Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Blockchain Meets Metaverse and Digital Asset Management: A Comprehensive Survey

VU TUAN TRUONG[1], LONG BAO LE[2], (Senior Member, IEEE), AND DUSIT NIYATO[3], (Fellow, IEEE)

[1, 2]INRS-EMT, University of Québec, Montréal, Québec, Canada
[3]Nanyang Technological University, Singapore

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

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 first provide necessary background of blockchain technology and the metaverse. Then, 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 governance system and metaverse infrastructure. We then provide a technical review of blockchain-based digital asset management, which plays a vital role in distinguishing the metaverse from other existing multimedia systems. Finally, we discuss various social aspects, privacy, security issues, and a wide range of open challenges of the blockchain-empowered metaverse.

INDEX TERMS Artificial intelligence, Blockchain, Digital asset management, Internet of things, Metaverse, 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 vivid experience. 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. 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. The metaverse is expected to revolutionize various aspects of life such as education [2], healthcare [3], entertainment [4], e-commerce [5], smart manufacturing and other social services [6].

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 [7]. Similarly, other tech giants like Microsoft, Google, and Nvidia have also taken solid steps to advance the metaverse with huge investments [8]. Existing metaverse projects and platforms such as Fornite[1], Roblox[2], and The 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. In particular, while the metaverse is envisioned to be a global virtual world in which people are not restricted to any particular platform, 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 single organization. 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. Otherwise, if a particular organization has all rights to generate/ delete digital contents and virtual currencies, the platform would eventually lack the desirable fairness and sustainability.

B. MOTIVATIONS

Blockchain technology could empower the metaverse with these above characteristics, thus enabling a truly virtual society. 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 various outstanding properties such as immutability, transparency, decentralization, and security.

Cryptocurrency, an important derivation of blockchain technology, would play a vital role in the metaverse's economic system. Furthermore, major key technologies derived from blockchain such as smart contract, Non-Fungible Token (NFT) [9], Decentralized Autonomous Organization (DAO) [10], Decentralized Finance (DeFi) [11], and Decentralized applications (dApps) [12] 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 interoperability.

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.

C. EXISTING SURVEYS

There were several recent surveys on metaverse and related enabling technologies, and the list has been growing rapidly over recent years. The paper [13] could be considered as the one whose purpose is most similar to our current work, since it mainly discusses the role of blockchain in the metaverse. In that study, the authors mostly focus on applications related to data management such as data acquisition, data storage, data sharing, data privacy, data interoperability and how these applications impact the metaverse and its enabling technologies. However, data management is only one of the various important blockchain-based metaverse use cases as shown in Table 1. In fact, many other crucial applications that truly revolutionize the metaverse such as digital asset management are either not included or just introduced. Meanwhile, related published works on the mentioned applications have not been analyzed in the survey. Two recent papers [14], [15] both present the use of blockchain combined with AI in the metaverse. They present 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. The included use cases are just limited to introduction or brief discussion. The authors in [16] survey the metaverse in a broader technical perspective, where blockchain technology is considered one of eight pillars of metaverse enablers. Nevertheless, only several aspects of blockchain were introduced such as data storage, data sharing, and data interoperability, while most key blockchain-enabled applications were not

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

covered in the paper. The contribution of blockchain to the metaverse is also illustrated partly in [17] as one of edge-enabling technologies. The paper mostly concentrates on use cases related to mobile edge computing and communication networks, while deeper and comprehensive analysis on blockchain-based applications such as the governance system were not carried out. Similarly, other metaverse and social media surveys [18]–[23] mention 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.

D. CONTRIBUTIONS

Aiming to fill the existing gaps in the literature, our paper provides comprehensive discussions on the role of blockchain technology 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. These use cases are divided into metaverse virtual services and the economic systems of the metaverse.
- Thirdly, we describe the impacts of blockchain on the metaverse from the system perspective, including applications for the governance system and for the metaverse infrastructure.
- Next, we conduct an in-depth technical analysis on digital assets in the metaverse, and present a 8-stage digital asset management workflow for this virtual world.
- Then, we discuss various important aspects such as security, privacy and social, ethical issues of the metaverse.
- Finally, we discuss open challenges in integrating blockchain into the metaverse from both technical and social angles.

Table 1 presents the contribution of our works 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. Section II presents the background of blockchain, the metaverse, and the potential integration of blockchain into the metaverse. Then, various blockchain-based applications in the metaverse are discussed in Section III. In Section IV, we present how blockchain technology empowers the metaverse from the system perspective. Section V focuses on the roles of blockchain for digital asset management. Section VI provides discussion of metaverse security, privacy and social, ethical aspects. Open challenges are discussed in Section VII, while Section VIII concludes the paper. For convenience, the list of abbreviations is given in Table 2. Besides, the organization structure of this survey is given in Fig. 1.

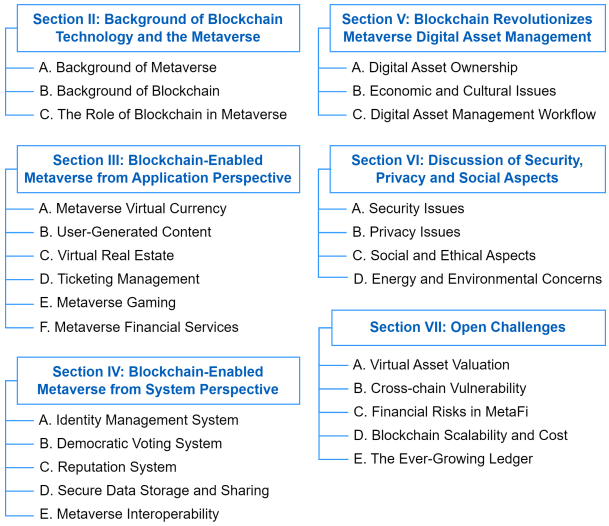

FIGURE 1. General structure of the survey.

II. BACKGROUND OF BLOCKCHAIN TECHNOLOGY AND THE METAVERSE

In this section, we provide the background of metaverse and blockchain. For the metaverse, we introduce its architecture, characteristics, backbone technologies and a wide range of applications. For blockchain technology, we discuss its general structure, properties, consensus algorithms, and cross-chain mechanisms. Then, we briefly describe how blockchain can empower and enable the metaverse.

A. 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. 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 freely. Users in Second Life can even register for real-world Intellectual Property (IP) rights to protect their 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,

[4]https://secondlife.com/

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

Content	[13]	[14]	[15]	[16]	[17]	[18]	[19]	[24]	[20]	[21]	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, ticketing management, and metaverse finance.	+	+			++	+		+	+		+++
The survey shows how blockchain empowers the metaverse governance system with identity management, democratic voting, and reputation systems.						+				++	+++
The study analyzes the contribution of blockchain to the metaverse infrastructure with data management, and blockchain-enabled interoperability.	++			+	+++				+		+++

TABLE 2. List of Abbreviations

Abbreviation	Definition
ABAC	Attribute-Based Access Control
AGU	Attribute Grant Unit
AI	Artificial Intelligence
AR	Augmented Reality
DAO	Decentralized Autonomous Organization
DApps	Decentralized Applications
DCF	Discounted Cash Flow
DDS	Data Depository Server
DeFi	Decentralized Finance
DFS	Distributed File System
DID	Decentralized Identifier Document
DRM	Digital Right Management
DT	Digital Twin
IoT	Internet of Things
IP	Intellectual Property
IPFS	InterPlanetary File System
MetaFi	Metaverse Finance
MMO	Massively Multiplayer Online
NFT	Non-Fungible Token
NLP	Natural Language Processing
NPC	Non-Player Character
NVT	Network Value to Transactions
PDP	Policy Decision Point
PDS	Policy Depository Server
PE	Price to Earnings
PEP	Policy Enforcement Point
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
REL	Rights Expression Language
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

blockchain technology revolutionizes metaverse digital asset management and provides necessary tools to address a wide range of issues in the metaverse.

1) Metaverse Architecture

The metaverse is envisioned to be an immersive 3D virtual world that reflects the physical world in various aspects such as society, politics, culture, and economy [25]. In this digital world, people can participate in different virtual activities such as working, playing games, shopping, trading assets, and even purchasing virtual lands [14]. To take part in the Metaverse, users use wearable AR/VR devices and represent themselves as a real-time digital avatar, which reflects their appearance with a variety of facial expressions and gestures.

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.

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. The networking infrastructure can consist of various elements such as satellite, unmanned aerial vehicle (UAV) communications, and especially 5G and beyond wireless networks. To efficiently handle and process the metaverse data, an appropriate combination of various computing technologies is crucial, such as cloud, edge, and end-user computing. For example, while computationally extensive tasks can be processed at cloud data centers, applications requiring fast response should be carried out at the edge servers to improve user experience. Besides, data storage is also an important factor in the metaverse infrastructure, and it could be facilitated by blockchain. 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 especially interoperability.

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. 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. To boost user experience further, AI can be utilized to realize many potential metaverse functions and applications. 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. Translation and other Natural Language Processing (NLP) techniques are also very useful in the metaverse, a borderless environment in which users come from many different nations. Besides, blockchain could also contribute to this process with smart contract, cryptocurrency, NFT, and decentralized applications.

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. Users participate in the platform through their avatars, thereby involving in a variety of activities and services such as education, entertainment, and healthcare. At the highest extent, the metaverse could bring users an entire virtual "second life".

2) 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. 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 single 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 has a global unique identity across platforms. With the specific identity, they can move between different metaverses seamlessly. Users can also transfer digital assets across metaverses. Furthermore, the ultimate version of the metaverse could even interact with the real world.
- **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 [16].

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.

3) 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 [16]. 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.
- **Digital Twin:** DT uses real world data to create digital representations of physical objects. It enables the synchronized property of the metaverse, 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 [27].
- **Artificial Intelligence:** AI contributes to the metaverse in different ways. Firstly, it could create and empower several metaverse technologies, thereby indirectly contributing to the metaverse. Moreover, it can enable the automatic creation process such as creating vivid digital avatars through learning user emotions and facial expressions. Besides, it can be ulilized to develop various virtual smart services such as smart NPCs (non-player character) and automatic translation, recommendation.
- **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 [28].
- **Cloud and Edge Computing:** While wearable devices often have limited processing power and storage capacity [29], the servers running the metaverse 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

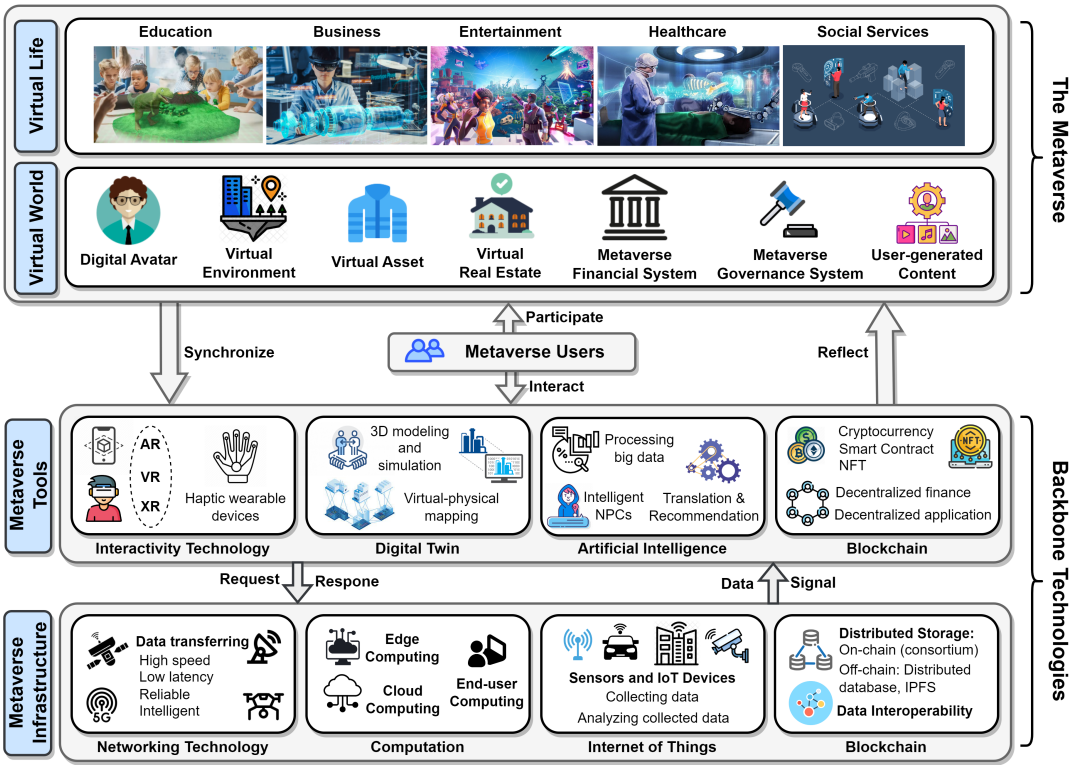

FIGURE 2. General architecture of the metaverse, constructed by various advanced technologies.

is crucial in processing the tremendous amount of data in the metaverse while delivering the required quality of service.

- **Networking Technologies (5G/6G Wireless):** 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. Furthermore, state-of-the-art networking 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.
- **Blockchain:** Blockchain is the key technology which enables the decentralized, interoperable, and sustainable characteristics of the metaverse. It could create the entire economic system of the metaverse, while helping to maintain the value of digital assets. Blockchain could also contribute to the metaverse interoperability with cross-chain communication and multi-chain platforms. This technology and its impact on the metaverse are also the main concentration of this paper.

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. 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.

4) 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 [30]. 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 [31]. Besides, virtual factories in the metaverse could enhance the productivity for businesses, while digital workplaces offer convenient communication between staff [32].
- **Entertainment:** The metaverse can be considered as the future of the entertainment industry [33]. It offers immersive play-to-earn games, provides unlimited spaces for virtual concerts, virtual reality theme parks [34] and exhibitions.
- **Healthcare:** The metaverse with VR/AR and DT technologies could revolutionize the surgical practice and medical training for the healthcare sector [35]. Moreover, medical records could be stored on blockchain within the metaverse platform to ensure security and

integrity.

- **Social Services:** The metaverse could change both social and commercial insurance sectors by leveraging the blockchain technology for transparent document storage [36]. 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. However, within the scope of the paper, we concentrate more on applications enabled by blockchain.

B. BACKGROUND OF BLOCKCHAIN TECHNOLOGY

1) 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 [37]. 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.

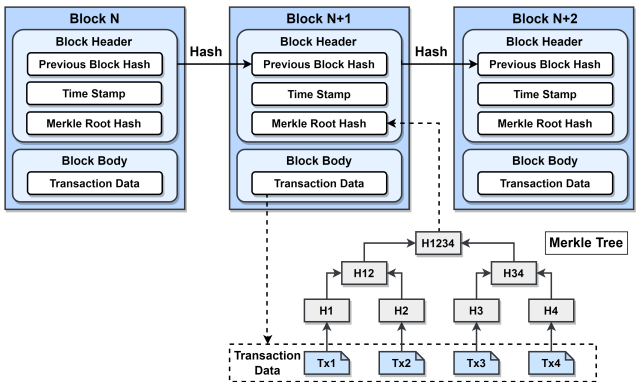

FIGURE 3. The general structure of a blockchain. The Merkle tree allows users to verify payments quickly without having to download the entire transaction history [38]. The block header actually often contains more fields, depending on particular blockchain.

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. 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.

2) 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 a consensus algorithm. 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 [39] and the popular ones include Proof of Work (PoW) and Proof of Stake (PoS) algorithms [40]. In PoW, nodes in the network compete to solve a mathematical problem 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. 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. 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.

3) 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*. 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 smart contracts 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 always available on-chain, every participant can verify its source code and make sure of its functionality. Smart contract functions are done automatically without the any trust assumption and the intervention of intermediaries. Smart contract programming languages are usually *turing complete*, so its applications are almost unlimited and only depend on the creativity of users [41].

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 [9]. 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 [12]. DeFi [11] 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 such as Visa and MasterCard.

4) 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 [42]. It helps independent blockchains connect together to form a large network, which could be considered to be the Internet of blockchains [43]. In general, blockchain interoperability often includes cross-chain bridge [44] and multi-chain platform [45], 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. Blockchains within the ecosystem must be designed with specific requirements and common standards to be able to communicate with each other. Current prominent multi-chain ecosystems include Polkadot [46] and Cosmos [47].

