Besides, a consortium blockchain with personalized block structure is deployed as a fact-base for malicious codes, storing all malware detection results. Blockchain characteristics ensure that the fact-base is transparent and secure, while also providing evidence tracking of malware.

For secure firmware processes, the authors in [119] designed a blockchain-based firmware update scheme for embedded IoT devices, using blockchain to securely check

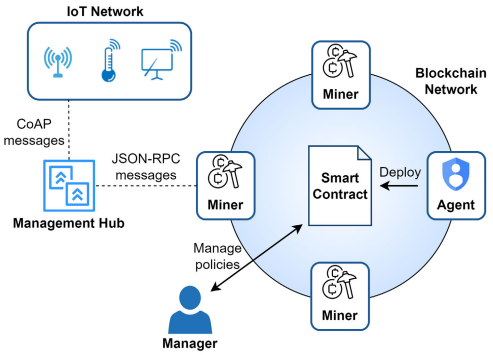

FIGURE 11. Securing access control based on smart contract presented in [128].

the firmware version, validate the correctness, and download the latest firmware update. To do so, the block structure has been modified to include a new verification field, which consists of firmware version, logs, hashing verifier, and related information. The distributed model allows IoT devices quickly check and download the latest firmware version, thereby minimizing the vulnerable period and preventing devices from firmware-related attacks.

2) BLOCKCHAIN-BASED SECURITY FOR METAVERSE COMMUNICATION NETWORK

Network intrusion detection [121] is an effective mechanism to prevent a wide range of cyberattacks such as DoS, ransomware, worms, backdoors, and man-in-the-middle attacks [132]. Regarding blockchain-based intrusion detection, the authors in [133] proposed a collaborative intrusion detection model named *Deep Blockchain Framework*. Specifically, multiple nodes in the blockchain network collaboratively run a bidirectional long short-term memory deep learning algorithm to detect network intrusion in different subnetworks. The detection results and intrusion alerts are then stored permanently on blockchain, enabling a large-scale intrusion detection scheme with enhanced accuracy thanks to the collaborative operation. The proposed framework is assessed on UNSW-NB15 [134], a research-oriented data set for network intrusion detection systems, resulting in high efficiency and accuracy.

To prevent routing attacks in wireless networks, the authors in [123] proposed a routing scheduling algorithm with trust management based on blockchain and reinforcement learning. In this scheme, nodes dynamically select shortest routing paths thanks to a reinforcement learning model, while routing information is stored on blockchain to offer data integrity and traceability. Besides, a token-based incentive mechanism on PoA blockchain consensus ensures that malicious routing information would not be uploaded to the blockchain network.

Regarding sybil attack, a blockchain-based framework for sybil attack detection in wireless sensor networks is presented in [135]. In this scheme, blockchain is used to manage the state of sensor nodes in the network, in which any

changes (e.g., in location) will be recorded into blockchain transactions. With continuous on-chain observation of node's status, a sybil node (which has the same identity with a legitimate node, but different timestamp and connection) will be detected when it tries to access the network.

3) BLOCKCHAIN-BASED SECURITY FOR METAVERSE COMPUTING AND STORAGE

In terms of computation in the metaverse, smart contract can be used to improve security of AI models [136] and distributed learning mechanisms [137], [138]. The authors in [136] utilize smart contracts to directly implement AI algorithms such as Linear Regression, Naive Bayes, and Neural Networks to empower the metaverse. By this way, the "AI smart contract" can make cognitive decisions automatically with trust establishment. This removes the centralized parties and provides resistance to SPOF and tampering. Besides, training data are stored on IPFS to ensure integrity. Using up to $16 gas fee for each prediction, this can be an acceptable trade-off in case the AI-based decision is significantly important. However, larger and more complex models will require much more resource and would not be applicable in practice.

Besides, distributed learning models for the metaverse can also suffer various threats such as poisoning attacks. The authors in [139] proposed a reputation-based mechanism that prevents collusion and poisoning attacks in FL by a consortium blockchain with contract-theory-based incentive. Specifically, participant's reputation is calculated by a multi-weight subjective logic model, based on their interaction history and frequency. Besides, a five-stage worker selection scheme is designed to recognize malicious candidates and avoid collusion attacks.

In terms of cloud and edge computing, blockchain can be utilized as a countermeasure to resource-related attacks. The authors in [140] introduced *EdgeChain*, a blockchain-based framework for edge computing that resists DoS and resource exhaustion attacks. The framework is built on top of a credit-based resource management scheme, deployed on smart contracts. If there are edge nodes making maliciously consecutive resource requests, the smart contracts with built-in policies will execute automatically to identify the malicious node and reduce its balance. Since attack logs are stored transparently on blockchain, these data can also be used to calculate credit of edge nodes to actively prevent future attacks.

E. PRIVACY COUNTERMEASURES

1) BLOCKCHAIN-BASED PRIVACY FOR METAVERES END DEVICES

When users use wearable AR/VR devices in the metaverse, these devices must collect their personal information for different purposes such as construction of avatars and profiles [2]. To protect data privacy of wearable embedded devices, the authors in [141] proposed a ring signature-based framework for privacy preserving of wearable IoT devices. Blockchain is combined with ring signature protocol [142] to enhance user privacy, in which the signatures are mixed among groups (i.e., the ring) so that the identity of signature's owner is kept secret. Data privacy is further improved thanks to a double encryption process with ARX symmetric encryption for data and asymmetric encryption for authentication.

In terms of device access control, the authors in [143] introduced *FairAccess*, a privacy-preserving framework for IoT access control management based on smart contracts. In this framework, access control policies (e.g., ABAC) are codified in smart contracts and triggered by FairAccess transactions. Whenever necessary access control conditions are fulfilled, the requesters will receive a token to obtain access to the specific protected resource. This is done automatically by smart contracts, thus eliminating data leakage risks from third-party authorities.

Besides, location tracking is another major privacy concern of wearable devices in the metaverse. The authors in [144] proposed a privacy-preserving blockchain architecture optimized for IoT devices, which can be applied to protect devices from location tracking. In this architecture, IoT vehicles and devices store location information in built-in storage that is not disclosed to third parties. The owners can decide what data can be exchanged, while communication in the network is encrypted using asymmetric encryption to further protect privacy.

2) BLOCKCHAIN-BASED PRIVACY FOR METAVERES COMMUNICATION NETWORK

In terms of networking technology, the authors in [145] proposed a blockchain-based authentication handover framework for 5G networks with enhanced privacy protection. In [145], the handover mechanism utilizes blockchain and software defined networking (SDN) to transmit authentication keys in 5G, thus eliminating eavesdropping and third-party privacy leakage. Specifically, these data are encrypted by blockchain-based keys, then divided into multiple parts and transmitted along different paths as programmed by the SDN controller. Therefore, privacy level can be adjusted by modifying the number of transmission paths, resulting in a trade-off for complexity.

At lower system level, eavesdropping in communication can be prevented by physical layer security (PLS) technique [146], in which there would be relay operators exploiting the physical layer properties of channels to protect information against eavesdropper through proper signal coding and processing. In terms of PLS, the authors in [147] proposed a distributive auction scheme for PLS based on blockchain and double auction theory. Firstly, a blockchain-based incentive mechanism is designed to encourage users participate in the distributed auction process of PLS. Secondly, smart contracts help verifying bids, preventing cheating such as multiple-bid submission and fake identities.

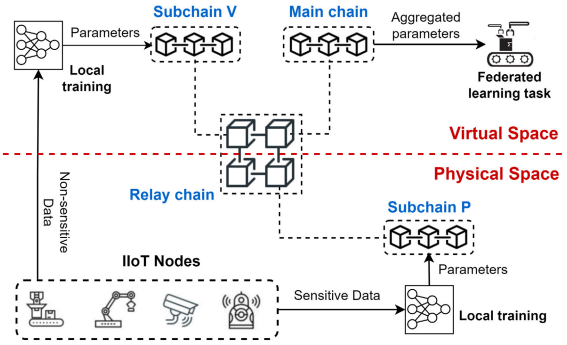

FIGURE 12. Privacy-preserving federated learning framework for industrial metaverse presented in [148].

3) BLOCKCHAIN-BASED PRIVACY FOR METAVERES COMPUTING AND STORAGE

The authors in [148] designed a federated learning scheme for industrial metaverses, using blockchain to prevent privacy leakage of sensitive data. In this scheme, data collected by IoT nodes are classified into sensitive and non-sensitive data types. Illustrated in Fig. 12, while non-sensitive data can be transmitted to higher-level systems for normal learning-based metaverse tasks, sensitive data are kept in the physical space to protect privacy. In the physical space, IoT edge devices perform local federated training, then submit the trained parameters to one of multiple subblockchains. Finally, all learned parameters from subchains are aggregated in a main blockchain, finishing a federated learning iteration. As a result, privacy is protected efficiently since sensitive data are all kept at the physical level.

However, the parameter updating process can also be prone to privacy risks such as inference attack (i.e., attackers attempt to obtain information from the learned parameters). Weng et al. [149] proposed *DeepChain*, a privacy-preserving scheme for federated learning, in which privacy is ensured during the gradient collecting process. Specifically, after a node finishes a local training iteration, it must encrypt the trained parameters before uploading them to prevent inference attack. A ZKP-based proof of correctness is attached into the uploaded gradients so that participants can determine whether the gradients are correctly computed, while they can learn nothing from it. A collaborative process among parties is required to decrypt the parameters, while a blockchain-based incentive mechanism ensures that the process will be correctly executed by the majority of participants.

In terms of cloud computing and storage, Liang et al. [150] proposed a blockchain-based cloud data provenance architecture with enhanced privacy preservation, named *ProvChain*. In this scheme, user privacy is protected thanks to an ID hashing mechanism that only allows the data auditor to access the provenance data, while identity of the owner is kept secret and cannot be inferred from the recorded data. For data privacy, provenance data are encrypted by the key pairs generated by the cloud service provider.

VII. METAVERSE DIGITAL ASSET MANAGEMENT

This section describes the roles and potentials of blockchain for digital asset management in the metaverse. There is a need for a digital asset management system that guarantees the rights of users and protects the platform from bad content. In this section, we discuss an 8-stage workflow for metaverse digital asset management integrating the blockchain technology as shown in Fig. 13.

A. IDEATION AND CREATION

In these two stages, users firstly develop the ideas of the digital products of interest. Then, they utilize tools suggested or provided by the publishers to realize their ideas before going through a series of stages to ensure the quality of digital assets and the rights of the creators. During this process, blockchain could enable a shared development environment in which multiple creators contribute to a particular digital content. For example, the authors in [151] introduced a decentralized content creation platform for digital learning using blockchain. In particular, blockchain is used in the content development process, where multiple creators take part in a permissioned blockchain. After a topic is created, any approved participant could propose adding customized content to the topic through the blockchain-based framework. It makes the creation process decentralized and transparent among creators. Furthermore, smart contracts can be utilized for versioning control in the content creation process. A tree structure of content versions is presented in [152] for tracing the video source origin. In this structure, the original digital content is stored in IPFS and pointed to by a smart contract. Other creators could request to make another customized version of the content and represent it as another smart contract. The new content's smart contract is considered as a ''child'' contract and it points to the ''parent'' contract (e.g., the source content), forming a tree-like model. As a result, users can easily trace back to the source version of the content from any branches.

B. CLASSIFICATION AND REVIEWING

The digital world could be affected negatively in both legality and social acceptance if there are illegal, offensive digital contents available in the platform. Thus, it is crucial to construct an auditing strategy that can filter out illegal contents efficiently. To facilitate the reviewing task, several blockchain-based techniques have been proposed. For instance, a platform combating against Internet of fake media things is proposed in [153]. The authors introduced a blockchain-based solution using PoA consensus to control the source of news. In this scheme, whenever a piece of news is submitted, it must be validated by a group of validators selected by reputation score. Then, validators rely on documents submitted by news organizations to decide the eligibility of each news. If a consensus is reached and the news is approved, a transaction containing the news is committed into the blockchain. Otherwise, the news

TABLE 6. Literature reviews on security and privacy of metaverse infrastructure with the corresponding blockchain-based countermeasures.

Aspect	Security		Privacy	
Infrastructure Layer	**Ref.**	**Countermeasures**	**Ref.**	**Countermeasures**
Metaverse End Device	[127]	Securing access control with resistance to SPOF, data tampering, and impersonation attacks.	[141]	Ensuring data privacy of wearable embedded devices by encryption and signature techniques.
	[128]	Smart contracts regulate access control policies, offering protection against DoS, spoofing attacks.	[143]	Eliminating third-party privacy leakage in access control of devices.
	[131]	Detecting malware attacks in mobile devices.	[144]	Preventing location tracking by built-in storage and encryption techniques in communication.
	[119]	Protecting firmware update process of devices.		
Communication Network	[133]	Network intrusion detection to further prevent DoS, malware, backdoors, and fuzzers attacks.	[145]	Preventing eavesdropping and third-party data leakage in authentication handover of 5G.
	[123]	Prevention of routing attacks and SPOF threats	[147]	Protecting data privacy in networking by physical layer security based on blockchain.
	[135]	Sybil attack detection in wireless sensor network.		
Computing & Storage	[136]	Securing AI model in metaverse by blockchain based "AI smart contracts".	[148]	Privacy preserving technique for sensitive data at physical level of metaverse's FL models.
	[139]	Protecting FL models from poisoning attacks, fraudulent injection, and sybil attacks.	[149]	A framework for FL that resists inference attacks from gradient collecting process.
	[140]	Prevention of DDoS and resource exhaustion attacks in edge computing.	[150]	Privacy preservation of data provenance and user identity in cloud computing and storage.

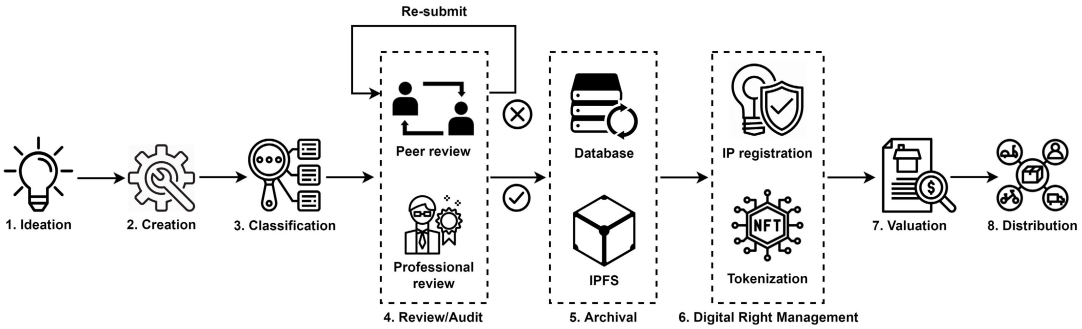

FIGURE 13. The 8-stage digital asset management workflow in the metaverse.

considered as fake news and its publisher is punished by reducing reputation.

Similar solutions could be adopted in the metaverse for reviewing UGCs. However, the metaverse needs an efficient system that can be applied for various types of digital content. The authors in [154] proposed a decision making system using a consensus algorithm based on PoA. In this scheme, each decision is assigned a ranking score calculated based on the total up votes and down votes of reviewers. The work also shows that using the PoA-based consensus in the decision making process could reduce processing time up to 5 times compared to PoW algorithm, while the power consumption is negligible [154].

C. ARCHIVAL AND DIGITAL RIGHTS MANAGEMENT

After a virtual content is approved, its associated files must be stored in a specific database or IPFS for reservation and further usage. Different storage solutions could be adopted depending on the purpose of the creators and the type of digital assets. Two types of digital asset can be defined based on its usage and attributes as follows:

- **Unique digital assets:** This type of digital asset strongly emphasizes the uniqueness and ownership of the asset. A digital asset is valuable due to the fact that it is unique, owned by the right owner, and other similar products in the market, if any, are all illegal copies. NFT is an efficient technique to manage this type of digital asset.
- **Access-based digital assets:** Uniqueness is not an important factor for this type of digital asset. Instead, these digital assets could be accessed by multiple users who have registered or purchased license through a digital rights management (DRM) system [155].

For access-based digital assets, storing source files in centralized databases such as cloud storage is a suitable solution, since it is convenient to access the files and easy to enforce access-control policies. A typical digital rights management system for this type of asset is presented in [156] (Fig. 14). In this scheme, digital assets are protected and distributed by third-party authorities with an associated license. Therefore, the traditional system is prone to SPOF and third-party risks. To solve these issues, blockchain technology can be used to provide a decentralized environment for the authorization

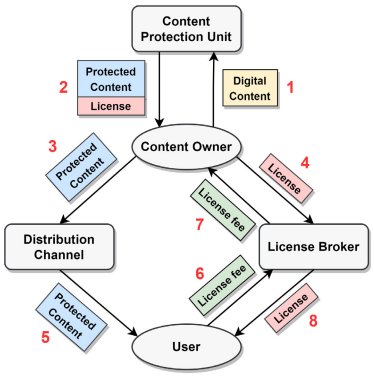

FIGURE 14. A typical digital rights management system [156].