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 through a normal transaction. All of these tokens are then locked in the smart contract and cannot be used by anyone. 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. Note that the operator could be a single node or a group of validators depending on specific designs of the bridges.

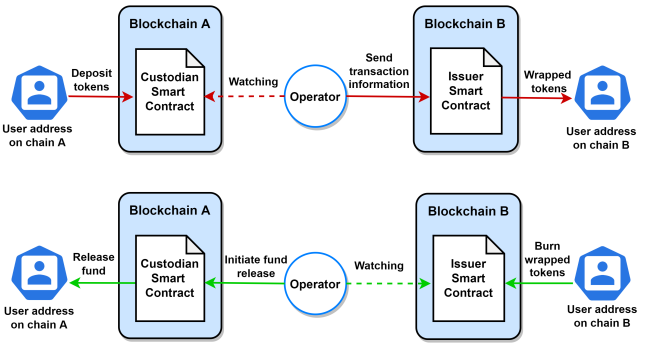

FIGURE 4. The general operation of blockchain cross-chain communication. The process above with red lines is to transfer tokens from one blockchain to another, while the figure below with green lines illustrates how tokens are transferred back to the original chain.

Whenever a node wants to transfer its tokens back to chain A, it sends them to the *issuer smart contract*, where these wrapped tokens will be burned. The operator periodically observes the burning process and transfers necessary information to the custodian smart contract on chain A.

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

After confirming that wrapped tokens have been burned, the *custodian smart contract* unlocks deposited tokens and sends them to the node's address on chain A.

C. BLOCKCHAIN ROLE IN METAVERSE

The concept of MMO games can give the early sense of the metaverse in which there is a virtual world where players can participate as virtual characters. Players can also communicate with each other, trade in-game items, and join various activities. One may wonder what really distinguishes the metaverse from a traditional MMO game. The first improvement to be mentioned may be the integration of VR/AR technology that provides users an immersive experience in such virtual worlds. However, this does not seem to be sufficient to attain unique characteristics of the metaverse as it is still merely a game where almost everything is under control of the game developers. On the other hand, the emerging blockchain technology offers the metaverse exactly what it needs to become a complete virtual society. With blockchain, the metaverse can be constructed as a decentralized digital world in which all participants operate it rather than following some fixed rules released by the organizations. Furthermore, NFT and cryptocurrency could enable a reliable and stable economic system in the metaverse, while DeFi and dApps provide a variety of virtual services which are similar to real-world services. They are shown in Fig. 5.

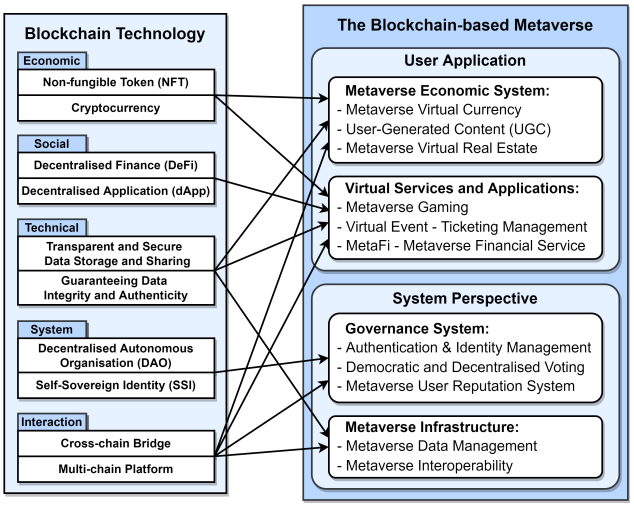

FIGURE 5. Blockchain technology enables the metaverse in different perspectives

The integration of blockchain into the metaverse is not just limited to user-side applications. This technology can also empower the metaverse from the system perspective. Advanced technologies based on blockchain such as Self-Sovereign Identity (SSI) [48] and DAO [10] can be leveraged to build a democratic governance system in the metaverse. Furthermore, blockchain with its outstanding properties such as immutability, transparency, and decentralization could be considered to be a secure option for data storage if it is combined appropriately with other traditional storage techniques.

III. BLOCKCHAIN-ENABLED METAVERSE FROM USER APPLICATION PERSPECTIVE

In this section, we present possible contributions of blockchain technology to the metaverse from the user applications perspective, including the metaverse economic system and metaverse virtual services. While the blockchain-enabled economic system includes components such as virtual currencies, UGCs, and virtual real estate, metaverse virtual services cover application areas such as gaming, metaverse financial services, and ticketing management for virtual events. For each of these potential use cases, we first discuss related technical issues, then describe how blockchain can help solving these problems. According to various metaverse features and applications, a summary of some existing metaverse platforms based on these features is provided in Table 3.

A. METAVERSE VIRTUAL CURRENCY

The metaverse is expected to be a global virtual world where participants can take part in a wide range of activities similar to the physical world [16]. Important activities include shopping, working, playing games, and other social businesses and services. To this end, there is a need for a medium of exchange between customers and service providers in this virtual society. Since user interactions in the metaverse occur in the virtual space and in the real-time manner, using traditional fiat currencies seems not a suitable option. Firstly, the metaverse is a global environment so trading virtual items or exchange currencies between users in different countries are regular activities [49]. Using the traditional legal currency system for cross-border transactions is very costly and complicated with numerous procedures and additional fees. Moreover, since the metaverse would not rely on any government or centralized organization for operation, its economic system must be transparent, consistent, and verifiable to avoid scams and frauds. Although some current metaverse platforms such as Roblox still allow users to buy in-game items by fiat currencies [50], there is a strong need for a virtual currency, or even an ecosystem of digital currencies.

Blockchain technology offers a suitable solution - cryptocurrency, which solves most of the above issues. Actually, cryptocurrency is the first and most ubiquitous application of blockchain technology. It has various desirable features for the metaverse economic system:

- **Cross-border Payment:** Blockchain-based cryptocurrencies are distributed globally through the Internet instead of being controlled by any government like the traditional fiat currency system.
- **Privacy:** When it comes to cryptocurrency, identity of users is encoded to a long string of characters called addresses, so finding out the real-life identity of any user in the metaverse is almost impossible.
- **Decentralization:** As the metaverse would not be under control of any third-party authority, trading among users should be direct and permissionless.

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	✗	✗	✗	✓	✗	✗	✗
The Sandbox	Pixowl	NFT-based Game	✓	✓	✓	✓	✓	✓	✓
Cryptovoxels	Nolan Consulting	NFT-based Game	✓	✓	✗	✗	✓	✗	✓
Somnium	Somnium Space	VR Game	✓	✓	✓	✗	✓	✗	✓
Axie Infinity	Sky Mavis	NFT-based Game	✗	✓	✓	✓	✓	✓	✓

- **Immutability:** Blockchain-based cryptocurrencies ensure the immutability of transactions as they are almost impossible to be changed after being submitted onto the chain.

With the above properties, cryptocurrencies are crucial to construct a complete financial system for the metaverse. Many metaverse platforms currently use cryptocurrencies for their economic systems. Axie Infinity[8], a blockchain-based gaming metaverse, uses two types of fungible token for their currency system, which are SLP and AXS. While SLP is spent on breeding Axies (the Pokemon-inspired in-game creatures), AXS can be used to vote on the development direction of the game. Both of them can be considered as digital currencies and can be traded or exchanged for other cryptocurrencies such as Ethereum. Besides, Decentraland, a virtual reality platform empowered by the Ethereum blockchain [51], introduces MANA tokens as the virtual currency. With MANA, users can buy or trade land and pay for virtual assets and services in the virtual world. Similarly, SAND is the cryptocurrency used in The SandBox[9], another popular 3D metaverse platform. This digital currency can be spent on purchasing items and virtual real estate in the platform.

B. USER-GENERATED CONTENT

Encouraging the creativity of users is one of the most important prerequisites of the metaverse, and UGC is a powerful driving force of this virtual space. With this feature, users can be creators of virtual assets such as clothes, vehicles, buildings and contents like videos, images or music. This could give users a great sense of freedom and make them more interested in the metaverse, thus attracting more people to the platform. This has been proved by the popularity of various mods (modifications) of video games such as Grand Theft Auto [52] in which users can create any items or even a new map with its own rules and gameplay. The success of YouTube with user-generated videos also affirms the potential of UGC and user's creativity [53]. Therefore, UGCs are expected to become a vital part of the metaverse.

However, UGCs could be copied easily and become valueless since they are all digital contents. To maintain the value of such UGCs, they should be represented as NFTs [9]. NFTs can be used to represent the ownership of digital assets such as arts, videos, postcards or in-game items [19]. With the uniqueness property, NFTs cannot be replicated or equated with any other assets. Specifically, each NFT exists on a particular blockchain and it has a unique identification on the chain. NFTs can be traded through transactions on the blockchain, thus they are transparent on the chain and everybody can keep track of its history. Moreover, being stored on the blockchain also means that it has the non-tampering characteristic. These features make NFT-based UGCs valuable.

Several metaverse platforms currently use NFT to tokenize UGCs such as Decentraland [54] where users can generate their own UGCs to decorate their avatars and build the environment around their lands [20]. Similarly, Roblox and The Sandbox are two other popular metaverse platforms allowing users to generate and sell UGCs [55]. In Roblox, users use *Roblox Studio*[10] to generate virtual items such as clothes, gears, and even body part, which can be traded between players. On the other hand, UGCs in The Sandbox are represented as smart contract ERC-1155 on the Ethereum blockchain [56]. These UGCs are classified into three categories, which are entity, equipment, and block. While block is a user-generated version of basic in-game landscape blocks, equipment is anything that could be worn by avatars, and entity is UGCs that are placed in the virtual space.

C. METAVERSE VIRTUAL REAL ESTATE

In the real world, real estate refers to lands along with any permanent improvements attached to the land such as buildings and houses. Real estate can be used for various purposes including rental, investment, marketing, event organization or retail display. Since the metaverse aims to represent the real

[8]https://axieinfinity.com/
[9]https://www.sandbox.game/en/
[10]https://www.roblox.com/create

world to the highest extent, such activities should be maintained. However, while land in the physical world is unique since it belongs to the earth's surface, real estate in a digital world can be duplicated and counterfeited easily. Fortunately, blockchain and specifically NFT provide a suitable solution to address this problem for virtual real estate. Representing the digital real estate as NFT and storing it in the blockchain make it fully benefit from core properties of blockchain and NFT, namely unique, transparent, immutable, and anti counterfeiting. These characteristics make the metaverse real estate valuable compared to that in other centralized platforms. We envision two development stages of the metaverse real estate as follows:

- **Digital Natives:** The digital world is independent from the physical world. Land or virtual real estate is represented as square blocks or pixels in a large metaverse map. Virtual land in a particular metaverse is only available in that metaverse.
- **Physical-virtual Co-existence:** This is the highest level of metaverse, in which the virtual world reflects exactly the physical world. In this development stage, we could imagine a virtual world where users can, for example, go shopping in a virtual New York, a digital Tokyo or any place in the world instead of arbitrary square blocks.

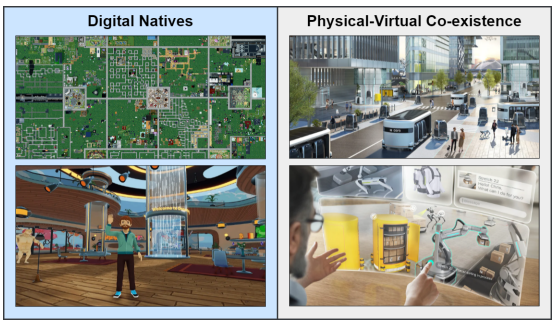

FIGURE 6. Two development stages of metaverse real estate. Pictures on the left illustrate a digital world that is separate from the physical world, in which real estate is represented as square blocks on a virtual 2D map. Pictures on the right show a virtual world that reflects the physical world exactly, where virtual real estate can be mapped to real-world real estate.

The above developments of metaverse real estate are shown in Fig. 6. Since the second stage requires huge efforts and the maturity of various advanced technologies such as DT [57], AR/VR, most current metaverse platforms are still in the first development stage. Prominent existing real estate ecosystems include Roblox, Sandbox, Decentraland, Cryptovoxels[11], and Somnium[12]. Due to the emergence of blockchain and metaverse, various companies have been heavily investing in virtual land properties. For instance, Republic Realm, a leader in metaverse and NFT innovation and investment, paid $4.3 million for virtual land in Sandbox [58], the largest metaverse real estate ecosystem. The company is developing 100 islands called Fantasy Islands with their own villas and a related market of boats and jet skis. Besides, Tokens.com, a blockchain company, acquired 50% of virtual real estate company *Metaverse Group* for $1.7 million [59]. In terms of digital marketing, Acura, a car brand owned by Honda Motor Company, has built a virtual showroom on virtual real estate in Decentraland [60]. People can indeed join the showroom in third-person or first-person mode and walk around to see the newest car models of the brand. Acura also plans to allow customers to place NFTs to the showroom as galleries.

[11]https://www.cryptovoxels.com/
[12]https://somniumspace.com/

D. METAVERSE VIRTUAL EVENT - TICKETING MANAGEMENT

The metaverse real estate as presented in Section III-C provides users a large space to immerse themselves into the 3D virtual world with a variety of social activities. Metaverse-based virtual events represent one of the most popular use cases that has been adopted, and it has even replaced the real-world events to some extent during the Covid-19 pandemic. For example, hundreds of graduating UC Berkeley students attended a virtual commencement ceremony organized in Minecraft [61]. Students and their families took part in the ceremony and many of them even streamed it around the world. Another well-known virtual event is the historic concert of Travis Scott in Fortnite, attracting more than 12 million participants to attend and enjoy his performance [61].

For this purpose, blockchain technology offers an appropriate solution for ticketing management. In fact, managing a ticketing or coupon system is a highly complex operation which involves the management of an issuing process of tickets, recording sold tickets for tax purposes, and the most important, verifying the authenticity and correctness of the tickets [62]. From the organization perspective, event organizers must apply proper strategies to ensure their issued tickets not counterfeited [63]. Moreover, the fairness could be threatened when demand is greater than supply. In this circumstance, tickets may be circulated in the black market, where some individuals may unfairly profit from selling tickets at higher prices. On the other hand, from the customer perspective, participants cannot be sure of the exact number of tickets issued by the organizers. They may suspect that the organizers have issued more tickets than announced, thereby pushing the price up while the quality of the event goes down. In the worse case, customers cannot be certain that the ticket they bought is actually valid or not. These problems can be addressed by applying blockchain technology and NFT in the ticketing process.

The main advantage of using blockchain and NFTs for ticketing is that it provides the ability to verify the validity of a ticket and to keep track of the tickets after they are sold. All tickets are securely linked to the buyers, and all transactions related to any ticket are stored in the blockchain. Therefore, tickets cannot be counterfeited, while the distribution and verification process can be done efficiently. Furthermore, the organizers can adjust the smart contract code to add more features to their NFT-based tickets. For instance, they can

prohibit the resale of tickets or limit the number of resellers per ticket. This ensures ticket price be reasonable, and it also eliminates the possibility of scalping, scamming, and fraudulent transactions.

In the metaverse, privacy is a crucial factor for ticketing management in virtual events. If the identity of the buyers are leaked, they might be attacked by hackers. To this end, Cha *et al.* proposed a privacy preserving blockchain-based ticketing service [62], using blockchains to store information related to events and tickets, whereas Non-Interactive Zero-Knowledge Proofs (ZKP) are used to preserve user privacy. It allows users to prove the ownership to their tickets and ensures the integrity of data, while it does not public user data so that the privacy is guaranteed at the highest extent.

Besides privacy, user experience is also an important factor in the metaverse. The author in [63] developed a blockchain-based prototype system for concert tickets to prevent ticket theft and fraud. A convenient user application is provided which allows users to transfer tickets on their smart phones conveniently, as well as facilitates the process at the entrance gate.