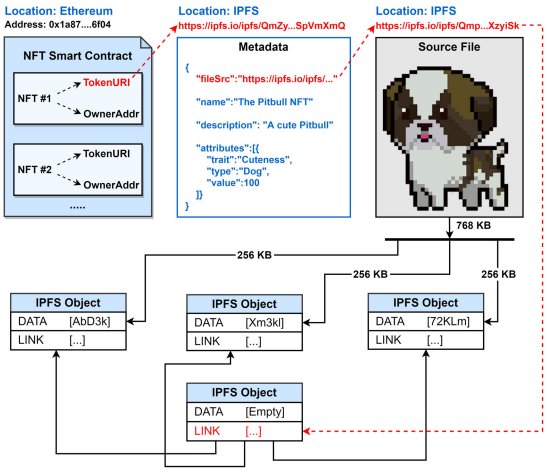

FIGURE 15. Tokenize digital assets to NFTs and store on IPFS.

process and access management. Zhu et al. [157] propose a distributed permissioned system using blockchain and Attribute-based Access Control (ABAC) model for digital asset access control. In this framework, a customer must initialize a multi-signature blockchain transaction, then collect four signatures from different ABAC-based components to request access of digital assets. In comparison with the traditional DRM model, this system is more automatic and decentralized thanks to blockchain, while it is more flexible thanks to the ABAC model.

For unique digital assets, tokenizing them into NFTs is an ideal option compared to other traditional techniques such as watermarking or fingerprinting. In addition, storing NFT data using decentralized file storage techniques like IPFS is a suitable solution which not only ensures the permanence of data, but also protects data from unintended modification.

To tokenize digital assets into NFTs using IPFS, the source files of the asset are first split up and stored in multiple IPFS objects (Fig. 15). Each IPFS object contains up to 256 KB data and a unique link and they will be stored by different nodes in the network. There is also an additional empty object that links all other objects, forming a single link of the source file. Then, a metadata file is created and stored in IPFS, containing necessary information about the digital asset such as name, description, attributes, and the source file's link.

D. DIGITAL ASSET VALUATION

After digital right management, digital assets are then ready to be distributed in the market for trading. Another important stage in the magenagement workflow is digital asset valuation. According to the IEEE Standard for blockchain-based digital asset management [158], the valuation of a digital asset depends on the following factors:

- **Future revenue:** This is the potential revenue that a digital asset could generate and it is marked as positive cash flow.
- **Future expenses:** The operation cost that a digital asset could consume. It is marked as negative cash flow.
- **Price fluctuation:** When a digital asset is distributed into the marketplace, its price would increase/decrease based on its platform and the market.

For digital asset valuation, blockchain could help in recording the measurement of properties for digital assets [158]. For further usage, if the amortization of a digital asset has been tested carefully and the owner has a valuation model, the re-measurement of value could be done automatically by smart contracts [158]. On the one hand, this eliminates the role of centralized third parties, thus optimizing the profit of these platforms and countering human errors. On the other hand, smart contract code is fixed on the blockchain so the pricing model cannot be changed. When users want to adopt a new pricing model, another smart contract must be constructed, resulting in additional fee and lack of flexibility.

E. DIGITAL ASSET DISTRIBUTION

The final stage in the metaverse digital asset management workflow is to distribute digital assets to metaverse users. Different types of assets should be distributed in different channels based on their attributes.

For access-based digital assets, blockchain technology could make the distribution process more decentralized by eliminating third-party entity. Specifically, smart contracts take responsibility for controlling the payment process and granting customers keys or licenses to access digital products. For instance, the authors in [159] present a blockchain-based system utilizing smart contracts to distribute digital images in a permissioned network. In this design, every watermarked image is stored in cloud storage, while its hash is committed to a scalable blockchain through transactions. Whenever a customer wants to access an image, she sends a request to an administrator smart contract through a payment transaction. After receiving payment, the smart contract sends the session key to the customer, allowing her to download the image from the cloud storage. If the image has been modified in the cloud storage, the customer can report the mismatch of the image's hash to the smart contract to receive her fund back.

For unique digital assets tokenized as NFTs, they can be distributed on NFT marketplaces to take advantage of

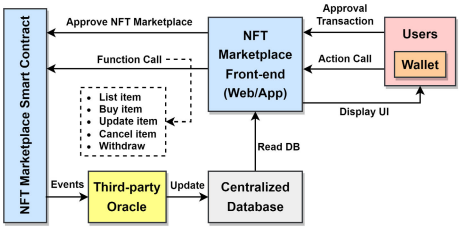

FIGURE 16. Structure and operation of a typical NFT marketplace.

the decentralized property. The structure and operation of a typical NFT marketplace is presented in Fig. 16.

Since blockchain storage does not have query methods, the dApp still needs a centralized database such as MongoDB to update every change of the smart contract in real time. When a user wants to take actions such as listing an NFT for sale, she must approve the NFT marketplace smart contract through an approval transaction, so that the smart contract is allowed to transfer specific NFTs on behalf of the owner. Through the front-end, she then calls the ''list item'' function of the ERC-721 smart contract with the address of the smart contract, the NFT's token ID, and a desired price for her NFT. After a new NFT is listed, the marketplace smart contract emits an event, which is then listened by a third-party oracle so that the new item is updated to the database. Other actions such as buying items, updating price, canceling items, or withdrawing funds also follow the above process.

VIII. OPEN CHALLENGES

There are many challenges to the development of the metaverse that must be addressed in the coming years. While research challenges and issues come from different backbone technologies of the metaverse, we mainly discuss the ones which related to blockchain technology, from both technical and social angles.

A. SOCIAL CONCERNS

The potentials of the blockchain-enabled metaverse have been exploited thoroughly in the study. Nevertheless, addressing persistent social challenges is crucial for enhancing societal acceptance of the metaverse. Initially, the absence of proper national and international regulations may result in severe fraud, crime, and misinformation within the virtual realm. Several solutions have been figured out to prevent certain cryptocurrency-related scams [160], in which blockchain transactions and smart contract bytecodes are analyzed to detect scams. However, existing solutions primarily focus on mitigating phishing scams, while countering other forms of scams and crimes, such as money laundering, remains untapped. Additionally, some studies aim to address the dissemination of false information on social media through blockchain [161], [162], but the metaverse encompasses a wider range and malicious actors can easily spread disinformation through interactions between avatars.

Besides, the blockchain-metaverse alliance can pose a significant risk to the environment due to its high energy consumption needs. Some studies concentrate on improving the energy efficiency of blockchain's consensus mechanism [163], while some others investigate using the computational resources of the PoW process for meaningful purposes such as deep learning and federated learning [164]. However, this could result in security trade-offs due to the blockchain trilemma. Thus, further research is needed to address the social implications of the blockchain-empowered metaverse.

B. VIRTUAL ASSET VALUATION

There have been various extremely valuable virtual contents issued and traded in the market. *The Merge*, an NFT artwork created by the digital artist Pak, has been sold for $91.8 million on Nifty Gateway [165]. That is also the most expensive NFT ever sold, with 28,983 collectors pitched together to purchase 312,686 parts of this NFT.

However, it is still vague in evaluating virtual assets. There are already several NFT scams that raise the price of worthless NFTs to very high values. In particular, organizations issuing those NFT projects often associate themselves with some existing successful projects, or they create the artificially drive up demand by buying their owns NFTs with high prices through different accounts created by themselves.

When it comes to the metaverse, some traditional valuation methods such as the DCF model and the Market approach in the financial sector could be deployed as presented in Section VII-D, but they all have their own weaknesses. While the NVT Ratio in the Market approach could not predict a bubble before it happens, the DCF model requires too many assumptions in cash flow projection, thus being prone to errors. The efficiency and accuracy of such methods have not been verified concretely, thus virtual asset valuation in the metaverse is still an open issue and further research must be conducted to develop more suitable solutions.