E. BLOCKCHAIN FOR METAVERSE GAMING

Gaming is among the earliest and hottest applications of the metaverse. Since the metaverse is still in its infancy, there must be many further improvements before it really comes into life and contributes real value to the society. During the development of the metaverse, gaming provides an excellent environment for technological improvements to be implemented and it gives an interesting means for users to explore the metaverse. In terms of metaverse games, blockchain technology plays a key role and contributes to various aspects of such platforms. In the following, we define two levels of metaverse gaming:

- **The metaverse as a particular game:** The metaverse itself can be considered as a particular game with predefined gameplay and rules. For example, Axie Infinity[13] can be viewed as a blockchain-based gaming metaverse where players collect and breed digital pets called Axies that can be used to compete in a turn-based card game.
- **Games within the metaverse:** The metaverse is considered as a virtual world supporting different activities, and gaming is one of them. Users can play games at certain places within the digital world. For instance, some places in Decentraland offer board games or casino games [64], where users can play and earn virtual tokens.

For the first scenario where the entire metaverse is a single game, blockchain and NFT are usually adopted to tokenize in-game assets, making them unique and valuable. For the second circumstance, blockchain ensures the transparency of in-game rules. Considering a traditional game where all game rules are hidden behind the code in a centralized game server, the production of any random number is usually unsupervised. For example, a video game may claim that opening an in-game treasure has 25% chance of winning a rare and valuable item; however, the real figure could be relatively lower as game manufacturers often claim a higher winning possibility to attract game players. Even in some casino games like poker or blackjack, the games can be pre-programmed to put players at disadvantages with high possibility of losing money. In metaverse games, critical game rules could be carried out as smart contracts and stored on blockchains. Thereby, the transparency of game rules is guaranteed as game players can supervise those smart contracts when they are implemented.

Many metaverse games have been introduced and most of them use blockchain technology as a key component. Roblox[14] is a global user-created game platform allowing users to create their own block-based characters and play through a wide range of different games [50]. Another popular metaverse game is Sandbox[15], which offers players a plot of virtual land in the form of NFTs based on the Ethereum blockchain. Sandbox provides players a virtual world where they can build and monetize their own virtual experiences [65]. Fortnite[16], a massively popular game that started out as a Battle Royale has now evolved into metaverse gaming [66], where players can construct buildings, bunkers, and even build islands. However, the greatest experience in the Fortnite metaverse may be live concerts that have been held in this platform [61].

F. METAFI - METAVERSE FINANCIAL SERVICES

In the physical world, we participate in a wide range of financial activities everyday. Similarly, the metaverse must also reflect all those activities and services, and blockchain along with the emerging DeFi technologies provide suitable tools to realize them in a decentralized manner [67]. In the following, we firstly classify financial activities into three main types which are personal, corporate, and public finance. Then, we discuss how these activities can be reflected in the metaverse by using blockchain technology and its related mechanisms.

- **Personal Finance:** This specifies individual's financial situation and activity, mainly related to person's earnings. Possible use cases for the metaverse in terms of personal finance include saving, investment, borrowing, and lending [68]. Besides creating and trading virtual assets to earn digital currencies, metaverse users can deposit their currencies to liquidity pools [69] constructed by smart contracts, thus earning the interests every day, or even every several seconds. On the other hand, users can also borrow digital money from the pool with a reasonable interest rate, and then use it for their personal purposes. Different from the traditional banking system, all these activities are decentralized without third-party

[13]https://axieinfinity.com/

[14]https://www.roblox.com/

[15]https://www.sandbox.game/en/

[16]https://www.epicgames.com/fortnite/en-US/home

authorities [70]. In other words, savings interest does not need to be shared with any third parties; they can be managed automatically by smart contracts.

- **Corporate Finance:** This refers to financial activities related to running a corporation. For example, a company may raise fund by issuing stocks and bonds. When it comes to the metaverse, stocks and bonds issued by a company can be represented as NFTs or fungible tokens in the virtual world, thus facilitating the validation process and ensuring the integrity of those assets [71]. The issuing process based on smart contracts is also transparent to the public, so everyone can be sure of their benefits [72]. Moreover, companies participating in the metaverse can utilize DAO to make their financial decisions [73].
- **Public Finance:** This includes financial services related to the society such as tax or social insurance. For these purposes, the blockchain technology could be a game changer [74], [75]. The critical aspects of tax and insurance include the publishing and transparency of documentation and methods to manage identities of both issuers and customers. Blockchain technology with its transparent nature and advanced identity management techniques could facilitate these processes [76]. With the metaverse, all necessary information related to insurance products is always available, while it can be transferred seamlessly across platforms through cross-chain mechanisms of blockchain technology. Therefore, it could be considered as the key diving force for the metaverse in public financial services.

Blockchain and DeFi technologies have shown their potential to establish the entire financial system in the metaverse enabling various financial activities and services. However, there are still financial risks since it lacks government guarantees and the DeFi technology itself is still in the early stage. Further development of DeFi and appropriate policies from governments are needed to keep the MetaFi safe and reliable.

G. LESSONS LEARNED

1) Blockchain-enabled Metaverse Economic System

Thanks to blockchain technology, the metaverse may have its own complete virtual economy which is comparable to the real-world economic system. In this digital world, participants can use cryptocurrency as the main payment method. It not only facilitates cross-border payment with the decentralized characteristic, but also improves security thanks to its immutable and tamper-proof properties. Furthermore, users can create virtual assets and prove their ownership of such creations using smart contract and NFT. Thereby, creating and trading UGCs may become an official source of income of metaverse creators. Meanwhile, NFT-enabled virtual real estate can be used to organize business virtual marketing and various virtual activities of users.

2) Metaverse Virtual Services and Applications

Blockchain offers metaverse users a wide range of financial services. For personal finance, it includes saving, investment, borrowing and lending virtual currency without the need of third-party authorities. For corporate finance, companies can issue NFT-based stocks and bonds in the metaverse to raise funds. The decentralized environment regulated by smart contracts could prevent stock market manipulation, thus ensuring the benefit of participants. Moreover, various public financial services such as taxes or insurance in the metaverse can be facilitate by blockchain with its decentralized and transparent properties. As insurance information is stored on blockchain, it is immutable and always available for access.

In terms of entertainment applications, blockchain and smart contracts can be integrated into metaverse games to ensure the game rules by making them transparent and immutable. NFT is also an important mechanism which can be used to tokenize in-game items, thereby guaranteeing the ownership of these assets. Finally, blockchain enables metaverse virtual events with effective ticketing management methods. It ensures the fairness in issuing tickets and provides users with ability to verify and keep tracks of the tickets as all data are transparent to the public.

IV. BLOCKCHAIN-ENABLED METAVERSE FROM SYSTEM PERSPECTIVE

In this section, we discuss the potentials of blockchain for the metaverse from the system perspective, including the metaverse governance system and metaverse infrastructure. In terms of governance, blockchain offers a global identity management system, the democratic voting scheme, and a reliable reputation system. Blockchain could also contribute to build the metaverse infrastructure by providing efficient solutions for decentralized data storage and metaverse interoperability.

A. IDENTITY AND AUTHENTICATION MANAGEMENT

In the real world, identity is probably one of the most important assets which defines who we are. Depending on specific purposes, one may have various identities such as identification, passport, driver license or student code. In specific circumstances, we may have to present our identity credentials to access some services or to take part in certain activities, e.g., proving we are over 18 to buy alcohol. Similarly, identity also plays a vital role in the virtual world, and the metaverse is not an exception [77]. In general, user identity in a digital world could be classified into three types:

- **Centralized Identity:** The digital identity is managed by a single enterprise to control authentication [78]. Each user needs at least one digital identity credential for each organisation, e.g., a Gmail account.
- **Federated Identity** [79]**:** The digital identity is stored across multiple distinct identity management systems. For instance, we use a single Gmail account to access multiple websites with the option "Login with Google".

- **Self-sovereign Identity** [80]**:** The digital identity is owned and fully managed by an individual user. It guarantees privacy by removing the need to store personal data on a centralized database and gives users entire control over what information they share [81].

In the metaverse, each user must have a unique digital identity to distinguish herself/himself from others. However, identity management in the metaverse is even harder in comparison with that in the physical world since there is no third-party having the right to store and verify user identify. While centralized identity and federated identity are vulnerable to potential privacy risks [82], SSI could be an appropriate authentication method for the metaverse. In particular, SSI consists of three emerging mechanisms which are Verifiable Credentials [83], Decentralized Identifiers [84], and Blockchain. With SSI, there will be no more username/password schemes where users have tons of passwords to remember, whereas organizations control all user information. Instead, users can prove their identity through verifiable credentials [48]. Each user or organization is associated with a unique decentralized identifier document (DID) which could be used across different platforms throughout the Internet. To this end, blockchain technology plays the role of storing all DIDs and making them immutable, transparent, and secure thanks to its decentralized property [85]. Moreover, Zero-knowledge Proof [86] could be used to enable the SSI. As a result, users can prove their identity without revealing any personal information, or they can reveal only the information that they want to share [87].

Various studies are currently underway to further enhance the SSI technology and make it more feasible to be deployed into the metaverse. The authors in [88] proposed 12 design patterns for an SSI system based on blockchain technology, classified them into three categories, namely key management patterns, decentralised identifier management patterns, and credential design patterns. In the context of metaverse, they could be utilized to fit specific purposes. For instance, if an organization wants to manage their participants in a metaverse platform, the Identifier Registry scheme of DID Management Patterns can be a suitable solution. In this scheme, attributes of identities are mapped to an off-chain storage such as IPFS, while the associated location of the identifier (e.g., the IPFS hash link) is managed by smart contracts. This could help prevent single point of failure (SPOF) and ensure that only the identity owner has the right to modify the identifier data.

Besides, privacy is a crucial factor in terms of metaverse identity system. If user information is leaked in the virtual world, their real-world life might be threatened seriously. The authors in [89] proposed a privacy-preserving SSI framework for digital platforms, named *Casper*. In this framework, all personal information will be stored on user's devices (e.g., mobile wallet) instead of any centralized database to guarantee user privacy. Furthermore, all data within the platform are signed by the corresponding parties using RSA digital signature, thus improving data integrity and security. With these essential features, users can be more confident when participating in the metaverse. Besides, unauthorized users can also present potential threats to blockchain-based identity systems. Esposito *et al.* [90] presented a distributed authentication framework for smart city applications based on blockchain technology. The framework can protect identity data from malicious and unauthorized users in a large scale scenario.

Although security and privacy are the major concerns when it comes to authentication in the metaverse, user experience is also an important factor. The authors in [91] presented an user-friendly SSI framework for the metaverse, in which each user owns an unique identity which could not be counterfeited and altered since it is stored on blockchains. Whenever the user wants to receive a virtual service, she will show her credential, which could be verified easily with a SSI wallet and the QR code. Meanwhile, the user is not required to provide any additional information.

Authentication in the metaverse is not limited to the user side. Instead, authentication management of IoT devices in the metaverse infrastructure is also an important factor. The authors in [92] introduced *bubbles of trust*, a blockchain-based authentication system for IoT devices that protects data integrity and availability. The system provides "bubble" zones that allow devices to identify and trust each other within a same zone. To further enhance security and performance of IoT authentication, the authors in [93] proposed a hybird scheme based on blockchain for multi-WSN. In the scheme, IoT nodes are divided into different types based on their capability, thus forming a hierarchical network to optimize efficiency. Whereas, both local and public blockchain are utilized to provide resistance to a wide range of attacks and offer mutual authentication.

B. DEMOCRATIC VOTING SYSTEM

Governance is a vital factor shaping the future of any digital platform. In traditional centralized systems such as a game or a social media, the organization who created the platform could unilaterally decide its future orientation. They can propose several minor updates to improve user experience, but sometimes, there might be some updates that entirely change the rules and policies of the virtual system. Unfortunately, users have no choice but to accept the changes.

Going towards the decentralized environment in the metaverse, the authors in [94] highlight three requirements for governance in any future digital ecosystem:

- **Respecting human rights:** Governance of the global digital content ecosystem must ensure that any actions taken in response to government orders on content removal should respect international human rights law.
- **Decentralized:** Governance models should be open, participative, transparent, and consensus-driven.
- **Publicly accountable:** Governance should follow a fundamental principle of public accountability. For instance, private companies that do content moderation should be held accountable to the public interest.

Blockchain technology again offers a potential solution satisfying most of these requirements if the DAO approach is employed [95]. In particular, DAO is a straightforward approach for decentralized governance in the metaverse based on the underlying smart contract mechanism. DAO is generally flat and democratized, where voting is required by members for any changes or updates to be adopted [96]. With DAO, all offered services are handled automatically in a decentralized manner without any centrally controlled governance system which is prone to manipulation. Furthermore, being deployed through smart contracts means that it is transparent since all users and developers can observe its source code. Decentraland is one of the most popular platforms adopting DAO, where users and stakeholders could vote to determine how the virtual world operates and evolves [51]. In this platform, the community will propose and vote on any policy update, including a wide range of aspects such as upgrading LAND (virtual land in Decentraland) and estates, specifying dates of future LAND auctions, determining marketplace fees or even replacing members of the Security Council. Additionally, Sandbox is aiming to run DAO in 2022 to offer landowners a much more prominent voice in the platform [65].

In addition to DAO, blockchain and smart contract can be utilized in various ways to engineer a reliable voting scheme for the metaverse. The authors in [97] presented BSJC, a proof of completeness algorithm that builds the specific blockchain for the electronic voting platform. In this scheme, blockchain facilitates the polling process by providing anonymity and security in election. However, there is still a third party involving in the process, making it vulnerable to data leakage, privacy issues and biased results. To ensure the highest extent of privacy, the authors in [98] proposed the first deployment of a self-tallying voting system that maximizes voter privacy, named *Open Vote Network*. Since the scheme is transparent and self-tallying thanks to ZKP, the role of third-party authority is eliminated completely. A proof of concept was implemented on Ethereum official testnet to estimate computational cost and demonstrate its feasibility. On the other hand, the voting size in the proposed framework was limited to just around 60 electors. This scalability limitation could hinder it from being adopted widely.

To fill the gap of scalability and performance constraints, Khan *et al.* [99] investigated a wide range of permissioned and permissionless blockchain settings across various scenarios of e-voting system to determine the optimized trade-offs between different properties. As a result, a blockchain-based voting scheme has been proposed and implemented with optimized performance and scalability. However, voter's integrity is not considered in this design, while it was shown to be insecure against quantum attacks [100]. In fact, the future quantum computing technology might pose a severe threat to these blockchain-based systems, thus it is necessary to proactively figure out possible solutions for this type of attack. To this end, the authors in [101] 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 [102] to make the system more resistant to quantum attacks. Furthermore, transparency and auditing functions are also provided in the scheme.

When adopting blockchain for the metaverse voting system, the cost of hosting a massive voting scheme should also be considered. The authors in [103] presented a blockchain-based e-voting system that improves security, while the hosting cost is optimized. Besides, the immutability feature of blockchain might become a double-edged sword in the metaverse. If a voter accidentally submits a wrong vote, the unexpected results will be recorded immutably on the blockchain. The authors in [104] designed a blockchain-based e-voting system that allows voters to change their votes according to a predefined deadline. By doing so, the voting system not only obtains necessary security features of blockchain technology, but it also offers better practical operation thanks to the withdrawal model. A multi-candidate system has been deployed on peer-to-peer Linux platforms to verify this design.

C. REPUTATION SYSTEM

The reputation system provides mechanisms that allow users and service providers to build trust through reputation. This can be evaluated based on feedback, rankings, ratings, and reviews of users for any service they have received. For example, reputation systems are usually used by E-commerce platforms such as eBay and Amazon in which users can rate the products that they have bought. This implies an incentive mechanism which encourages service providers to offer only good services to maintain their ranking. Otherwise, they would receive negative feedback and it impacts negatively their business. For social media such as Facebook or Instagram, there are also some indirect forms of reputation system built based on the number of followers of an account, or the number of "likes" for each of user's pictures and videos. Having an account with numerous followers may imply that the user is well-known and likely to be reputable within the platform. Therefore, the user could become service providers, who offers personalized marketing services.

When it comes to the metaverse, a reputation system could provide a powerful mechanism to prevent fraud, scam and improve the quality of service throughout the ecosystem. This is illustrated partly in the *Nosedive episode*[17] of the science fiction film series *Black Mirror*. In this world, people can rate each other in a five-point score for any interaction between them. Similarly, with a reliable reputation system, users in the metaverse could rate others after receiving their products, services or after any interaction with each other. However, creating fake reputation is very popular in such online platforms if the system is centralized. Since all the ratings are not transparent to the public, users can create numerous fake accounts to rate for themselves. Furthermore,

[17] https://ew.com/recap/black-mirror-season-3-episode-1-nosedive/

the central organization controlling the reputation system could easily change the rating data to earn benefits.