C. CROSS-CHAIN VULNERABILITY

We have learned that cross-chain mechanisms enable metaverse interoperability, allowing a global virtual environment where users could send assets, messages, and data across platforms. However, transferring virtual assets between blockchains is actually not that simple. The operation of cross-chain communication has been described in section III-D. This mechanism raises two serious problems:

- **Centralization:** The intervention of the third-party operator eliminates the desirable decentralized property. The cross-chain bridge is usually more centralized than the blockchains to which it connects. Therefore, attacking a cross-chain bridge is usually easier than attacking the blockchains themselves.
- **Put all eggs in one basket:** Since all users must deposit their tokens to a smart contract account, the smart contract contains a huge amount of money from different sources and becomes vulnerable to attacks. In other

words, attacking a cross-chain bridge is usually more lucrative than directly attacking the blockchains.

Many recent attacks have proven the vulnerability of current cross-chain mechanisms. Poly Network, a cross-chain interoperability protocol for Ethereum, Binance Smart Chain, and Polygon, have been hacked in 2021. The attacker has stolen $610 million within just 1 hour [166], making it one of the most severe attacks in the cryptocurrency space. Similarly, the vulnerability in centralization of Ronin Network, a bridge between Axie Infinity and Ethereum, has been exploited, and $650 million has been stolen by attackers [167]. This would pose a threat to the economic system of the metaverse and impact social acceptance of such platforms.

D. FINANCIAL RISKS IN MetaFi

MetaFi has been introduced in Section IV-C with a variety of financial services provided to metaverse users. However, the lack of central authorities could raise serious financial risks in certain circumstances. In traditional banking systems, our deposits in central banks are often guaranteed by the government or its associated insurance corporations. On the other hand, in a virtual and decentralized environment, almost no similar insurances are available to protect customers from financial risks.

Besides, volatility is a critical problem of using cryptocurrency as a payment method in the metaverse. Although stablecoins have been introduced as a solution for volatility, there are still many issues with this technology. Stablecoins are cryptocurrencies whose market values are pegged to external reference such as fiat currencies, cryptocurrency or other real assets such as gold or real estate. In fact, the collapse of various algorithmic stablecoins has partly proved its vulnerability. The crash of Terra project with the stablecoin UST led to the loss of about $60 billion in the ecosystem's market capitalization [168], raising a warning for stablecoins which are not fully backed by reliable assets. A critical issue is how to prove that the organization proposing a stablecoin is reserving enough real assets as collateral for their stablecoin. In this case, the problem is back to the trust between users and service providers, although trustless characteristic is one of the most well-known properties of cryptocurrency.

E. BLOCKCHAIN SCALABILITY AND COST

The cryptocurrency system deployed in the Metaverse must be as fast as possible to deal with the high demand of the market. However, cryptocurrency and blockchain face the scalability problem [169]. In a traditional centralized system, user transactions and information are submitted to a centralized server and all clients are implied to trust the server. Therefore, the process is simple and fast. In contrast, transactions in a decentralized network are spread throughout the trustless system, thus complex mechanisms are needed to reach the consensus among nodes.

To solve the scalability issue, we can use committee-based consensus algorithm with a small group of validators responsible for validating transactions. However, this means that certain degree of decentralization must be sacrificed. If this trend continues, the blockchain-based metaverse would eventually evolve towards a centralized environment, thus eliminating the benefits of using blockchain over traditional financial systems. Another solution is to use layer-2 networks such as *channel*, *plasma*, and *rollups* built on top of the main chain which is used for the metaverse economic system. Nevertheless, they add more complexity to the metaverse currency system, while each of them still has its own limitations. For example, a channel only allows interaction between two nodes, whereas plasma has an extremely high confirmation time, around several days or even a week. Therefore, to be applicable for the metaverse, the scalability of blockchain technology should be improved further.

F. THE EVER-GROWING LEDGER

Even if various proper mechanisms are deployed to improve blockchain scalability and transaction rate in the metaverse, one still needs to develop efficient techniques to store this endlessly long history of transactions. With the huge number of daily transactions submitted in the metaverse, the number of nodes who can afford this large amount of data would decrease over time. This issue comes from two technical properties of blockchains:

- Blockchain is immutable, meaning that its transaction history cannot be changed so it just grows up and becomes larger over time.
- Blockchains are decentralised. Only those who keep the full history of the ledger can validate transactions.

Several studies have attempted to propose methods to prune old data from blockchain [170], [171]. However, this eliminates the immutable characteristic of blockchain. As blockchain is used in the metaverse not only for payments, but also for storing data and digital assets, immutability is indeed important. Hence, further inventions are needed to tackle this issue to maintain the stability and prevent potential risks related to decentralization and security in the metaverse economic system.

IX. CONCLUSION

In this paper, we presented a comprehensive and in-depth survey of the blockchain-enabled metaverse. Thorough the study, the potentials blockchain has been shown in various use cases of the metaverse, ranging from user application, system perspective, to security and privacy enabler of the metaverse infrastructure. Also, blockchain is often combined with other technology such as IoT and AI to offer further advance applications. That is to say, the integration of blockchain into the metaverse is crucial to ensure the decentralization, security, and privacy of this virtual world. However, several issues with blockchain technology have also been identified, indicating a need for further improvement before it can be fully applied in the metaverse. We expect that our paper can provide metaverse researchers and developers a clear vision

of the blockchain-empowered metaverse, thus facilitating further research in this burgeoning area.

For future research, the idea of a multiple-metaverse architecture based on blockchain interoperability could be developed further. To this end, all sub-metaverses should follow a common design standard to be applicable with each other. Finally, all current metaverse platforms would eventually connect together to form a global virtual world, in which each of them offers different sets of virtual services. Moreover, further innovations are required to develop suitable and efficient blockchain-based solutions enabling various metaverse infrastructure functions and applications in order to realize the full-flesh metaverse in the coming years.

REFERENCES

[1] J. Joshua, "Information bodies: Computational anxiety in Neal Stephenson's snow crash," *Interdiscipl. Literary Stud.*, vol. 19, no. 1, pp. 17–47, Mar. 2017, doi: 10.5325/intelitestud.19.1.0017.

[2] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 319–352, 1st Quart., 2023, doi: 10.1109/COMST.2022.3202047.

[3] M. Xu, W. C. Ng, W. Y. B. Lim, J. Kang, Z. Xiong, D. Niyato, Q. Yang, X. Shen, and C. Miao, "A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 656–700, 1st Quart., 2023, doi: 10.1109/COMST.2022.3221119.

[4] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, "Fusing blockchain and AI with metaverse: A survey," *IEEE Open J. Comput. Soc.*, vol. 3, pp. 122–136, 2022, doi: 10.1109/OJCS.2022.3188249.

[5] L. L. Locurcio, "Dental education in the metaverse," *Brit. Dental J.*, vol. 232, no. 4, p. 191, Feb. 2022, doi: 10.1038/s41415-022-3990-7.

[6] 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.

[7] S. Bardzell and K. Shankar, "Video game technologies and virtual design: A study of virtual design teams in a metaverse," in *Proc. Int. Conf. Virtual Reality*, 2007, pp. 607–616, doi: 10.1007/978-3-540-73335-5_65.

[8] H. Jeong, Y. Yi, and D. Kim, "An innovative e-commerce platform incorporating metaverse to live commerce," *Int. J. Innov. Comput., Inf. Control*, vol. 18, no. 1, pp. 221–229, Feb. 2022, doi: 10.24507/ijicic.18.01.221.

[9] S.-V. Rehm, L. Goel, and M. Crespi, "The metaverse as mediator between technology, trends, and the digital transformation of society and business," *J. For Virtual Worlds Res.*, vol. 8, no. 2, pp. 1–8, Oct. 2015, doi: 10.4101/jvwr.v8i2.7149.

[10] A. H. J. Kastrenakes. (2021). *Facebook is Spending at Least $10 Billion This Year on its Metaverse Division*. [Online]. Available: https://www.theverge.com/2021/10/25/22745381/facebook-reality-labs-10-billion-metaverse

[11] K. Rees. (2022). *These 8 Tech Giants Have Invested Big in the Metaverse*. [Online]. Available: https://www.makeuseof.com/companies-investing-in-metaverse/

[12] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019, doi: 10.1109/JIOT.2019.2920987.

[13] U. W. Chohan, "Non-fungible tokens: Blockchains, scarcity, and value," in *Proc. Crit. Blockchain Res. Initiative (CBRI) Work. Papers*, Mar. 2021, p. 14, doi: 10.2139/ssrn.3822743.