On the other hand, with a blockchain-based reputation framework, users can submit a rating transaction to the chain whenever they to rate for a service provider. As transactions on blockchains are immutable, users can be confident about the correctness of the reputation system. Moreover, users can keep track of the rating list of any particular service provider since these data are always transparent and available on-chain. No one can control and gain illicit profits from the system, making it fairer and more reliable. The transaction fee when submitting rating transactions to the blockchain could be considered as a method to discourage Sybil attack. The reputation of any particular service provider can be evaluated through a reputation score or based on the amount of total rating fee. If the reputation system is strong enough when it is deployed into the metaverse, it could help discouraging illegal action in the virtual world efficiently.

In the metaverse, users may hesitate to vote low ratings for other people due to the fear of retaliation from the recipients. Thus, a privacy-preserving mechanism is necessary in this case to guarantee the rights of the voters. The authors in [105] proposed a trustless reputation system that preserves user privacy based on blockchain technology. On the one hand, blockchain technology is used to provide decentralized and trustless properties for the system. On the other hand, that technology is leveraged by ZKP mechanism to ensure user privacy. With the zero-knowledge proofs, voters can completely hide their identity, while the reputation system can still confirm the correctness of the votes. However, a blockchain-based reputation system might suffer from low efficiency due to scalability issue of blockchain. To overcome this problem, the authors in [106] proposed an anonymous reputation system IIoT-Enabled Retail Marketing, in which Ouroboros blockchain consensus mechanism is utilized to provide higher efficiency and security. Besides blockchain, non-interactive ZKP is also used to offer identity anonymity. A proof-of-concept prototype on Parity Ethereum has been conducted to prove the performance of the system.

In a real circumstance, there could be significant conflicts between voters and the corresponding recipients when the reviews are submitted. The authors in [107] proposed to add an arbitrator entity in their IoT data review system to deal with this issue. According to the proposed solution, whenever a conflict occurs between the reviewer and the rating recipient, an arbitrator will validate the data and make a decision. An incentive mechanism is utilized to encourage both users and arbitrators to act honestly. In addition, IBM Watson Tone Analyzer[18], a natural language understanding mechanism using deep learning, is also used to filter out fake reviews. However, this frameworks still requires a third-party authority, which is the arbitrator. Therefore, biased decisions can still be made even when incentive mechanisms are implemented. To truly realize the decentralized metaverse, the intervention of third-party authorities must be minimized or even eliminated completely. Li *et al.* [108] presented a blockchain-based reputation system for e-commerce, *RepChain*, which is privacy-preserving and verifiable without third-party intervention. Specifically, two-move blind signatures are leveraged to create anonymous credentials, thus preventing user identity from being leaked. Furthermore, Zero-Knowledge Range Proof (ZKRP) is used to verify the submitted reviews and detect abnormal reviews. Thereby, the ratings would be more reliable, while the system remains fully decentralized.

Fairness is also a major concern of the metaverse reputation system. Intuitively, the vote of a low-reputation user should have less impact than the one with high reputation score. The authors in [109] 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. As a result, it could further improve the fairness and quality of votes in the system.

D. BLOCKCHAIN FOR SECURE DATA STORAGE AND SHARING

Data storage and data sharing in the metaverse are two critical tasks, playing a vital role within the entire ecosystem. If data in the metaverse are stored in traditional centralized databases, it would be vulnerable to various risks. Firstly, the data are completely controlled by a centralized server, which means that the metaverse organizers can easily modify any data or even use it for malicious purposes. Secondly, when the centralized database is hacked, the attacker could potentially manipulate the network. Finally, data sharing is limited since no one but the metaverse organizers have the right to access the centralized database. For some use cases such as metaverse-based healthcare systems, medical records should be shared among doctors, allowing them to access necessary information of their patients in the reliable and timely manner. For data storage and sharing, blockchain technology offers decentralization, security, immutability and transparency.

However, storing data on blockchains still experiences certain limitations. Firstly, it is extremely expensive. For example, it costs about 4,444$ for storing only 1MB of data on the Ethereum blockchain in 2018[19], the current price would be much higher at the moment. The reason for this high cost is that those data have to be stored by every full node throughout the network. Secondly, querying data from blockchains runs into performance and bandwidth issues as blockchains have no initial query language like regular databases. Such the decentralized nature of blockchain becomes the main obstacle hindering it from being used for pervasive data storage. Several strategies can be deployed, on the one hand, to maintain certain beneficial properties of blockchain in

[18]https://www.ibm.com/cloud/watson-natural-language-understanding

[19]https://medium.com/coinmonks/storing-on-ethereum-analyzing-the-costs-922d41d6b316

data storage, while still addresses its limitations in terms of storage cost and query speed.

1) Consortium Blockchain for Data Storage

The first possible solution is to store data on consortium blockchains instead of public chains. Here, the range of participants is limited so that only those who are selected or authorized can access and control the blockchain [110]. It is different from public blockchains where every one can participate in the network without asking for permission. Using a consortium blockchain could bring the following benefits for data storage in the metaverse:

- **Faster and Lower Cost:** Since the number of participants in consortium blockchains is usually small, the consensus among nodes can be reached faster, thereby improving the processing speed and almost eliminating the transaction cost. This is very important as the operation of the metaverse must be real-time.
- **Flexible:** The architecture of consortium blockchains can be adjusted to fit the purposes of its applications. In this case, the blockchain can be designed only for data storage, while other features such as payment transactions or even the digital currency application could be eliminated. Thereby, the blockchain can be optimized for storing data, allowing massive and convenient data storage.
- **Privacy:** The stored data are only transparent to participants of the blockchain and hidden to the public. Although this means that the transparent nature of the blockchain is sacrificed, it helps guarantee the privacy in certain cases.

It can be used effectively in several circumstances preferring privacy over transparency. In fact, as long as the majority of participants act legally, most important properties of a general blockchain are still maintained, including immutability, security, and certain level of decentralization.

2) Off-chain Data Storage

Another solution for data storage in the metaverse is to utilize off-chain mechanisms. In particular, only the hash of the data or a small part of the data is stored on the blockchain, while the original metadata can be stored by using traditional storage mechanisms. In comparison with the metadata, the hash is very small so the storage cost is low enough for it to be stored on-chain. In this design, certain advantages of blockchain can still be maintained, while we can enjoy the benefits of traditional storage mechanisms including low cost and convenient query methods. At each data accessing instant, we can compute the hash of the metadata and compare it to the corresponding hash stored on the blockchain. This means that the immutable property of blockchain is relaxed to tamper-proof feature, i.e., the metadata could be modified within the database, but everyone can recognize those changes by keeping track of the ledger.

For particular applications and use cases of the metaverse, the level of decentralization and transparency can be adjusted based on different storage mechanisms [111]. In general, options for off-chain data storage in the metaverse include traditional centralized databases, distributed databases, and distributed file systems [112].

- **Centralized database:** Metadata are stored in a traditional database such as MySQL[20] or MongoDB[21]. This solution achieves high querying capacity and low storage cost for massive amount of data. However, it is vulnerable to SPOF. If some of data is lost or modified due to hacking or technical problems, it cannot ever be recovered. Besides, this method offers the low level of transparency since only the central authority can access the data. The role of blockchain here is only to provide non-tampering characteristic so everyone can validate the correctness of the data. For example, Cryptopunks is a collection of NFT on the Ethereum blockchain, consisting of Cryptopunks images stored in a centralized website cache [113].
- **Distributed database:** In distributed databases, the data are repeated across many nodes in different locations. This solves the SPOF issue of centralized database as distributed data enable data redundancy, ensuring the availability of data even when data loss happens in some nodes. Besides, the querying capacity is still high and the cost of storing massive data is relatively low, but it is not as good as in centralized databases according to these two criteria. On the other hand, this storage method is still controlled by a third-party authority and it does not provide data transparency.
- **Distributed file system (DFS):** Similar to the distributed database, DFS also generates data redundancy to address the SPOF issue. However, DFS is not under control of any central authority; instead, it is a peer-to-peer network in which files are stored across the system with certain number of replicas. Thereby, DFS is totally decentralized and transparent just like a public blockchain, while its storage capacity is greater than that due to blockchain. In comparison with database, DFS lacks querying methods. InterPlanetary File System (IPFS) is a popular DFS which is widely used in various use cases. For example, the authors in [114] propose a framework using IPFS to store patient diagnostic reports. In this framework, the hash of every record is stored in a distributed hash table on the blockchain. Patients can easily access their healthcare records by using its corresponding hash.

Table 4 presents a comprehensive comparison between different storage strategies for the metaverse. In summary, each method has its own strength and drawbacks so they must be used appropriately based on particular use cases.

In the metaverse infrastructure, numerous IoT devices collect data from the physical world to reflect it into the virtual world. Managing such the huge amount of data could

[20]https://www.mysql.com/
[21]https://www.mongodb.com/

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

be a big challenge, especially with trust issues of centralized storage system. Li *et al.* [115] proposed a blockchain-based scheme for large-scale IoT data storage. In this design, the blockchain works as a third party to manage data storage and authentication without any trusted server. Moreover, certificateless cryptography is implemented in the design, offering an efficient way to authenticate IoT devices. As a result, the design is proved to be *IND-CCA* secure, and it also achieves traceability and accountability thanks to the blockchain's features.

When data are stored on blockchain, every node on the network must store a replica of the on-chain data to ensure its integrity. However, it is impossible to require all metaverse users to store these massive data when they participate in the platform. This data redundancy issue could be solved thanks to another approach introduced by the authors in [116]. Specifically, the integrity of data is guaranteed by regenerative code technology, which allows the failed data on a damaged node to be recovered by surviving nodes in the network. The proposed framework can reconstruct the original files with real-time performance and offers blockchain-enabled security features.

Healthcare in the metaverse is also a potential domain with a variety of applications such as telemedicine or healthcare education [117]. While many of these applications are based on AR/ VR technology, blockchain-based data storage could also offer many benefits to the metaverse healthcare system. Liu *et al.* [118] proposed a medical data sharing framework utilizing blockchain technology. With a reasonable communication cost which is linearly proportional to the size of data, the framework provides various security and privacy features such as tamper resistance, autonomy, and anonymity. On the other hand, Azaria *et al.* [119] focused on offering medical big data to researchers with an adaptable framework named *MedRec* for medical data sharing. However, storing medical data on-chain leads to unavoidable trade-offs for scalability and operation cost. Xia *et al.* [120] proposed another approach that stores medical data in cloud environments, while blockchain is utilized to control the access of sensitive data. Besides, blockchain-based data storage can facilitate digital twin for the metaverse infrastructure. Huang *et al.* [121] constructed a peer-to-peer network to manage DT data based on blockchain and smart contract. The results show that the network can enhance data sharing efficiency and ensure data authenticity for digital twin of product.

Since metaverse data are from various sources, data ownership must be guaranteed to ensure the benefits of metaverse participants. The authors in [122] proposed an auditable IoT data storage and sharing scheme utilizing blockchain for data management. In this scheme, besides the storage layer, a data access control layer based on blockchain is integrated to the system to protect data ownership of users. On the other hand, cloud storage is used for blockchain off-chain storage to offer higher storage capability. However, cloud storage might lead to data integrity problem if data are altered in the storage environment. To tackle this problem, the authors in [123] proposed a blockchain-based data storage for IoT data without relying on third-party authority. In the proposal, a dynamic data verification scheme is implemented to ensure data integrity. A prototype of the system is also constructed to prove its high performance and feasibility.

In terms of metaverse software applications, blockchain data sharing can be used as a software connector with enhanced security properties. Xu *et al.* [124] proposed a blockchain-based connector for software services in which a blockchain layer is constructed as a a decentralized trading market for data sharing. There are also many other metaverse applications that can be empowered by blockchain-based data storage such as virtual insurance, virtual real estate, and education [20], [125], [126]. Thus, the role of blockchain for data storage and data sharing infrastructure of the metaverse is undeniable.

E. BLOCKCHAIN FOR METAVERSE INTEROPERABILITY

During the early development phase of the metaverse, there are various metaverse platforms constructed by different organizations and companies which come with different ideas, features, and visions. Virtual worlds created by different companies seem initially lack connectivity and interaction with each other. Moving towards the next development phase, different virtual worlds would gradually connect to each other [16], thus allowing users to participate in different metaverses using a single identity. However, one critical challenge for a global multi-metaverse platform is to find a way to encourage different metaverse companies, including the giant ones, to collaborate and connect their metaverses together. Meta claimed that the metaverse should not be owned by a single company, instead, multiple organisations, developers, and creators will jointly build the metaverse [127]. In other words, collaborations among multiple companies to build a global metaverse are possible in the future.

According to two metaverse-related standards, which are ISO/IEC 23005 standards for Interfacing with Virtual Worlds [128] and IEEE 2888 standards [129], the virtual world would not be a single entity. Instead, there will be multiple virtual worlds (i.e., multiple sub-metaverses) connect

to each other, and each of them possesses different sets of characteristics to be optimized for specific purposes. To this end, blockchain interoperability is an important feature of the metaverse where blockchain-based solutions can be developed for secure data sharing between different sub-metaverses [130]–[132].

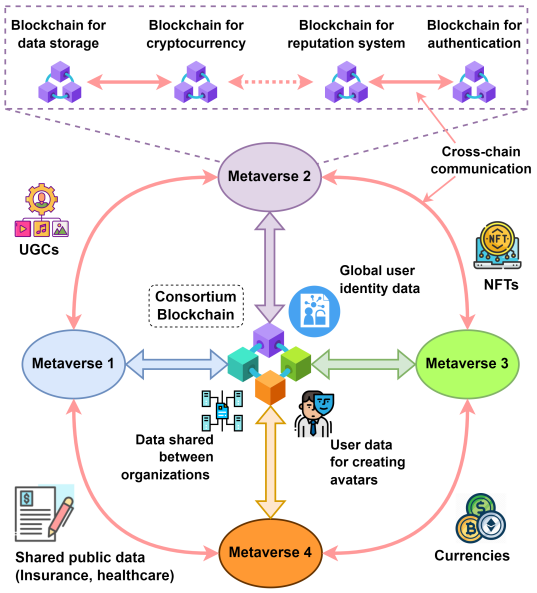

FIGURE 7. The global multi-metaverse architecture. From the system perspective, different metaverse companies could share necessary data with each other through a consortium blockchain. From the user perspective, all users could connect to different metaverses and send virtual assets, currencies across platforms through cross-chain bridges.

On the other hand, it is challenging if not impossible to design a single blockchain network that could handle all desirable applications in a sub-metaverse. Instead, there should be multiple blockchains deployed in each sub-metaverse, in which each blockchain is optimized for certain applications. Due to the well-known blockchain trilemma [22], if a blockchain is optimized for some specific properties (e.g., decentralization), other properties (e.g., scalability) must be sacrificed to a certain extent. Therefore, it is more likely that there will be multiple blockchains operating within each particular metaverse, and each blockchain is optimized only for its specific purposes. For instance, a blockchain for metaverse virtual currency should be optimized for scalability and confirmation speed to improve user experience. However, according to the blockchain trilemma, such the blockchain must sacrifice certain level of decentralization to achieve that requirement. On the other hand, a blockchain for metaverse voting system must maximize decentralization and transparency to ensure that all decisions are fair and democratic once they are released. However, confirmation speed could be sacrificed partly since it is not an important factor in this case.

[22]https://medium.com/certik/the-blockchain-trilemma-decentralized-scalable-and-secure-e9d8c41a87b3

Fig. 7 presents an envisioned version of the interoperable metaverse, in which there are multiple sub-metaverses, while in each sub-metaverse, there are also different blockchains for specific purposes.

In that scheme, cross-chain mechanisms could be utilized to allow different blockchains within a particular metaverse, and blockchains in different metaverses to communicate with each other. Thereby, users can send their virtual assets such as UGCs, NFTs, and currencies within and across metaverse platforms [133]. Public data such as insurance or healthcare information can also be shared between metaverses by these cross-chain bridges [134], [135].