[14] S. Wang, W. Ding, J. Li, Y. Yuan, L. Ouyang, and F.-Y. Wang, "Decentralized autonomous organizations: Concept, model, and applications," *IEEE Trans. Computat. Social Syst.*, vol. 6, no. 5, pp. 870–878, Oct. 2019, doi: 10.1109/TCSS.2019.2938190.

[15] Y. Chen and C. Bellavitis, "Blockchain disruption and decentralized finance: The rise of decentralized business models," *J. Bus. Venturing Insights*, vol. 13, Jun. 2020, Art. no. e00151, doi: 10.1016/j.jbvi.2019.e00151.

[16] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. Leung, "Decentralized applications: The blockchain-empowered software system," *IEEE Access*, vol. 6, pp. 53019–53033, 2018, doi: 10.1109/ACCESS.2018.2870644.

[17] 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.

[18] H.-J. Jeon, H.-C. Youn, S.-M. Ko, and T.-H. Kim, "Blockchain and AI meet in the metaverse," in *Advances in the Convergence of Blockchain and Artificial Intelligence*. London, U.K.: IntechOpen, 2022, p. 73.

[19] M. A. Hisseine, D. Chen, and X. Yang, "The application of blockchain in social media: A systematic literature review," *Appl. Sci.*, vol. 12, no. 13, p. 6567, Jun. 2022, doi: 10.3390/app12136567.

[20] H. Duan, J. Li, S. Fan, Z. Lin, X. Wu, and W. Cai, "Metaverse for social good: A university campus prototype," in *Proc. 29th ACM Int. Conf. Multimedia*, Oct. 2021, pp. 153–161, doi: 10.1145/3474085.3479238.

[21] Y. K. Dwivedi et al., "Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," *Int. J. Inf. Manage.*, vol. 66, Oct. 2022, Art. no. 102542, doi: 10.1016/j.ijinfomgt.2022.102542.

[22] 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.

[23] V. Mayer-Schonberger and J. Crowley, "Napster's second life: The regulatory challenges of virtual worlds," *Northwestern Univ. Law Rev.*, vol. 100, no. 4, p. 1775, 2006.

[24] S. B. Far and A. I. Rad, "Applying digital twins in metaverse: User interface, security and privacy challenges," *J. Metaverse*, vol. 2, no. 1, pp. 8–16, Jun. 2022.

[25] L. V. Kiong, *Metaverse Made Easy: A Beginner's Guide to the Metaverse: Everything you need to know about Metaverse, NFT and GameFi*. 2022.

[26] J. Han, J. Yun, J. Jang, and K.-R. Park, "User-friendly home automation based on 3D virtual world," *IEEE Trans. Consum. Electron.*, vol. 56, no. 3, pp. 1843–1847, Aug. 2010, doi: 10.1109/TCE.2010.5606335.

[27] S. Mihai, M. Yaqoob, D. V. Hung, W. Davis, P. Towakel, M. Raza, M. Karamanoglu, B. Barn, D. Shetve, R. V. Prasad, H. Venkataraman, R. Trestian, and H. X. Nguyen, "Digital twins: A survey on enabling technologies, challenges, trends and future prospects," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2255–2291, 4th Quart., 2022, doi: 10.1109/COMST.2022.3208773.

[28] F. Tao, H. Zhang, A. Liu, and A. Y. Nee, "Digital twin in industry: State-of-the-art," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2405–2415, Apr. 2018, doi: 10.1109/TII.2018.2873186.

[29] A. Fuller, Z. Fan, C. Day, and C. Barlow, "Digital twin: Enabling technologies, challenges and open research," *IEEE Access*, vol. 8, pp. 108952–108971, 2020, doi: 10.1109/ACCESS.2020.2998358.

[30] S. Suhail, R. Hussain, R. Jurdak, and C. S. Hong, "Trustworthy digital twins in the industrial Internet of Things with blockchain," *IEEE Internet Comput.*, vol. 26, no. 3, pp. 58–67, May 2022, doi: 10.1109/MIC.2021.3059320.

[31] X. Niu and W. Feng, "Immersive entertainment environments—From theme parks to metaverse," in *Proc. Int. Conf. Hum.-Comput. Interact.*, 2022, pp. 392–403, doi: 10.1007/978-3-031-05463-1_27.

[32] S. Nakamoto. (2008). *Bitcoin Whitepaper*. [Online]. Available: https://bitcoin.org/bitcoin

[33] H. Liu, X. Luo, H. Liu, and X. Xia, "Merkle tree: A fundamental component of blockchains," in *Proc. Int. Conf. Electron. Inf. Eng. Comput. Sci. (EIECS)*, Sep. 2021, pp. 556–561, doi: 10.1109/EIECS53707.2021.9588047.

[34] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 1st Quart., 2020, doi: 10.1109/COMST.2020.2969706.

[35] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019, doi: 10.1109/ACCESS.2019.2896108.

[36] W. Zou, D. Lo, P. S. Kochhar, X.-B.-D. Le, X. Xia, Y. Feng, Z. Chen, and B. Xu, "Smart contract development: Challenges and opportunities," *IEEE Trans. Softw. Eng.*, vol. 47, no. 10, pp. 2084–2106, Oct. 2021, doi: 10.1109/TSE.2019.2942301.

[37] T. Górski, "The $k + 1$ symmetric test pattern for smart contracts," *Symmetry*, vol. 14, no. 8, p. 1686, Aug. 2022, doi: 10.3390/sym14081686.

[38] N. Sánchez-Gómez, J. Torres-Valderrama, J. A. García-García, J. J. Gutiérrez, and M. J. Escalona, "Model-based software design and testing in blockchain smart contracts: A systematic literature review," *IEEE Access*, vol. 8, pp. 164556–164569, 2020, doi: 10.1109/ACCESS.2020.3021502.

[39] S. Punathumkandi, V. M. Sundaram, and P. Panneer, "Interoperable permissioned-blockchain with sustainable performance," *Sustainability*, vol. 13, no. 20, p. 11132, Oct. 2021, doi: 10.3390/su132011132.

[40] H. Tam Vo, Z. Wang, D. Karunamoorthy, J. Wagner, E. Abebe, and M. Mohania, "Internet of Blockchains: Techniques and challenges ahead," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1574–1581, doi: 10.1109/Cybermatics_2018.2018.00264.

[41] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," White Paper, 2016, vol. 21, pp. 2327–4662.

[42] J. Kwon and E. Buchman, "Cosmos whitepaper," Netw. Distrib. Ledgers, White Paper, Dec. 2020, pp. 1–32.

[43] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1977–2008, 3rd Quart., 2020, doi: 10.1109/COMST.2020.2975999.

[44] M. H. U. Rehman, K. Salah, E. Damiani, and D. Svetinovic, "Trust in blockchain cryptocurrency ecosystem," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1196–1212, Nov. 2020, doi: 10.1109/TEM.2019.2948861.

[45] J. Chiu and T. V. Koeppl, "The economics of cryptocurrencies—Bitcoin and beyond," *Can. J. Econ.*, vol. 55, no. 4, pp. 1762–1798, Oct. 2022, doi: 10.2139/ssrn.3048124.

[46] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, Jul. 2018, doi: 10.1145/3212998.

[47] M. Saad, L. Njilla, C. Kamhoua, and A. Mohaisen, "Countering selfish mining in blockchains," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2019, pp. 360–364, doi: 10.1109/ICCNC.2019.8685577.

[48] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research perspectives and challenges for bitcoin and cryptocurrencies," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 104–121, doi: 10.1109/SP.2015.14.

[49] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from Bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 397–411, doi: 10.1109/SP.2013.34.

[50] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 254–269, doi: 10.1145/2976749.2978309.

[51] S. McBride. (2020). *Welcome to the 'metaverse'*. [Online]. Available: https://www.forbes.com/sites/stephenmcbride1/2021/03/23/welcome-to-the-metaverse

[52] A. Manzoor, M. Samarin, D. Mason, and M. Ylianttila, "Scavenger hunt: Utilization of blockchain and IoT for a location-based game," *IEEE Access*, vol. 8, pp. 204863–204879, 2020, doi: 10.1109/ACCESS.2020.3037182.

[53] M. Du, Q. Chen, L. Liu, and X. Ma, "A blockchain-based random number generation algorithm and the application in blockchain games," in *Proc. IEEE Int. Conf. Syst., Man Cybern. (SMC)*, Oct. 2019, pp. 3498–3503, doi: 10.1109/SMC.2019.8914618.

[54] S.-C. Cha, W.-C. Peng, T.-Y. Hsu, C.-L. Chang, and S.-W. Li, "A blockchain-based privacy preserving ticketing service," in *Proc. IEEE 7th Global Conf. Consum. Electron. (GCCE)*, Oct. 2018, pp. 585–587, doi: 10.1109/GCCE.2018.8574479.

[55] X. Zeng, N. Hao, J. Zheng, and X. Xu, "A consortium blockchain paradigm on hyperledger-based peer-to-peer lending system," *China Commun.*, vol. 16, no. 8, pp. 38–50, Aug. 2019, doi: 10.23919/JCC.2019.08.004.

[56] V. Hassija, G. Bansal, V. Chamola, N. Kumar, and M. Guizani, "Secure lending: Blockchain and prospect theory-based decentralized credit scoring model," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 2566–2575, Oct. 2020, doi: 10.1109/TNSE.2020.2982488.

[57] H. Al-Shaibani, N. Lasla, and M. Abdallah, "Consortium blockchain-based decentralized stock exchange platform," *IEEE Access*, vol. 8, pp. 123711–123725, 2020, doi: 10.1109/ACCESS.2020.3005663.

[58] T. Lepoint, G. Ciocarlie, and K. Eldefrawy, "BlockCIS—A blockchain-based cyber insurance system," in *Proc. IEEE Int. Conf. Cloud Eng. (IC2E)*, Apr. 2018, pp. 378–384, doi: 10.1109/IC2E.2018.00072.

[59] P. P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-based healthcare: Background, consensus, platforms, and use cases," *IEEE Syst. J.*, vol. 15, no. 1, pp. 85–94, Mar. 2021, doi: 10.1109/JSYST.2020.2963840.

[60] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.

[61] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, "A blockchain-based medical data sharing and protection scheme," *IEEE Access*, vol. 7, pp. 118943–118953, 2019, doi: 10.1109/ACCESS.2019.2937685.

[62] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018, doi: 10.1109/ACCESS.2018.2789929.

[63] M. A. Rahman, M. S. Abuludin, L. X. Yuan, M. S. Islam, and A. T. Asyhari, "EduChain: CIA-compliant blockchain for intelligent cyber defense of microservices in education industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 1930–1938, Mar. 2022, doi: 10.1109/TII.2021.3093475.

[64] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1008–1027, Nov. 2020, doi: 10.1109/TEM.2019.2926471.

[65] S. S. Panda, D. Jena, B. K. Mohanta, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Authentication and key management in distributed IoT using blockchain technology," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12947–12954, Aug. 2021, doi: 10.1109/JIOT.2021.3063806.

[66] M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, and M. Guizani, "Blockchain-assisted secure device authentication for cross-domain industrial IoT," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 5, pp. 942–954, May 2020, doi: 10.1109/JSAC.2020.2980916.

[67] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K.-R. Choo, "Blockchain-based cross-domain authentication for intelligent 5G-enabled Internet of Drones," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6224–6238, Apr. 2022, doi: 10.1109/JIOT.2021.3113321.

[68] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K.-K.-R. Choo, "HomeChain: A blockchain-based secure mutual authentication system for smart homes," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 818–829, Feb. 2020, doi: 10.1109/JIOT.2019.2944400.

[69] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4146–4155, Jun. 2020, doi: 10.1109/TII.2019.2948053.

[70] E. Maler and D. Reed, "The venn of identity: Options and issues in federated identity management," *IEEE Secur. Privacy*, vol. 6, no. 2, pp. 16–23, Mar./Apr. 2008, doi: 10.1109/MSP.2008.50.

[71] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In search of self-sovereign identity leveraging blockchain technology," *IEEE Access*, vol. 7, pp. 103059–103079, 2019, doi: 10.1109/ACCESS.2019.2931173.

[72] Q. Stokkink and J. Pouwelse, "Deployment of a blockchain-based self-sovereign identity," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1336–1342, doi: 10.1109/Cybermatics_2018.2018.00230.

[73] P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A Sybil-resistant scalable blockchain," *Future Gener. Comput. Syst.*, vol. 107, pp. 770–780, Jun. 2020, doi: 10.1016/j.future.2017.08.048.

[74] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, Sep. 2018, doi: 10.1016/j.cose.2018.06.004.

[75] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Inf. Process. Manage.*, vol. 58, no. 2, Mar. 2021, Art. no. 102468, doi: 10.1016/j.ipm.2020.102468.

[76] F. Cirillo, G. Solmaz, E. L. Berz, M. Bauer, B. Cheng, and E. Kovacs, "A standard-based open source IoT platform: FIWARE," *IEEE Internet Things Mag.*, vol. 2, no. 3, pp. 12–18, Sep. 2019, doi: 10.1109/IOTM.0001.1800022.