Furthermore, different metaverse companies could participate in a consortium blockchain to share certain data in a decentralized manner. This consortium blockchain includes various data that must be shared to construct digital avatars, validate user identity, and provide different virtual services. By this way, a user can appear in different metaverses without repeatedly registering a different identity for each platform. Besides, users do not have to go through sophisticated procedures multiple times (e.g., scanning appearance and providing personal information) since those data are all shared among metaverse organizations. Since consortium blockchain cannot be access by the public, it guarantees user privacy, while still maintains the decentralized property.

When applying blockchain interoperability on the metaverse, a common standard is necessary to minimize potential conflicts between platforms and reduce development cost. The authors in [136] proposed an interoperable blockchain architecture, inspired by the design philosophy of the Internet. Its goal is to define a standard for common components of a blockchain interoperability system, thereby making cross-chain communication more reliable with lower cost. However, this means that all blockchains integrated in the metaverse must be constructed from scratch to follow to the proposed design, which might cost enormous monetary and human resources. To overcome this issue, the authors in [135] proposed another approach for blockchain interoperability that works directly on the application layer, meaning that every blockchain can use this solution as long as it supports smart contract. Specifically, there is an incentive mechanism in which if users act dishonestly when the cross-chain communication is made, they will lose more money than the amount they earn from the dishonest action. Thereby, the metaverse could utilize current prominent blockchain platforms instead of having to build a new blockchain system from the beginning.

In fact, most studies on blockchain interoperability focus on public blockchain (i.e., permissionless blockchain). Section IV-D shows that consortium blockchain (i.e., permissioned blockchain) is also a suitable option for the metaverse in many use cases, thus interoperability of permissioned blockchain is also necessary. To this end, the authors in [131] designed a novel infrastructure to solve the interoperability of permissioned blockchain. Thereby, a permissioned blockchain can connect to other permissioned ones, and also

to public blockchains. Experiments have been carried out between Hyperledger Fabric and Ethereum blockchain to prove the feasibility of the proposed architecture.

Interoperability implemented with blockchain gateways could suffer from crashing, making the system unstable. Belchior *et al.* [132] proposed Hermes, a middleware framework for blockchain interoperability that offers crash-recovery features based on the Open Digital Asset Protocol, thereby ensuring the assets are consistent between the source and recipients.

While transferring asset across metaverses is the major task, interoperability of programmable smart contracts is also important for the metaverse. Liu *et al.* [137] proposed *HyperService*, a framework offering programmability across heterogeneous blockchains. This allows users to build cross-chain decentralized applications, which are crucial in the metaverse. In terms of metaverse applications based on interoperability, Dagher *et al.* [138] proposed a blockchain-based framework for electronic health records with interoperability and advanced security features. The framework use smart contracts and cryptographic techniques to protect patients' sensitive information. To further enhance security of blockchain interoperability, Malavolta *et al.* [139] proposed a framework offering security for payment-channel networks based on anonymous multi-hop locks. Remarkably, security features in the framework are totally provable.

F. LESSONS LEARNED

Table 5 provides a summary of literature reviews on different blockchain-based applications of the metaverse from the system perspective. It is obvious that blockchain could enable a wide range of applications and improve the metaverse in different ways.

1) Metaverse Governance System

Virtual world governance can be benefit from blockchain technology in various aspects. Firstly, blockchain is a key component of the SSI system using in identity and authentication management. The SSI system guarantees user privacy by eliminating the need to store personal data on decentralized databased and giving users the right to choose what information to share. Secondly, blockchain DAO allows a democratic voting scheme where all users have a voice in determining how the virtual world operates and evolves. Finally, blockchain technology can be used to construct the metaverse reputation system, where each user is assigned a reputation score illustrating their credibility in the virtual world. While metaverse users could rate others after receiving any products or services, these ratings can be stored on blockchain as transactions to ensure transparency and fairness.

2) Blockchain-based Metaverse Infrastructure

Blockchain can offer the metaverse various data storage methods with different level of decentralization and privacy. Although storing data on public blockchain is the most decentralized method, it is not an appropriate solution in most cases since the storage cost is too high. Therefore, on-chain storage is only implemented on consortium or private blockchain, where the storage cost is significantly lower and privacy takes precedence over decentralization. For public blockchain, off-chain storage can be used with centralized databases, distributed databases or distributed file systems to adjust the trade-offs between different factors such as decentralization, storage cost, transparency, data redundancy and querying capacity. In brief, while off-chain storage using centralized databases is the fastest and cheapest solution, distributed file systems such as IPFS, on the other hand, offer the highest level of decentralization for blockchain storage. Besides blockchain-based data storage, cross-chain mechanisms and multi-chain platforms can enable metaverse interoperability, allowing different metaverse platforms communicate and interact with each other seamlessly.

V. BLOCKCHAIN REVOLUTIONIZES METAVERSE DIGITAL ASSET MANAGEMENT

This section describes the roles and potentials of blockchain for digital asset management in the metaverse. To track the evolution of digital assets over time, we consider the three development phases of metaverse. The earliest development phase was stimulated by MMO games where some simple concepts of metaverse were introduced for the first time. The second phase, called metaverse 1.0, was inspired by the popular game platform Second Life when the term "metaverse" appeared and key aspects of this virtual world started receiving growing interests from the community. The next development phase, refereed to as metaverse 2.0, is empowered and revolutionized by the blockchain technology. In the following, we discuss different technical and social aspects of the digital assets and present the 8-stage digital asset management workflow for the future metaverse.

A. DIGITAL ASSET OWNERSHIP

In early platforms appearing in the first development phase like MMO games, the entire virtual world is created by professionals such as developers, designers, and artists. Therefore, users mostly follow a gameplay that has already been arranged, and it does not encourage much user innovation and creativity. In this type of virtual world, both assets and currency are completely controlled by game providers, while users have no rights of ownership. On the other hand, game publishers usually allow users to create items by spending in-game raw materials collected during their playing process. By regulating the scarcity of these raw materials, game providers could entirely control the value of each item in the platform.

When Second Life was published, there was a huge breakthrough in terms of digital asset ownership as Linden Lab announced that they grant users the IP rights for their creations [140]. This means that users are the owners of everything that they create. This property rights is guaranteed by real-world IP laws. Although the IP rights grant users the ownership for

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

Application	Ref.	Issue	Proposed Solutions	Technology
Identity and Authentication System	[88]	Lack of systematic design and patterns	Propose 12 design patterns, classified into 3 categories. Facilitate further development of SSI systems.	Blockchain, SSI, IPFS
	[89]	Privacy threat to authentication system	Store personal information on user devices instead of databases. Data are signed using RSA digital signature.	SSI, RSA digital signature
	[91]	Lack of user-friendly identity framework	Provide metaverse users a convenient application that is integrated with SSI wallet and uses QR code.	Blockchain, SSI
	[92]	Data integrity and availability issue	Nodes in the system are divided into different zones. Nodes within a zone can identify and trust each other.	Blockchain
	[93]	Performance and security limitations	Construct a hierarchical network based on node's capability to optimize efficiency and provide mutual authentication.	Local, public blockchain
	[90]	Risks from malicious and unauthorized users	Blockchain is used to eliminate single root of trust and protect the system from malicious actors.	Blockchain, IoT
Metaverse Democratic Voting Scheme	[97]	Security threats in centralized platforms	Utilize blockchain to facilitate polling process, thereby offering anonymity and various security features.	Blockchain
	[98]	Voter privacy leakage	Eliminate the role of third party to ensure privacy with ZKP.	Blockchain, ZKP
	[99]	Performance and scalability limitation	Investigate the trade-offs of blockchain-based voting system in various scenarios to optimize performance and scalability.	Blockchain
	[104]	Risks of immutability	Design a withdrawal model to allow the change of votes.	Blockchain
	[101]	Quantum attacks	Utilize code-based Niederreiter to prevent quantum attacks.	Niederreiter code
	[103]	High cost of massive voting system	Optimizing the hosting cost of blockchain-based voting system in a nationwide scheme.	Blockchain
Metaverse Reputation System	[105]	Privacy threat to reputation system	Leverage ZK proofs to hide user identity when rating. Utilize blockchain to provide decentralization and trust.	Blockchain, ZKP
	[106]	Low efficiency and scalability	Boost efficiency by utilizing Ouroboros consensus protocol. Provide anonymity thanks to non-interactive ZKP.	Blockchain, non-interactive ZKP
	[107]	Conflicts between reviewers and recipients	Add an arbitrator to resolve conflicts between participants. Use IBM Watson Analyzer to filter out fake reviews.	Blockchain, deep learning
	[108]	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
	[109]	Fairness of rating	Calculate reputation score based on a weighted formula.	Blockchain
Metaverse Data Storage and Sharing	[115]	Trust issues of centralized storage	Large-scale data storage is managed by blockchain. Certificateless cryptography for device authentication.	Certificateless cryptography
	[116]	Data redundancy issue of blockchain	Allow failed data on damaged nodes to be recovered by surviving nodes using regenerative code.	Regenerative code, blockchain
	[118]	Privacy issue of medical document	Use blockchain for storing medical records to provide tamper resistance, autonomy and anonymity.	Blockchain
	[119]	Medical big data	Utilize blockchain data storage to offer medical big data.	Blockchain
	[120]	Off-chain medical data storage issues	Store medical data in cloud environments, while blockchain is used to control access of medical records and logs.	Blockchain
	[122]	Data ownership issue	Integrate a data access control layer on top of storage layer to protect data ownership.	Blockchain, cloud storage
	[123]	Data integrity problem	A dynamic data verification scheme is implemented to protect data integrity, without intervention of third party.	Blockchain, DFS, cloud storage
	[124]	Decentralized software data sharing	Construct a blockchain-as-a-connector framework for software data sharing based on smart contracts.	Blockchain
	[121]	Data management issues of digital twin	Propose a secure network for DT management based on blockchain transactions and smart contracts.	Blockchain, DT
Metaverse Interoperability	[136]	Lack of standards	Define common standards for blockchain interoperability.	Blockchain
	[135]	High development cost	Allow interoperability directly on the application layer.	Smart contract
	[131]	Lack interoperability of permissioned blockchain	Enable interoperability between permissioned blockchains and permissionless blockchains.	Hyperledger Fabric
	[132]	Gateways crashing	Design blockchain gateways with crash-recovery strategy.	Blockchain gateway
	[137]	Lack interoperability of smart contracts	Construct a framework that offers programmability across different heterogeneous blockchains.	Blockchain, DApp
	[138]	Privacy issue of medical record interoperability	Utilize blockchain to offer interoperability of health records. Privacy, security are ensured by cryptographic techniques.	Blockchain, cryptography
	[139]	Provable security	Design an interoperability framework with provable security.	Multi-hop locks

their digital assets, the virtual world providers could change their policies and ToS so that they can refuse to grant users the property rights. In this case, digital assets created after the introduction of the new policies could become the assets of the virtual world providers. In other words, the ownership policy of digital assets is still under the control of the virtual world providers.

In the last few years, many metaverse platforms integrating the blockchain technology have emerged where the blockchain helps address various technical challenges in digital asset ownership. In particular, users can prove their ownership of virtual items through NFTs [141]. With blockchain and NFT, users can completely own their creations regardless of the platform's policies.

B. ECONOMIC AND CULTURAL ISSUES

1) Trading Digital Assets

Many traditional platform like MMO games discourage or even ban trading virtual items for real-world currency [142], [143]. If users could trade digital assets with each other, it might negatively impact the revenue of the game publishers because some users would choose to buy items from the market rather than from the publishers. However, users can still trade virtual items on black markets and there is always a need for trading digital assets. Future virtual worlds should contain a free market where digital assets are treated as real commodities and could be traded freely among users.

When it comes to the metaverse 1.0 inspired by Second Life, users are allowed and even encouraged to create and trade virtual assets with each other. The virtual world provider, Linden Lab, even created virtual banks and websites allowing users to exchange virtual currency for real-world currency [144]. This means that users can truly earn capital gain and transfer virtual wealth into real-world wealth. However, the exchange rate is decided by Linden Lab as they control the total supply of virtual currency. The virtual economy, therefore, depends greatly on the trust of users in the publishers. If the publishers, for some reasons, generate massive amount of virtual currency, thereby decreasing the value of both digital assets and currency, the benefit of users might not be ensured. Hence, it is desired that the next-generation metaverse should be decentralized and trust-less so that no party could unilaterally control the virtual economy created by the platform.

The birth of blockchain technology marked a new milestone in the development of next-generation metaverses as it solves the mentioned centralized issue. In particular, most important blockchain networks such as Bitcoin and Ethereum employ distributed mechanisms (i.e., concensus algorithms) for cryptocurrency issuance and data storage; as a result, the value of virtual currency and digital assets will not depend on any single authority. Instead, it is determined by the free market. This makes the metaverse an ideal environment for creativity and innovation, where creators could create real wealth through the virtual world.

2) Digital Asset Quality and Cultural Issues

Digital asset management strategies in use could strongly impact the quality of underlying assets. In traditional MMO games, assets in the virtual world are created by professionals who are designers, developers, and artists. Therefore, the quality and cultural factors are usually taken into consideration as new content is often moderated thoroughly before it is released into the virtual world. When it comes to the metaverse, the main creators of digital content are its users. When users have the freedom to create and upload digital content/assets, some of the contents could have poor quality or they can even be illegal and offensive [145]. Furthermore, it might cause conflicts such as violation of cultural norms of certain countries or religions since the metaverse is published globally and they can be accessed from many countries [146].

3) Digital Asset Taxation

When virtual wealth can be translated into real-world wealth, taxation is inevitable for the metaverse. In traditional platforms like MMO games, users mostly trade virtual items with each other through unofficial channels, so it is almost unenforceable for taxation to be applied. On the other hand, metaverse platforms usually allow users to trade virtual assets freely and legally. It is designed to promote commerce and even to provide an official source of income. For taxes to be applied in the metaverse, the virtual platform should be constructed properly; otherwise, it may be unenforceable or it could even discourage users from participating in the platform. There are two opposing viewpoints regarding taxation in the virtual world, which are refereed to as internal and external viewpoints in the following [147]:

- **Internal viewpoint:** Virtual currencies should be treated as cash equivalents, and transactions in the virtual world can be considered separately. Therefore, taxes must be applied to transactions related to trading digital assets.
- **External viewpoint:** Virtual currencies have no real-world value until they are exchanged for real-world currency. Therefore, taxes should only be applied when users convert virtual currencies to a traditional currency such as US dollars and it is considered as a source of income.

The internal viewpoint could prevent the virtual economy from large-scale tax evasion and unfairness in taxation since tax is applied to every transaction, including intermediate exchanges. However, it faces difficulties in enforcement, as the metaverse is a virtual world where users are anonymous, thus tracking transactions of every user is very difficult or even impossible. On the other hand, the external viewpoint is more enforceable as it is easy to recognize user income when they exchange virtual currency for real-world currency. Besides, only the companies that take responsibility for exchanging virtual currency for real-world currency collect the sales tax. However, as mentioned above, it is more vulnerable to tax evasion when intermediate transactions in the virtual

world are not taken into account. Each viewpoint has its own strengths and weaknesses, and these trade-offs should be considered carefully to design a tax policy for the metaverse. In fact, taxation for cryptocurrency is still a debating topic in most countries [148]. For example, businesses in Singapore must pay tax on the profit made from trading cryptocurrency, while tax residents in Dubai pay no tax for their personal income, including income from cryptocurrency [148].

C. DIGITAL ASSET MANAGEMENT WORKFLOW

As metaverse users are encouraged to create and trade digital assets in a free market, there is a need for a digital asset management system that facilitates this trend, guarantees the rights of users, and protects the platform from bad content. In this section, we propose the 8-stage workflow for metaverse digital asset management integrating the blockchain technology as shown in Fig. 8. Specifically, users first create digital assets based on their ideas. Then, the created assets are classified into appropriate categories and reviewed by professionals or other users who have knowledge in the underlying fields. After a digital content is accepted, it is stored in a database or IPFS and protected by suitable strategies such as IP laws, watermarking, fingerprinting or NFT tokenization. Finally, it is evaluated before being distributed to the market.