[77] D. Hardt. (2012). *The OAuth 2.0 Authorization Framework*. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6749.txt
[78] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Trans. Serv. Comput.*, vol. 13, no. 2, pp. 241–251, Mar./Apr. 2020, doi: 10.1109/TSC.2020.2964537.
[79] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1972–1983, Mar. 2020, doi: 10.1109/TII.2019.2938001.
[80] J. Wang, L. Wu, K.-K.-R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1984–1992, Mar. 2020, doi: 10.1109/TII.2019.2936278.
[81] X. Jia, D. He, N. Kumar, and K.-K.-R. Choo, "A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing," *IEEE Syst. J.*, vol. 14, no. 1, pp. 560–571, Mar. 2020, doi: 10.1109/JSYST.2019.2896064.
[82] Y. Bai, Q. Hu, S.-H. Seo, K. Kang, and J. J. Lee, "Public participation consortium blockchain for smart city governance," *IEEE Internet Things J.*, vol. 9, no. 3, pp. 2094–2108, Feb. 2022, doi: 10.1109/JIOT.2021.3091151.
[83] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019, doi: 10.1109/ACCESS.2019.2895670.
[84] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2017, pp. 357–375, doi: 10.1007/978-3-319-70972-7_20.
[85] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Future Gener. Comput. Syst.*, vol. 105, pp. 13–26, Apr. 2020, doi: 10.1016/j.future.2019.11.005.
[86] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—Review and open research challenges," *Sensors*, vol. 21, no. 17, p. 5874, Aug. 2021, doi: 10.3390/s21175874.
[87] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020, doi: 10.1109/ACCESS.2020.2968985.
[88] S. Gao, D. Zheng, R. Guo, C. Jing, and C. Hu, "An anti-quantum E-voting protocol in blockchain with audit function," *IEEE Access*, vol. 7, pp. 115304–115316, 2019, doi: 10.1109/ACCESS.2019.2935895.
[89] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-based E-voting system," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2018, pp. 983–986, doi: 10.1109/CLOUD.2018.00151.
[90] R. Dennis and G. Owen, "Rep on the block: A next generation reputation system based on the blockchain," in *Proc. 10th Int. Conf. for Internet Technol. Secured Trans. (ICITST)*, Dec. 2015, pp. 131–138, doi: 10.1109/ICITST.2015.7412073.
[91] T. Wang, J. Guo, S. Ai, and J. Cao, "RBT: A distributed reputation system for blockchain-based peer-to-peer energy trading with fairness consideration," *Appl. Energy*, vol. 295, Aug. 2021, Art. no. 117056, doi: 10.1016/j.apenergy.2021.117056.
[92] S. Khezr, A. Yassine, R. Benlamri, and M. S. Hossain, "An edge intelligent blockchain-based reputation system for IIoT data ecosystem," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 8346–8355, Nov. 2022, doi: 10.1109/TII.2022.3174065.
[93] Y. Liu, Z. Xiong, Q. Hu, D. Niyato, J. Zhang, C. Miao, C. Leung, and Z. Tian, "VRepChain: A decentralized and privacy-preserving reputation system for social Internet of Vehicles based on blockchain," *IEEE Trans. Veh. Technol.*, vol. 71, no. 12, pp. 13242–13253, Dec. 2022, doi: 10.1109/TVT.2022.3198004.
[94] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A trustless privacy-preserving reputation system," in *Proc. IFIP Int. Conf. ICT Syst. Secur. Privacy Protection*, 2016, pp. 398–411, doi: 10.1007/978-3-319-33630-5_27.
[95] Y. Yu, S. Liu, L. Guo, P. L. Yeoh, B. Vucetic, and Y. Li, "CrowdR-FBC: A distributed fog-blockchains for mobile crowdsourcing reputation management," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8722–8735, Sep. 2020, doi: 10.1109/JIOT.2020.2996229.
[96] D. Liu, A. Alahmadi, J. Ni, X. Lin, and X. Shen, "Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3527–3537, Jun. 2019, doi: 10.1109/TII.2019.2898900.
[97] B. Bunz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 315–334, doi: 10.1109/SP.2018.00020.
[98] M. Li, L. Zhu, Z. Zhang, C. Lal, M. Conti, and M. Alazab, "Anonymous and verifiable reputation system for E-Commerce platforms based on blockchain," *IEEE Trans. Netw. Serv. Manage.*, vol. 18, no. 4, pp. 4434–4449, Dec. 2021, doi: 10.1109/TNSM.2021.3098439.
[99] Z. Xiong, Y. Zhang, N. C. Luong, D. Niyato, P. Wang, and N. Guizani, "The best of both worlds: A general architecture for data management in blockchain-enabled Internet-of-Things," *IEEE Netw.*, vol. 34, no. 1, pp. 166–173, Jan. 2020, doi: 10.1109/MNET.001.1900095.
[100] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan./Feb. 2018, doi: 10.1109/MCC.2018.011791712.
[101] M. Zhaofeng, W. Xiaochang, D. K. Jain, H. Khan, G. Hongmin, and W. Zhen, "A blockchain-based trusted data management scheme in edge computing," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2013–2021, Mar. 2020, doi: 10.1109/TII.2019.2933482.
[102] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a service," *IEEE Trans. Serv. Comput.*, vol. 13, no. 2, pp. 289–300, Mar./Apr. 2020, doi: 10.1109/TSC.2019.2953033.
[103] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019, doi: 10.1109/COMST.2018.2886932.
[104] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, "Blockchain for large-scale Internet of Things data storage and protection," *IEEE Trans. Serv. Comput.*, vol. 12, no. 5, pp. 762–771, Sep. 2019, doi: 10.1109/TSC.2018.2853167.
[105] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain meets cloud computing: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 2009–2030, 3rd Quart., 2020, doi: 10.1109/COMST.2020.2989392.
[106] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jun. 2017, pp. 468–475, doi: 10.1109/ICWS.2017.54.
[107] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2018, doi: 10.1109/JIOT.2018.2875542.
[108] W. Liang, Y. Fan, K.-C. Li, D. Zhang, and J.-L. Gaudiot, "Secure data storage and recovery in industrial blockchain network environments," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6543–6552, Oct. 2020, doi: 10.1109/TII.2020.2966069.
[109] K. V. Rashmi, N. B. Shah, K. Ramchandran, and P. V. Kumar, "Regenerating codes for errors and erasures in distributed storage," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2012, pp. 1202–1206, doi: 10.1109/ISIT.2012.6283046.
[110] T. Hardjono, A. Lipton, and A. Pentland, "Toward an interoperability architecture for blockchain autonomous systems," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1298–1309, Nov. 2020, doi: 10.1109/TEM.2019.2920154.
[111] Trusted Computing Group. (2003). *TPM 2.0 Specification*. [Online]. Available: https://trustedcomputinggroup.org/resource/tpm-library-specification/
[112] F. McKeen, I. Alexandrovich, A. Berenzon, C. V. Rozas, H. Shafi, V. Shanbhogue, and U. R. Savagaonkar, "Innovative instructions and software model for isolated execution," in *Proc. HASP@ ISCA*, Jun. 2013, vol. 10, no. 1, pp. 1–8.
[113] R. Belchior, A. Vasconcelos, M. Correia, and T. Hardjono, "HERMES: Fault-tolerant middleware for blockchain interoperability," *Future Gener. Comput. Syst.*, vol. 129, pp. 236–251, Apr. 2022, doi: 10.1016/j.future.2021.11.004.
[114] M. Hargreaves. (2021). *Open Digital Asset Protocol*. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-hargreaves-odap-02
[115] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4682–4696, Jun. 2020, doi: 10.1109/JIOT.2020.2969326.

[116] B. Falchuk, S. Loeb, and R. Neff, "The social metaverse: Battle for privacy," *IEEE Technol. Soc. Mag.*, vol. 37, no. 2, pp. 52–61, Jun. 2018, doi: 10.1109/MTS.2018.2826060.

[117] G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez, and A. Ribagorda, "Evolution, detection and analysis of malware for smart devices," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 961–987, 2nd Quart., 2014, doi: 10.1109/SURV.2013.101613.00077.

[118] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 446–471, 1st Quart., 2013, doi: 10.1109/SURV.2012.013012.00028.

[119] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment," *J. Supercomput.*, vol. 73, no. 3, pp. 1152–1167, Sep. 2017, doi: 10.1007/s11227-016-1870-0.

[120] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 4, pp. 586–602, Oct./Dec. 2017, doi: 10.1109/TETC.2016.2606384.

[121] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, "Network intrusion detection," *IEEE Netw.*, vol. 8, no. 3, pp. 26–41, May/Jun. 1994, doi: 10.1109/65.283931.

[122] J. R. Douceur, "The Sybil attack," in *Peer-to-Peer Systems*. Berlin, Germany: Springer, Oct. 2002, pp. 251–260.

[123] J. Yang, S. He, Y. Xu, L. Chen, and J. Ren, "A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks," *Sensors*, vol. 19, no. 4, p. 970, Feb. 2019, doi: 10.3390/s19040970.

[124] B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, "Designing blockchain-based access control protocol in IoT-enabled smart-grid system," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5744–5761, Apr. 2021, doi: 10.1109/JIOT.2020.3030308.

[125] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019, doi: 10.1109/COMST.2019.2894727.

[126] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-chain: A blockchain-based framework for security and privacy-assured Internet of Medical Things with effective access control," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11717–11731, Jul. 2021, doi: 10.1109/JIOT.2021.3058946.

[127] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019, doi: 10.1109/ACCESS.2019.2905846.

[128] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018, doi: 10.1109/JIOT.2018.2812239.

[129] E. Rescorla and N. Modadugu, "Datagram transport layer security version 1.2," Internet Eng. Task Force (IETF), USA, Tech. Rep. RFC 6347, Tech. Rep., 2012. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6347.html

[130] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack, "Uncover security design flaws using the stride approach," *MSDN Mag.*, vol. 15, no. 11, pp. 68–75, 2006.

[131] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium blockchain-based malware detection in mobile devices," *IEEE Access*, vol. 6, pp. 12118–12128, 2018, doi: 10.1109/ACCESS.2018.2805783.

[132] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2671–2701, 1st Quart., 2019, doi: 10.1109/COMST.2019.2896380.

[133] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K.-R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9463–9472, Jun. 2021, doi: 10.1109/JIOT.2020.2996590.

[134] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Nov. 2015, pp. 1–6, doi: 10.1109/MilCIS.2015.7348942.

[135] M. M. Arifeen, A. Al Mamun, T. Ahmed, M. S. Kaiser, and M. Mahmud, "A blockchain-based scheme for Sybil attack detection in underwater wireless sensor networks," in *Proc. Int. Conf. Trends Comput. Cogn. Eng. (TCCE)*, 2021, pp. 467–476.

[136] S. Badruddoja, R. Dantu, Y. He, M. Thompson, A. Salau, and K. Upadhyay, "Trusted AI with blockchain to empower metaverse," in *Proc. 4th Int. Conf. Blockchain Comput. Appl. (BCCA)*, Sep. 2022, pp. 237–244, doi: 10.1109/BCCA55292.2022.9922027.

[137] Y. Zhan, P. Li, Z. Qu, D. Zeng, and S. Guo, "A learning-based incentive mechanism for federated learning," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6360–6368, Jul. 2020, doi: 10.1109/JIOT.2020.2967772.

[138] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4298–4311, Apr. 2020, doi: 10.1109/TVT.2020.2973651.

[139] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10700–10714, Dec. 2019, doi: 10.1109/JIOT.2019.2940820.

[140] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, "EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4719–4732, Jun. 2019, doi: 10.1109/JIOT.2018.2878154.

[141] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019, doi: 10.3390/s19020326.

[142] L. Malina, J. Hajny, P. Dzurenda, and S. Ricci, "Lightweight ring signatures for decentralized privacy-preserving transactions," in *Proc. ICETE*, 2018, pp. 692–697.

[143] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "FairAccess: A new blockchain-based access control framework for the Internet of Things," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5943–5964, Feb. 2016, doi: 10.1002/sec.1748.

[144] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017, doi: 10.1109/MCOM.2017.1700879.

[145] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K.-R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1120–1132, Apr. 2021, doi: 10.1109/TNSE.2019.2937481.

[146] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011, doi: 10.1109/MWC.2011.5751298.

[147] A. S. Khan, Y. Rahulamathavan, B. Basutli, G. Zheng, B. Assadhan, and S. Lambotharan, "Blockchain-based distributive auction for relay-assisted secure communications," *IEEE Access*, vol. 7, pp. 95555–95568, 2019, doi: 10.1109/ACCESS.2019.2929136.

[148] J. Kang, D. Ye, J. Nie, J. Xiao, X. Deng, S. Wang, Z. Xiong, R. Yu, and D. Niyato, "Blockchain-based federated learning for industrial metaverses: Incentive scheme with optimal AoI," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Aug. 2022, pp. 71–78, doi: 10.1109/Blockchain55522.2022.00020.

[149] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "DeepChain: Auditable and privacy-preserving deep learning with blockchain-based incentive," *IEEE Trans. Depend. Sec. Comput.*, vol. 18, no. 5, pp. 2438–2455, Sep./Oct. 2019, doi: 10.1109/TDSC.2019.2952332.

[150] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID)*, May 2017, pp. 468–477, doi: 10.1109/CCGRID.2017.8.

[151] S. Koul, S. Singh, and R. Verma, "Decentralised content creation in digital learning: A blockchain concept," in *ICT With Intelligent Applications*. Berlin, Germany: Springer, 2022, pp. 583–591, doi: 10.1007/978-981-16-4177-0_57.

[152] H. Hasan and K. Salah, "Combating deepfake videos using blockchain and smart contracts," *IEEE Access*, vol. 7, pp. 41596–41606, 2019, doi: 10.1109/ACCESS.2019.2905689.

[153] Q. Chen, G. Srivastava, R. M. Parizi, M. Aloqaily, and I. A. Ridhawi, "An incentive-aware blockchain-based solution for Internet of Fake Media Things," *Inf. Process. Manage.*, vol. 57, no. 6, Nov. 2020, Art. no. 102370, doi: 10.1016/j.ipm.2020.102370.

[154] M. A. Manolache, S. Manolache, and N. Tapus, "Decision making using the blockchain proof of authority consensus," *Proc. Comput. Sci.*, vol. 199, pp. 580–588, Jan. 2022, doi: 10.1016/j.procs.2022.01.071.

[155] S. R. Subramanya and B. K. Yi, "Digital rights management," *IEEE Potentials*, vol. 25, no. 2, pp. 31–34, Mar./Apr. 2006, doi: 10.1109/MP.2006.1649008.

[156] W. Ku and C.-H. Chi, "Survey on the technological aspects of digital rights management," in *Proc. Int. Conf. Inf. Secur.*, 2004, pp. 391–403, doi: 10.1007/978-3-540-30144-8_33.
[157] Y. Zhu, Y. Qin, Z. Zhou, X. Song, G. Liu, and W. C.-C. Chu, "Digital asset management with distributed permission over blockchain and attribute-based access control," in *Proc. IEEE Int. Conf. Services Comput. (SCC)*, Jul. 2018, pp. 193–200, doi: 10.1109/SCC.2018.00032.
[158] *IEEE Standard for Blockchain-based Digital Asset Management*, IEEE Standard 2418.10-2022, Blockchain Standards Committee, IEEE Consumer Technology Society, Mar. 2022.
[159] A. Garba, A. D. Dwivedi, M. Kamal, G. Srivastava, M. Tariq, M. A. Hasan, and Z. Chen, "A digital rights management system based on a scalable blockchain," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2665–2680, Sep. 2021, doi: 10.1007/s12083-020-01023-z.
[160] P. N. Sureshbhai, P. Bhattacharya, and S. Tanwar, "KaRuNa: A blockchain-based sentiment analysis framework for fraud cryptocurrency schemes," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6, doi: 10.1109/ICCWorkshops49005.2020.9145151.
[161] S. Paul, J. I. Joy, S. Sarker, A.-A.-H. Shakib, S. Ahmed, and A. K. Das, "Fake news detection in social media using blockchain," in *Proc. 7th Int. Conf. Smart Comput. Commun. (ICSCC)*, Jun. 2019, pp. 1–5, doi: 10.1109/ICSCC.2019.8843597.
[162] A. Qayyum, J. Qadir, M. U. Janjua, and F. Sher, "Using blockchain to rein in the new post-truth world and check the spread of fake news," *IT Prof.*, vol. 21, no. 4, pp. 16–24, Jul. 2019, doi: 10.1109/MITP.2019.2910503.
[163] N. Lasla, L. Al-Sahan, M. Abdallah, and M. Younis, "Green-PoW: An energy-efficient blockchain proof-of-work consensus algorithm," *Comput. Netw.*, vol. 214, Sep. 2022, Art. no. 109118, doi: 10.1016/j.comnet.2022.109118.
[164] X. Qu, S. Wang, Q. Hu, and X. Cheng, "Proof of federated learning: A novel energy-recycling consensus algorithm," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 8, pp. 2074–2085, Aug. 2021, doi: 10.1109/TPDS.2021.3056773.
[165] N. Hall. (2021). *The World's Most Expensive NFT Just Sold for $91 Million, But What Does it Mean?* [Online]. Available: https://manofmany.com/entertainment/art/pak-merge-nft-sale
[166] Wikipedia. (2021). *Poly Network Exploit*. [Online]. Available: https://en.wikipedia.org/wiki/Poly_Network_exploit
[167] B. Pimentel. (2022). *Hackers Stole Nearly $650 Million From the Axie Infinity NFT Game*. [Online]. Available: https://www.protocol.com/bulletins/axie-infinity-ronin-hack
[168] "Terra stablecoin crash casts spotlight on ecosystem," in *Expert Briefings*. Oxford, U.K.: Oxford Analytica, 2022, doi: 10.1108/OXAN-ES270251.
[169] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems," *IEEE Netw.*, vol. 33, no. 5, pp. 166–173, Sep. 2019, doi: 10.1109/MNET.001.1800290.
[170] M. Florian, S. Henningsen, S. Beaucamp, and B. Scheuermann, "Erasing data from blockchain nodes," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroSPW)*, Jun. 2019, pp. 367–376, doi: 10.1109/EuroSPW.2019.00047.
[171] V. Buterin. (2015). *State Tree Pruning*. [Online]. Available: https://blog.ethereum.org/2015/06/26/state-tree-pruning/

VU TUAN TRUONG received the B.Eng. degree in electrical and computer engineering from Hanoi University of Technology and Technology (HUST), Vietnam, in 2021. He is currently pursuing the M.Sc. degree with the Institut National de la Recherche Scientifique (INRS), University of Quebec, Montreal, QC, Canada. His research interests include blockchain and enabling technologies for metaverse.

LONG BAO LE (Senior Member, IEEE) received the B.Eng. degree in electrical engineering from Ho Chi Minh City University of Technology, Vietnam, in 1999, the M.Eng. degree in telecommunications from Asian Institute of Technology, Thailand, in 2002, and the Ph.D. degree in electrical engineering from the University of Manitoba, Canada, in 2007. He was a Postdoctoral Researcher with Massachusetts Institute of Technology, from 2008 to 2010, and the University of Waterloo, from 2007 to 2008. Since 2010, he has been with the Institut National de la Recherche Scientifique (INRS), University of Quebec, Montreal, QC, Canada, where he is currently a Full Professor. He is the coauthor of the books *Radio Resource Management in Multi-Tier Cellular Wireless Networks* (Wiley, 2013) and *Radio Resource Management in Wireless Networks: An Engineering Approach* (Cambridge University Press, 2017). His current research interests include smartgrids, radio resource management, network control and optimization, and emerging enabling technologies for 5G-and-beyond wireless systems and the metaverse. He was a member of the Editorial Boards of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and IEEE COMMUNICATIONS SURVEYS AND TUTORIALS. He is currently an Editor of IEEE TRANSACTIONS ON COMMUNICATIONS and IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING.

DUSIT NIYATO (Fellow, IEEE) received the B.Eng. degree from King Mongkuts Institute of Technology Ladkrabang (KMITL), Thailand, in 1999, and the Ph.D. degree in electrical and computer engineering from the University of Manitoba, Canada, in 2008. He is currently a Professor with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests include sustainability, edge intelligence, decentralized machine learning, and incentive mechanism designs.