1) 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. For example, users in Second Life could use tools like Blender[23], a free and open-source 3D computer graphics software toolset, to create virtual content. This tool is also used widely for content creation in other platforms such as Decentraland. Maya[24] is another popular 3D computer graphics application which can be used to create virtual content in the metaverse. Maya is more suitable for large-scale production compared to Blender as it has been the industry standard for years in 3D modeling and animation. While Decentraland allows users to create virtual items using external tools such as Blender and Maya, the SandBox developed their own 3D editing tool, VoxEdit[25], that enables users to create voxel assets which are used in this metaverse as equipment for user avatars.

During the content creation process, blockchain could enable a shared development environment, where multiple creators create/contribute to a particular digital content. Thanks to smart contracts and consensus algorithms, different creators could reach agreement in customizing the product. For example, the authors in [149] introduce 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 lesson/topic is created, any approved participant could propose adding customized content to the topic through the blockchain-based framework. New additions are accepted only when the majority of network nodes reaches a consensus in approving the content. 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 [150] 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, which is the original content. Moreover, the child content could also have its own child branches, thus forming a tree-like model in content creation process. As a result, users can easily trace back to the source version of the content from any branches. After being created with specific tools, digital contents are normally stored as digital files, which could be imported into the metaverse for use or sold on marketplaces.

2) Digital Asset Classification and Reviewing

The digital world could be affected negatively in both legality and social acceptance if there are many illegal/offensive digital contents available in the platform. To address this issue, it is crucial to construct a reviewing/auditing strategy that can efficiently filter out illegal/bad contents before they are distributed in the virtual world. To this end, a blockchain-based mechanism with Proof of Authority (PoA) is such a suitable solution to meet these requirements. PoA is a consensus algorithm in which validators are chosen based on their reputation [151], i.e., those with higher reputation are more likely to be chosen as validators. If validators follow the rules and complete their work appropriately, they will earn certain financial reward and reputation score as an incentive mechanism. Otherwise, they can be punished if they act maliciously, e.g., accepting invalid transactions. Besides, every digital content must go through a classification stage before the reviewing process to ensure that it will be reviewed by appropriate reviewers [152]. This reviewing process could create a source of income for reviewers and it can be treated as an official job when the metaverse is accepted widely.

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 selected validators. Validators are chosen based on their reputation scores, which are updated regularly by a credibility scoring system. Then, validators rely on data/documents submitted by news organizations to decide the eligibility of each news. If a consensus is

[23]https://www.blender.org/
[24]https://www.autodesk.ca/en/products/maya/
[25]https://www.voxedit.io/

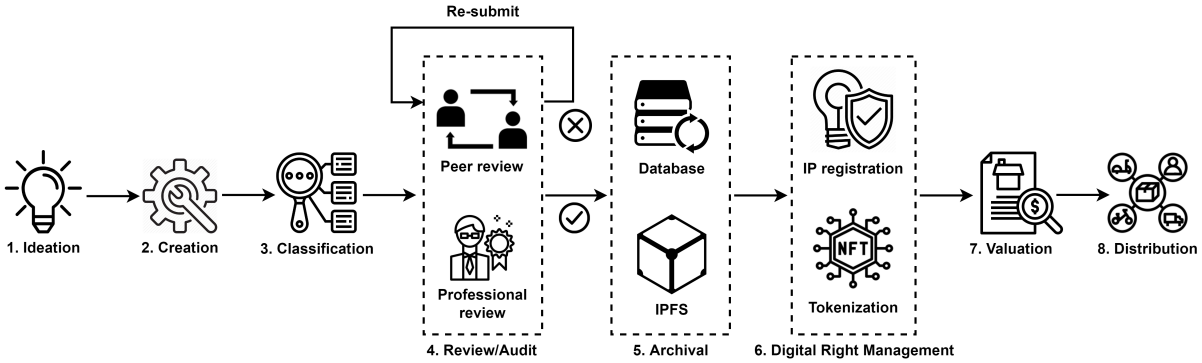

FIGURE 8. The 8-stage digital asset management workflow in the metaverse.

reached and the news is approved, a transaction containing the news is committed into the blockchain. Otherwise, the news considered as fake news and its publisher is punished by reducing his/her reputation score.

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 instead of only news like in above system. In particular, a comprehensive decision making strategy is necessary to decide whether to accept a digital content in the metaverse. The authors in [154] propose 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. Especially, each vote has a particular weight depending on the distance between the domain of the problem and the experience/expertise of the voter. The system was implemented on the Quorum network [155], while smart contracts are simulated using Remix IDE[26], and Truffle[27] is used for authentication. 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].

3) Digital Asset 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. To this end, we define two types of digital asset 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. Other techniques such as digital watermarking could also be employed as a proof of ownership for the asset [156].
- **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 [157].

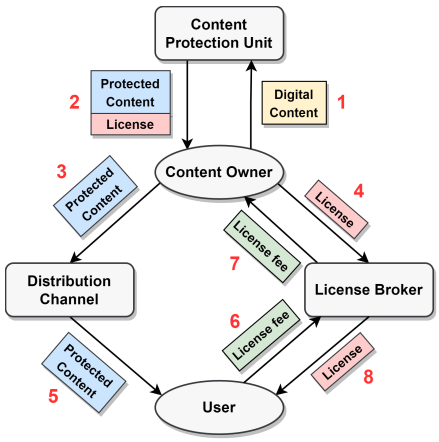

FIGURE 9. A typical digital rights management system [156].

DRM for access-based digital assets. For access-based digital assets, storing files in centralized databases such as a cloud storage is a suitable solution, since it is convenient to access/query the files and it is easy to define and enforce access-control rules/policies. A typical digital rights management system for this type of asset is presented in Fig. 9. Firstly, UGC is sent to a content protection unit, which takes responsibility for encoding the content in a Rights Expression Language (REL) and inserting a digital watermark and fingerprint. Then, the encoded content and its corresponding license are sent back to the content owner [156]. The owner sends the protected content to distribution channels, e.g., a digital marketplace, so that other users could retrieve the content widely. Meanwhile, the license is sent to the license broker, a trusted clearinghouse, to handle access requests from users. If a user wants to access the digital

[26]https://remix-project.org/
[27]https://trufflesuite.com/

content, she must pay a license fee to request the license, which could be used to decode the protected content. Then, the license broker can send the proceeds back to the content owner.

DRM for access-based digital assets could also be facilitated by using blockchain for access control. In this case, blockchain technology can provide a decentralized environment for the authorization process and access management, thus making the progress verifiable, transparent, and reducing the intervention of third parties. Yan Zhu *et al.* propose a distributed permissioned system using blockchain and Attribute-based Access Control [158] (ABAC) model for digital asset access control [159]. In this system, there are five ABAC components which are Policy Enforcement Point (PEP), Policy Decision Point (PDP), Data Depository Server (DDS), Policy Depository Server (PDS), and Attribute Grant Unit (AGU). Every digital content is stored in DDS, which is often a cloud storage. If a customer wants to access a digital content, she must send a registration transaction on the blockchain. This is a multi-signature transaction[28] that needs four signatures from the PEP, PDP, AGU and DDS to be valid. When the transaction collects enough signatures, the blockchain network accepts it and the customer is granted access to the digital content. In comparison with the above traditional DRM model, this system is more automatic, decentralized (with blockchain), and flexible (thanks to the ABAC model, as DRM policies could be adjusted dynamically in the PDS). However, it requires intensive communication between different components and additional blockchain transactions [160], which could significantly increase the operation cost and complexity of the system compared to traditional designs [161].

DRM for unique digital assets. For unique digital assets, tokenizing them into NFTs is a great option compared to other traditional techniques such as watermarking or fingerprinting. This is to prove the ownership of digital assets in a decentralized fashion, meanwhile allowing everyone to track its creator and history freely. However, storing NFT data on a centralized server is not a smart strategy as it eliminates most advantages of NFTs. Firstly, if the admin stops maintaining the server, all data of the NFT might disappear forever, causing the NFT blank. Furthermore, the admin could also change the NFT data without the owner's permission. Therefore, storing NFT data using decentralized file storage techniques like IPFS is a better solution granting metaverse users the true ownership. It not only ensures the permanence of data, but also prevents 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 (see Fig. 10). 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

[28]https://en.bitcoin.it/wiki/Multi-signature

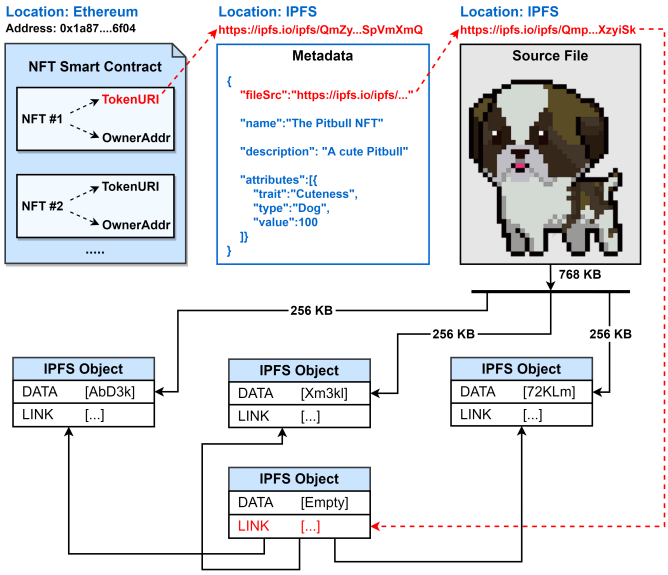

FIGURE 10. Tokenize digital assets to NFTs and store on IPFS.

of the source file. Then, a metadata file is created and stored in IPFS in a similar way, containing necessary information about the digital asset such as name, description, attributes, and of course, the link to the source file. Finally, users could mint a new NFT by calling the "mint" function of a specific ERC721 smart contract, where the argument "TokenURI" is such the link to the metadata which had been created in the previous step. However, files are immutable in IPFS so that it is more complex for version control compared to traditional storage methods since new files cannot overwrite the older ones. For version control, IPFS use the Git system. Whenever a new version of a file is generated, a new commit object is created and it points to the previous commit object of the file.

In summary, different storage and digital rights management strategies could be deployed depending on the specifics of digital assets. An access-based digital asset should be stored in a centralized database for more convenient and faster access, while third parties in the traditional digital rights management system would help manage and distribute the product to other users. On the other hand, other assets preferring uniqueness and ownership protection should be tokenized as NFTs and stored in IPFS. Besides, users can register IP rights for their digital content so that their assets are protected by not only technical mechanisms, but also real-world laws.

4) Digital Asset Valuation

After storing digital assets using an appropriate storage method and applying suitable strategies to protect the rights of the creators, 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 [162], 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.

Moreover, the price of a digital asset could be affected by amortization since its value can be volatile over time as the scarcity could be decreased as more users have access to it. For digital asset valuation, blockchain could help in recording the measurement of properties for digital assets. In a tamper-proof, distributed, and transparent storage environment offered by blockchain, internal and external stakeholders could fairly participate in the valuation process [162]. However, the storage cost of blockchain is usually greater than that of traditional storage solutions, while it is less convenient for reading data as blockchain has no querying methods. 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 [162]. On the one hand, this eliminates the role of centralized third parties, thus optimizing the profit of these platforms and countering possible 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 showing its lack of flexibility.

In addition, it has been shown that fluctuations in the value of cryptocurrencies could impact greatly the value of NFTs [163]. This implies the fairly high correlation between virtual currencies and other types of digital asset in the metaverse. For a blockchain-based economy in the metaverse, the valuation of cryptocurrencies used in the platform is also a crucial factor to valuate metaverse digital assets in general. Existing research works [164] suggest that although there are fundamental differences between traditional assets and emerging digital assets, traditional valuation methods could still be a good starting point for valuation and analysis of new digital asset classes [165]. Specifically, there are several traditional approaches to assess the fair value of a business and its stock such as the Market Approach [166] and the Discounted Cash Flow (DCF) Model [167], which are described in the following.

Market Approach: This is a valuation method that derives the value of an asset by examining the price of similar assets which have recently been sold. For business, the value of a company is estimated based on the comparison between the company and its peer companies in different aspects such as earnings, cash flow, and growth profile. These examinations often rely on the price to earnings (PE) ratio [168], which shows what investors are willing to pay today for a stock depending on its past and/or its future earning. For cryptocurrency-based digital assets, it remains a question if one can propose a metric similar to the PE ratio.

If cryptocurrency is considered to be a medium of exchange, the Equation of Exchange [169] in traditional macroeconomics could be a proper starting point to explore the value of this new type of currency:

$$MV = PT,$$

where M is the total supply, i.g., the total number of tokens, V is the velocity of money, which is the average frequency with which a token is spent, and P is the price level [170], which presents the overall price for a set of goods and services. In other words, it is the inverse of the price of token/currency [171]. Moreover, T denotes the total transaction volume each day. We replace $\frac{1}{P}$ by C, which is the price/cost of the token and replace $\frac{1}{V}$ by H, which is the average time a token is hold by a user. Then, we have:

$$H = \frac{MC}{T}.$$

At first glance, a high value of H could imply investors are expecting the high growth of the token as they hold on to it for a long time. Deeper analyses do reveal the similarity between this H metric and the PE ratio, which also shows the expectation of investors in the growth rates of a stock/company. It is obvious that MC is the Network Value (the Market Cap), so $H = \frac{MC}{T}$ is also the Network Value to Transaction Volume ratio. Willy Woo and Chris Burniske first present the idea of a PE ratio for cryptocurrencies [172], the NVT Ratio (Network Value to Transactions Ratio), which is such the H metric mentioned above. Different studies have been carried out to show the relationship between the NVT ratio and the network's value. A high NVT ratio implies a high speculative value and bubbles [172], while a low NVT does not necessarily mean that the token is under-valuated but it may indicate that the network is overused by speculators [173]. In other words, if the price of a token commences to rise, people tend to hold it (leading to higher H or NVT ratio) and expect that it is more profitable compared to other tokens. On the other hand, the price of a token is lower when more people try to sell it with high transaction volume, implying speculation [174].

The authors in [172] use the NVT ratio to show two Bitcoin's historic bubbles in 2011 and early 2013. In these years, Bitcoin's price exploded followed by NVT metric peaking above the normal values. These NVT ratios could imply bubbles, and Bitcoin's price indeed decreased 92% and 83% subsequently. Another example is the first rapid price rise in 2013 with 83% consolidation from peak to trough ($258 and $45). Despite the rapid rise, the NVT ratio did not signify a bubble as the transaction volume was high enough to keep the ratio within normal range. Indeed, although the price fells 83% off the peak, it recovered shortly after, indicating a normal price consolidation.

Discounted Cash Flow Model: The DCF model can be used to value a business in the present based on expectations of its future cash flows. The DCF model can be expressed as follows:

$$PV = \sum_{i=1}^{n} \frac{CFi}{(1+r)^i} + TV,$$

where PV is the present cash flow value [175], CFi is the cash flow at the end of year i, n is the number of years in the future, r is the discount rate of return[29], and TV is the terminal value. The discount rate suggests that the future cash flows must be discounted due to the risk of cash flows and the time value of money, i.e., one dollar of the next year is not worth the same as one dollar at the present.

If we consider digital asset valuation merely to determine the value of a digital asset at a given time, the DCF model does not seem to be an option as there is no sense of future cash flow. However, there are many digital assets that do return cash flows to their token holders through staking or contributing works to the network, e.g., staking cryptocurrency in a PoS network to become minter and earn minting reward. In other words, while the Market Approach with the NVT ratio is only applicable for digital assets used as medium of exchange, the DCF model is an appropriate valuation method for more complex cases where digital assets truly generate future cash flows.

The author in [173] use the DCF model to valuate the fair price of REN token, an Ethereum token of the Republic Protocol[30]. Firstly, a discount rate $r = 0.4$ is chosen based on different financial markets, while the cash flows for five consecutive years are taken from a report for a bull case scenario[31]. The Terminal Value is then calculated through the Gordon Growth Method with an estimated growth rate $g = 0.2$. After that, TV is added with yearly cash flows to calculate the final PV value which is approximately $4.7B. Finally, by dividing the network value PV by the number of tokens which is nearly 520 thousand tokens in circulation, the REN token is valued at $9.05 according to the DCF method.

5) 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 may be distributed in different channels based on their attributes.

Access-based digital asset distribution. For access-based digital assets, which could be accessed by different license owners, they should be stored on centralized databases for more convenient distribution. In traditional models, the process involves certain third parties such as distribution channels and license brokers as presented in Section V-C3. These third parties help creators distribute their assets widely to the market, but there must be a certain level of trust from the creator to the third parties. Furthermore, creators should have to share their profit with these third parties at certain rates depending on specific platforms.

Blockchain technology could make the distribution process more decentralized by eliminating a role of the middlemen. Specifically, smart contracts could take responsibility for controlling the payment process and granting customers keys or licenses to access digital products. For instance, the authors in [176] 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, the following process must be completed. Firstly, she sends a request to an administrator smart contract through a transaction. This transaction also includes the payment for purchasing the license. After receiving payment, the smart contract gets a session key and the hash of the content from the content owner then sends them to the customer. With the session key, the customer could download the image from the cloud storage, and then use the hash to verify the image that she has received. If the hashes do not match with each other, the image has been modified in the cloud storage and the customer could report the mismatch to the smart contract and receive her fund back. All transactions during this process are recorded on the blockchain and therefore, they are permanent and auditable.

Unique digital asset distribution. For unique digital assets tokenized as NFTs, they can be distributed on NFT marketplaces to take advantage of the decentralized property. The structure and operation of a typical NFT marketplace is presented in Fig. 11.

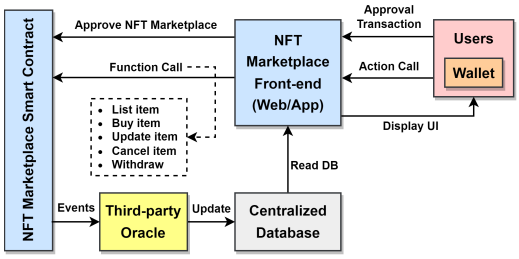

FIGURE 11. Structure and operation of a typical NFT marketplace.

While the back-end of the marketplace is actually a smart contract on the blockchain network, its front-end is often a website or an application. Since blockchain storage is not similar to traditional databases with query methods, the dApp still needs a centralized database like MongoDB to update every change of the smart contract in real time so that the front-end could query these data conveniently from the database. For connecting to the smart contract, a third-party oracle [177] is needed to listen to every event emitted by the smart contract. When a user wants to take an action such as listing an NFT for sale, she must first approve the NFT marketplace smart contract through a special approval

[29]https://www.investopedia.com/terms/d/discountrate.asp
[30]https://renproject.io/
[31]https://medium.com/greymatter/republic-protocol-analysis-and-valuation-e73fab4c32fc

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 smart contract and specifies the address of the ERC-721 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 such as Moralis[32] or Alchemy[33] so that the new item could be updated to the centralized database. Other actions such as buying an item, updating item's price, canceling an item or withdrawing funds from the marketplace, all following the above process. Although NFT marketplaces are constructed based on blockchain and smart contracts, the above process suggests that they still need third parties and certain trust assumptions [177]. To enhance the decentralized capability further, most oracle platforms also operate in a distributed fashion with different nodes and specific incentive mechanisms [178], [179].

VI. METAVERSE SECURITY, PRIVACY, SOCIAL, ENERGY AND ENVIRONMENTAL CONCERNS

In this section, we analyze the metaverse security, privacy, social aspects as well as energy and environmental concerns. On the one hand, with literature surveys on the most up-to-date studies, we investigate the potential use cases of blockchain to address these issues. On the other hand, we also discuss the drawbacks of blockchain for those aspects (e.g., environmental and social issues), thereby finding possible solutions to limit these disadvantages. Table 6 provides a summary of these issues and the corresponding solutions with comprehensive literature reviews.

A. SECURITY ISSUES

The metaverse can be envisioned to enable a virtual society that goes far beyond the entertainment purpose. It would also include a variety of activities related to economy, finance, and business. Therefore, security is definitely one of the most important factors in the metaverse, impacting on all other components of the virtual world. In general, hackers can attack the metaverse in different ways: (i) they attack the data storage facility to alter data or inject false data, thereby causing significant damage or even crashing the entire system; (ii) hackers attack the identity and authentication system, in which user identities are threatened severely; (iii) attackers can exploit lower level systems, which is the metaverse physical infrastructure with numerous IoT, DT devices and VR/AR equipment; (iv) they attack the access control systems built in different metaverse applications and services.

First of all, the blockchain technology can help improving security in metaverse data storage, and provide a secure identity management system for the metaverse. These aspects are discussed in Section IV-D and IV-A.

Since metaverse users will access a wide range of virtual services and activities, a secure and convenient access control scheme is indispensable. If the access control system is operated by a centralized third-party authority, hackers can attack the centralized server, or the third party itself can act maliciously, thus threatening the metaverse security. The authors in [180] proposed an architecture for access control services based on blockchain and smart contract. In this design, all ABAC-based policies are codified as smart contracts, deployed on the Ethereum blockchain. Whenever a user requests to access a service or a file, the corresponding smart contract will automatically verify the provided policies to make a final decision on whether to grant access to that user. Thereby, all third-party-related security issues are eliminated completely. However, an access control scheme is not limited to user services; IoT devices within the metaverse infrastructure can also take advantages of the mechanism. Ding *et al.* [181] presented a similar access control scheme, but it controls the access of IoT devices instead of user access. Security and performance analysis have proved the feasibility of the design [181].

Since the metaverse provides a wide range of applications in different domains, IoT devices under the metaverse infrastructure must be able to switch domain frequently, potentially causing various security issues. Shen *et al.* [182] proposed a secure cross-domain authentication mechanism for IoT devices, named *BASA*, that overcomes potential security risks. In the mechanism, identity-based signature protocol is utilized for the authentication process, whereas authentication and identity data from different domains are stored on a consortium blockchain to construct cross-domain trust. While the analysis of extensive experiments on the protocol can prove its efficiency and feasibility, no intermediaries are needed to maintain the operation of the system. Besides an authentication process, embedded IoT devices can also be attacked during its updating process. The authors in [183] designed a blockchain-based firmware update scheme for embedded IoT devices, using blockchain to securely check the firmware version, validate the correctness, and download the latest firmware update. However, using blockchain to offer security features may lead to high latency and low throughput due to the consensus process. The authors in [184] proposed a solution to improve latency of secure access control system, in which a consortium blockchain with the state-of-the-art Raft consensus algorithm is designed to make the consensus progress faster and more reliable. As a result, while the consensus time decreases to about 100 ms and throughput achieves five times higher than the popular Byzantine fault tolerance consensus, the system still offers necessary blockchain-enabled security features for access control.

Communication networks in the metaverse can also be a potentially vulnerable component that might suffer from a wide range of attacks. Hu *et al.* [185] proposed a blockchain-enabled scheme for dynamic resource sharing in 5G/6G wireless network, in which blockchain is utilized to improve

[32]https://moralis.io/
[33]https://www.alchemy.com/

distribution, security and automation of the system, while AI supports the decision-making process. On the other hand, Zhou *et al.* [186] focused on spectrum sharing in 5G wireless networks. They proposed a blockchain-based architecture for secure spectrum sharing that resists against various security threats thanks to blockchain and its incentive mechanism. In terms of network slicing, Boateng *et al.* [187] proposed an autonomous radio access network slicing scheme with secure resource trading. In this scheme, a consortium blockchain supporting hyperledger smart contract is implemented to ensure security among participants of the slicing network. The authors in [188] introduced a digital twin wireless network with blockchain-empowered federated learning for enhanced reliability and security. As a result, the metaverse networking infrastructure based on blockchain can benefit enormously in terms of security.

Besides, blockchain can also be used to improve security of AI models in the metaverse. To this end, one might think of using blockchain-based data storage to store training data. However, the authors in [189] used smart contracts to implement directly several AI algorithms such as Linear Regression, Naive Bayes, and even a simple Neural Network to empower the metaverse. By this way, the "AI smart contract" can collect data right inside the blockchain network, then make cognitive decisions automatically by itself. Therefore, this process could achieve the highest extent of decentralization and security. Using up to 16$ for each prediction and achieving the accuracy almost equal to the corresponding benchmark model in the python package Skikit-learn[34], this is an acceptable trade-off in case the AI-based decision is very important. In terms of federated learning, the authors in [190] presented a blockchain-empowered framework for data sharing in Internet of Vehicles. In this scheme, security of models' parameters is ensured thanks to a hybrid blockchain consisting of a permissioned blockchain and the local Directed Acyclic Graph.

B. PRIVACY ISSUES

Different from traditional platforms, the metaverse can collect far more sensitive information from its users, raising serious privacy concerns for the society. It is unavoidable that the more immersive and convenient experience is offered, the higher extent user privacy is at stake. For instance, to be able to create digital avatars that simulate user appearance, metaverse users must provide their own personal images or even allow the platform to scan their appearance. Furthermore, when participating in the metaverse, all of user's facial expressions, speech, movement, and even brain wave would be recorded continuously to be reflected into the digital avatars[35]. If these sensitive data are leaked or used for malicious purposes, user privacy and their physical life can be threatened severely.

[34]https://scikit-learn.org/stable/

[35]https://www.businessinsider.com/meta-metaverse-patents-track-eye-movement-facial-expressions-facebook-zuckerberg-2022-1

Besides data leakage, digital footprint tracking is another potential issue in terms of privacy. For example, when a user goes shopping in a virtual mall, another malicious avatar can follow the user movement, observe her shopping habits and listen to all of her conversations within the virtual world. While this problem can be prevented in the real world, it is much harder in the virtual world as it is challenging to know if someone is tracking our digital footprints, or it is just coincidence. The authors in [191] presented two ideas to overcome that privacy issue: (i) generating multiple clone avatars to overshadow the real one's activities, thereby preventing being tracked by malicious users; (ii) creating a "private copy" of some part of the virtual world with the same functions and features, thus offering users their own temporary private space. However, they are just temporary solutions, and further studies are still needed to guarantee the privacy of metaverse users.

In terms of data leakage, the blockchain technology could be utilized in different ways to overcome this problem and provide better data privacy. The authors in [192] 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. 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, these IoT edge devices perform local federated training, then submit the trained parameters to a blockchain, which is a subchain in a cross-chain platform consisting of multiple blockchains. Finally, all learned parameters from different subchains are aggregated in a main blockchain, finishing a federated learning circle. Thus, 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. Weng *et al.* [193] proposed *DeepChain*, a privacy-preserving scheme for federated learning, in which privacy is ensured during the gradient collecting process thanks to an incentive mechanism based on blockchain. With a similar approach, Zhao *et al.* [194] proposed a federated learning scheme that replaces the centralized aggregator in a traditional system by a specific blockchain. Whenever parameters are fully collected, an organization or customer is selected as miner to compute the averaged model.

Furthermore, metaverse cloud data storage infrastructure might also be prone to privacy leakage issues. To store and manage cloud data provenance, Liang *et al.* [195] proposed a blockchain-based cloud data provenance architecture, named *ProvChain*, with enhanced privacy preservation. In this scheme, user privacy is achieved 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 as a hash. However, the cloud environment is centralized so it could be dominated by third parties, thus suffering from severe privacy issues. In terms of distributed computing, Li *et al.* [196] proposed *CrowdBC*, a blockchain-

based distributed framework that leverages blockchain and related techniques allowing users to register without disclosing their true identity, while the computing solutions are also stored in distributed environments.

Cross-domain authentication of both users and IoT devices in the metaverse is a potential source of privacy leakage. The authors in [197] proposed a blockchain-based privacy-preserving scheme, called *XAuth*, to protect privacy of that process. Specifically, the large amount of identity data is managed by multiple merkle hash trees, stored on blockchain. Moreover, ZKP algorithm is devised to ensure cross-domain privacy protection. Theoretical proofs and practical experiments have proved its feasibility and efficiency in privacy-preserving. Access control of IoT devices is another potential source of privacy leakage. To overcome this issue, the authors in [198] introduced *FairAccess*, a decentralized privacy-preserving model for IoT access control model. In this model, blockchain is leveraged to guarantee the enforcement of access control policies, thus third party and related privacy risks are eliminated entirely. Besides, IoT sensor devices often have access to very detailed personal data, thus threatening severely to privacy of users. The authors in [199] proposed a framework in which user privacy is preserved by using blockchain and data certification mechanisms. Furthermore, IoT data can be healthcare information from IoT wearable devices, which are even more sensitive. The authors in [200] designed a privacy-preserving ring signature scheme using anonymous transactions of blockchain networks to hide user address and protect patient privacy. Expanding to the metaverse, users in the metaverse must wear different AR/VR devices to participate in the virtual world. Therefore, the above frameworks can be deployed to ensure user privacy when using these devices.

C. SOCIAL AND ETHICAL ASPECTS

Since the metaverse is currently in its infancy, the lack of national and global policies is one of the major obstacles preventing it from social acceptance. In fact, the metaverse and related keywords such as Web3 are being debated in many countries [201], [202]. Without proper policies and regularization, a variety of social and ethical issues could arise in the metaverse such as digital scam, data manipulation, disinformation, and even sexual harassment.

In a virtual world where user identities are hidden to ensure privacy, disinformation may be more popular than ever. Therefore, the metaverse could become a source of misleading information, thus impacting negatively on the society and its own development. There are currently several ideas of utilizing blockchain to combat fake news in social media platforms such as [203], [204]. In [203], the authors proposed a framework in which news are submitted as transactions on the blockchain network, and each blockchain validator will act as a news validator. The validation process is conducted anonymously to prevent bias, while the decentralized nature of blockchain further strengthens the fairness of the system. On the other hand, the authors in [204] proposed to manage the spread of fake news by another approach based on smart contracts. The proposed architecture constructs a credibility system for news verifiers, but the main task is still to filter out fake news by peer reviews. This idea is developed further in [205], where the news verification process is supported by AI and NLP models. In this scheme, data are collected to an *off-chain data lake*, analyzed by NLP models, and the results are transferred to smart contract to support the decision making process.

On the other hand, blockchain and its related applications also have its own social and ethical issues in the metaverse [206]. The first major concern about blockchain that must be mentioned is cryptocurrency-related scam. While it is obvious that more policies are needed to regularize the metaverse economic system if cryptocurrency is used widely, some technical ideas have been proposed to deal with these problems [207], [208]. The general idea is to use AI and deep learning models to detect scam and fraud based on public transaction information on a particular blockchain. Similarly, the framework proposed in [209] helps to detect scam even earlier by analysing smart contract's bytecodes. As a result, these models acquired relatively high performance for some type of cryptocurrency scams such as phishing scam on Bitcoin and Ethereum blockchains.

There are still many other social issues related to the metaverse such as its impacts on both physical and mental health of users, especially the young, when they participate in the platform for too long. Besides, the great freedom that the metaverse offers can become a double-edged sword that makes racism and sexual harassment harder to control. However, these problems are beyond the scope of this paper.

D. ENERGY AND ENVIRONMENTAL CONCERNS

Throughout this study, the advantages of blockchain technology for the metaverse have been proven in different ways. However, this combination could pose a severe threat to the environment, since enormous amount of energy is required to maintain the operation of both the metaverse and the multiple blockchain networks. In fact, most backbone technologies of the metaverse such as DT, AI, and IoT are very energy-hungry. Especially, blockchain with numerous miners involving in complicated consensus mechanisms such as PoW could be the most serious energy-related issue of the metaverse. It has been shown that the electricity demand of Bitcoin's PoW mechanism was about 60 TWh per year in early 2020 [210], while the annual figure for Ethereum's PoW reached a peak of 100 TWh in early 2022[36]. Although many other consensus algorithms such as PoS or PoA have been invented as an effort to reduce the energy consumption of blockchain networks, they still cannot solve the problem thoroughly [211], and usually compromise other properties of the blockchain such as security or decentralization.

Currently, there are several studies studying possible solutions to improve these energy-related issues. The authors

[36]https://digiconomist.net/ethereum-energy-consumption

in [212] proposed a Green-PoW mechanism that could reduce up to 50% energy consumption, while still maintain the necessary security of the original PoW. In the original PoW, whenever a miner successfully solves the PoW puzzle to mine a new block, all other miners will also give up their current work to turn to the puzzle of the next block, causing a huge waste of resource. On the other hand, the proposed Green-PoW grants these miners exclusivity to mine the next block as a compensation, thus reducing the number of miners on the upcoming block and thereby reducing the overall energy consumption. However, this mechanism partly decreases decentralization since there will be fewer miners involving in the mining process.

Another environmental friendly approach is to take advantages of computational resource during the consensus process, which is presented in [213]. In this approach, all miners utilize their resources to train deep learning models instead of trying to solve the meaningless PoW puzzles. The block proposer will be the first one who successfully obtains the deep learning model satisfying the required performance. Since AI and deep learning tasks are used frequently in the metaverse, this approach is such an appropriate option for metaverse energy saving. Moreover, the above process can still be utilized further in a decentralized environment like the metaverse. The authors in [214] proposed a novel consensus algorithm called *Proof of Federated Learning*. The idea of this algorithm is similar to the previously mentioned mechanism, but the deep learning tasks are replaced by federated learning in which the model is trained across multiple decentralized devices. Therefore, this consensus protocol is a natural fit for the blockchain-based metaverse in terms of energy saving and recycling.

Instead of trying to optimize the energy consumption of blockchain, we can also take an opposite approach in which blockchain is used to reduce the energy consumption of metaverse services. The authors in [130] introduced *MetaChain*, a blockchain-enabled framework for resource allocation in the metaverse based on sharding. Specifically, the framework utilizes smart contracts to facilitate the interactions between the metaverse service provider and metaverse users, thereby optimizing service management process. On the other hand, blockchain shards are designed to improve the efficiency of resource usage in the metaverse.

VII. 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. 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 [215]. That is also the most expensive NFT ever sold, with 28,983 collectors pitched together to purchase 312,686 parts of this NFT. On the other hand, *The First 5,000 Days*, a combination of 5,000 digital images created by the digital artist Mike Winkelmann, is considered the most valuable NFT artwork sold to a single purchaser ($69.3 million) [216].

However, it is quite 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, efficient methods to evaluate virtual assets and prevent scams are needed since they impact enormously the entire economic system of the digital world. Some traditional valuation methods such as the DCF model and the Market approach in the financial sector could be deployed as presented in Section V-C4, 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 proning to errors. Simultaneous Multi-Round Auction (SMRA) could be used to reduce uncertainty in NFT pricing [217]. In SMRA, the auction is implemented in rounds with a fixed countdown. Bidders can bid and win multiple items at the same time, while multiple items of related categories are auctioned concurrently. While the efficiency of such methods have not been verified concretely, they are relatively sophisticated and seem not appropriate for routine trading in the metaverse. Therefore, virtual asset valuation in the metaverse is still an open issue and further research must be conducted to develop more suitable solutions.

B. 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 II-B4. This mechanism raises two serious problems:

- **Centralization:** The intervention of the third-party operator eliminates the desirable decentralized property. The operator can be organized as a group of validators instead of just one node to improve decentralization; however, the 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 to use the bridge, 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

TABLE 6. Literature reviews on various issues related to different aspects of the metaverse.

Aspect	Ref.	Issue	Proposed Solutions	Technology
Security	[180]	Third-party-related attacks on access control system	Using smart contracts to codify ABAC policies and manage access control system.	Blockchain, ABAC
	[181]	Attacks on IoT-based access control	Using blockchain to record the distribution of attributes, thereby avoiding data tampering and SPOF.	Blockchain, ABAC, IoT
	[182]	Cross-domain-related security risks	Using a consortium blockchain to store cross-domain identity data. Authentication is based on specific signature protocol.	Identity-based signature, blockchain
	[184]	Security trade-offs with latency and throughput	Utilizing Raft consensus algorithm to improve latency and throughput, while security features are still ensured.	Blockchain with Raft consensus
	[189]	AI-related security risks	Directly use smart contract to deploy metaverse AI models.	Smart contracts
	[185]	Security risks of dynamic resource sharing	Utilizing blockchain to improve distribution, security and automation of dynamic resource sharing in 6G.	Blockchain, AI, 6G
	[186]	Security of spectrum sharing and allocation	Utilizing blockchain to ensure security of spectrum sharing and allocation in 5G heterogeneous networks.	Blockchain, 5G
	[187]	Security risks in network slicing scheme	A consortium blockchain helps ensuring security of resource trading among participants in the slicing network.	Blockchain, deep reinforcement learning
	[188]	Networking-related security risks of digital twin	Combine blockchain and federated learning to improve reliability and security of DT collaborative computing.	Blockchain, federated learning, DT
	[190]	Security of federated learning model parameters	Design hybird blockchain using directed acyclic graph to enhance the security of model parameters.	Blockchain, federated learning
	[183]	Attacks on embedded IoT devices	Proposed a blockchain-based firmware update scheme for embedded devices to enhance security.	Blockchain, IoT
Privacy	[191]	Digital footprint tracking	Generating clone avatars to shadow user activities. Creating private copy of virtual world to preserve privacy.	Clone avatars, private copy
	[192]	Privacy leakage of sensitive AI data	Keep sensitive data on a blockchain of IoT physical layer. Trained parameters are then merged in a relay chain.	Blockchain, IoT, federated learning
	[195]	Cloud data provenance leakage	Using ID hashing mechanism for privacy preservation. Hashing owner identity to hide sensitive information.	Blockchain, cloud storage
	[197]	Cross-domain privacy leakage	Storing large identity data in multiple merkle hash trees. Utilizing ZKP to ensure cross-domain privacy.	Merkle hash tree, ZKP, blockchain
	[193]	Privacy issues of training data in federated learning	A blockchain-based incentive mechanism is designed to ensure privacy in the training process of federated learning.	Blockchain, deep learning
	[196]	User privacy leakage in distributed computing	Allow users to register without revealing their true identity. Computing solutions are stored in distributed scheme.	Blockchain
	[198]	Third-party-related privacy leakage	Eliminate third-party authorities in IoT access control system to ensure privacy.	Blockchain, IoT
	[200]	Privacy concerns about logging of medical data	Design a privacy-preserving ring signature scheme for anonymous transactions instead of using public address.	Blockchain, IoT
	[199]	Privacy leakage of IoT sensor devices	Leverage data certification and blockchain to preserve privacy of IoT sensor devices.	Blockchain, IoT
	[194]	Privacy leakage when aggregating FL models	Use blockchain to replace the centralized aggregator in federated learning scheme.	Blockchain, IoT, federated learning
Social and Ethical Aspects	[203]	The spread of fake news in virtual platforms	News are posted as blockchain transactions, whereas validators verify news anonymously.	Blockchain
	[204]	Lack of automatic verification system	Filtering out fake news on digital platforms based on smart contracts with a credibility system for new verifiers.	Smart contract
	[205]	Verify news manually might cause bias	Collecting news data by a blockchain off-chain data lake. Utilizing NLP models to detect false information.	Blockchain, NLP
	[208]	Cryptocurrency-related scam and fraud	Using deep learning models to detect scams such (e.g., phishing scam) based on blockchain transaction information.	Deep learning
	[209]	Smart contract scam	Utilizing deep learning to analyze smart contract byte code.	Deep learning
Energy Consumption	[212]	PoW high energy consumption	Reducing PoW energy consumption by limiting the number of miners based on a compensation mechanism.	Blockchain
	[213], [214]	The useless waste of consensus protocols	Instead of wasting computation resource for the PoW puzzle, miners turn to train deep learning/federated learning models.	Deep learning, federated learning
	[130]	Waste of metaverse resource allocation	Using blockchain and sharding techniques to optimize resource allocation of metaverse infrastructure.	Blockchain, sharding mechanism

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 [218], 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 [219]. This would pose a threat to the economic system of the metaverse and impact social acceptance of such platforms. Therefore, it is crucial that more advanced protocols be invented to improve blockchain interoperability when they are deployed and integrated into the metaverse.

C. FINANCIAL RISKS IN METAFI

MetaFi has been introduced in Section III-F with a variety of financial services provided to metaverse users. Not only individuals, but also organizations can take advantages of this financial system, in which all financial activities such as lending, borrowing, investment, issuing stocks can be done without intermediaries. 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; hence, our funds are ensured to be safe even in the worst financial situations. On the other hand, in a completely virtual and decentralized environment like the metaverse, no similar insurances are available to protect customers from financial risks.

Besides, there is a critical problem of using cryptocurrency as a payment method in the metaverse, its volatile characteristic. Although stablecoins have been introduced as a solution for cryptocurrency 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 [220]. 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 [221], 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.

D. BLOCKCHAIN SCALABILITY AND COST

As there can be a very large number of users taking part in the metaverse everyday, the number of payment transactions for routine activities will definitely be very high. The cryptocurrency system deployed in the Metaverse must be as fast as possible to deal with the high demand of the market. However, not only cryptocurrency and blockchain, but also all decentralized systems face the scalability problem [222]. 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. Hence, sophisticated mechanisms are needed to validate these transactions and to reach the consensus among nodes. This is the reason for the limited processing speed of any blockchain system.

The Section II-B suggests a solution for blockchain scalability problem using committee-based consensus algorithm with a small group of validators responsible for validating transactions. However, this means that certain degree of decentralization for underlying blockchain is 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. Due to scalability limitations, transaction costs will inevitably go up when trading demand increases. If the number of transactions submitted into a blockchain exceeds the network's processing capacity, users even have to spend more money as a fee to get their transactions prioritized. Metaverse users may not prefer using cryptocurrency for their routine payments if it has higher transaction fee than traditional financial payment services. Therefore, to be applicable for the metaverse, the scalability of blockchain technology must be improved further.

E. 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 which can afford this large amount of data would decrease over time. In other words, the decentralization and security of the metaverse could eventually degrade. Visa, one of largest real-world payment networks, processes hundreds of millions of transactions per day[37]. Similarly, the number of daily transactions in the metaverse will become extremely high, posing a threat to the future of the metaverse economic

[37]https://www.cardrates.com/advice/number-of-credit-card-transactions-per-day-year/

system. 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 [223]–[225]. 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.

VIII. CONCLUSION

In this paper, we have presented a comprehensive and in-depth survey of the blockchain-enabled metaverse. We have introduced the metaverse concept and blockchain technology, including their architecture, characteristics, and applications. Then, we investigated a wide range of use cases in which blockchain helps enabling the metaverse from user application perspective, and from system and infrastructure point of views. For each use case, we discussed related technical issues, described how blockchain can potentially solve the current problems, and conducted literature reviews on related published works. A detailed technical analysis has also been carried out on the blockchain-based digital asset management in the metaverse. Furthermore, we analyzed crucial factors of the metaverse such as security, privacy, and various social aspects, thereby figuring out potential use cases of blockchain to improve the metaverse according to these aspects. Lastly, open challenges were discussed to provide future research directions for this interesting and important research topic. 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," *Interdisciplinary Literary Studies*, vol. 19, no. 1, pp. 17–47, 2017, doi: 10.5325/intelitestud.19.1.0017.

[2] L. Locurcio, "Dental education in the metaverse," *British Dental Journal*, vol. 232, no. 4, pp. 191–191, 2022, doi: 10.1038/s41415-022-3990-7.

[3] X. Yu, D. Owens, and D. Khazanchi, "Building socioemotional environments in metaverses for virtual teams in healthcare: A conceptual exploration," in *Proc. International Conference on Health Information Science*. Springer, 2012, pp. 4–12, doi: 10.1007/978-3-642-29361-0_3.

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

[5] H. Jeong, Y. Yi, and D. Kim, "An innovative e-commerce platform incorporating metaverse to live commerce," *International Journal of Innovative Computing, Information and Control*, vol. 18, no. 1, pp. 221–229, 2022, doi: 10.24507/ijicic.18.01.221.

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

[7] A. H. Jacob 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

[8] K. Rees. (2022) These 8 tech giants have invested big in the metaverse. [Online]. Available: https://www.makeuseof.com/companies-investing-in-metaverse/

[9] U. W. Chohan, "Non-fungible tokens: Blockchains, scarcity, and value," *Critical Blockchain Research Initiative (CBRI) Working Papers*, 2021, doi: 10.2139/ssrn.3822743.

[10] S. Wang, W. Ding, J. Li, Y. Yuan, L. Ouyang, and F.-Y. Wang, "Decentralized autonomous organizations: concept, model, and applications," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 5, pp. 870–878, 2019, doi: 10.1109/TCSS.2019.2938190.

[11] Y. Chen and C. Bellavitis, "Blockchain disruption and decentralized finance: The rise of decentralized business models," *Journal of Business Venturing Insights*, vol. 13, p. e00151, 2020, doi: 10.1016/j.jbvi.2019.e00151.

[12] 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. 53 019–53 033, 2018, doi: 10.1109/ACCESS.2018.2870644.

[13] T. R. Gadekallu, T. Huynh-The, W. Wang, G. Yenduri, P. Ranaweera, Q.-V. Pham, D. B. da Costa, and M. Liyanage, "Blockchain for the metaverse: A review," *arXiv preprint arXiv:2203.09738*, 2022.

[14] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, "Fusing blockchain and ai with metaverse: A survey," *IEEE Open Journal of the Computer Society*, vol. 3, pp. 122–136, 2022, doi: 10.1109/OJCS.2022.3188249.

[15] H.-j. Jeon, H.-c. Youn, S.-m. Ko, and T.-h. Kim, "Blockchain and ai meet in the metaverse," *Advances in the Convergence of Blockchain and Artificial Intelligence*, p. 73, 2022.

[16] L.-H. Lee, T. Braud, P. Zhou, L. Wang, D. Xu, Z. Lin, A. Kumar, C. Bermejo, and P. Hui, "All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda," *arXiv preprint arXiv:2110.05352*, 2021, doi: 10.48550/arXiv.2110.05352.

[17] M. Xu, W. C. Ng, W. Y. B. Lim, J. Kang, Z. Xiong, D. Niyato, Q. Yang, X. S. Shen, and C. Miao, "A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges," *IEEE Communications Surveys & Tutorials*, 2022, doi: 10.1109/COMST.2022.3221119.

[18] 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 Communications Surveys & Tutorials*, 2022, doi: 10.1109/COMST.2022.3202047.

[19] H. Ning, H. Wang, Y. Lin, W. Wang, S. Dhelim, F. Farha, J. Ding, and M. Daneshmand, "A survey on metaverse: the state-of-the-art, technologies, applications, and challenges," *arXiv preprint arXiv:2111.09673*, 2021, doi: 10.48550/arXiv.2111.09673.

[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 International Conference on Multimedia*, 2021, pp. 153–161, doi: 10.1145/3474085.3479238.

[21] C. B. Fernandez and P. Hui, "Life, the metaverse and everything: An overview of privacy, ethics, and governance in metaverse," *arXiv preprint arXiv:2204.01480*, 2022, doi: 10.48550/arXiv.2204.01480.

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

[23] Y. K. Dwivedi, L. Hughes, A. M. Baabdullah, S. Ribeiro-Navarrete, M. Giannakis, M. M. Al-Debei, D. Dennehy, B. Metri, D. Buhalis, C. M. Cheung *et al.*, "Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," *International Journal of Information Management*, vol. 66, p. 102542, 2022, doi: 10.1016/j.ijinfomgt.2022.102542.

[24] S.-M. Park and Y.-G. Kim, "A metaverse: taxonomy, components, applications, and open challenges," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2021.3140175.

[25] S. Mystakidis, "Metaverse," *Encyclopedia*, vol. 2, no. 1, pp. 486–497, 2022, doi: 10.3390/encyclopedia2010031.

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

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

[28] A. Fuller, Z. Fan, C. Day, and C. Barlow, "Digital twin: Enabling technologies, challenges and open research," *IEEE access*, vol. 8, pp. 108 952–108 971, 2020, doi: 10.1109/ACCESS.2020.2998358.

[29] Y.-W. Chong, W. Ismail, K. Ko, and C.-Y. Lee, "Energy harvesting for wearable devices: A review," *IEEE Sensors Journal*, vol. 19, no. 20, pp. 9047–9062, 2019, doi: 10.1109/JSEN.2019.2925638.

[30] C. Collins, "Looking to the future: Higher education in the metaverse," *Educause Review*, vol. 43, no. 5, pp. 50–52, 2008.

[31] S. Hollensen, P. Kotler, and M. O. Opresnik, "Metaverse–the new marketing universe," *Journal of Business Strategy*, 2022, doi: 10.1108/JBS-01-2022-0014.

[32] J. Goldston, T. J. Chaffer, and G. Martinez, "The metaverse as the digital leviathan: A case study of bit. country," *The Journal of Applied Business and Economics*, vol. 24, no. 2, pp. 40–59, 2022.

[33] C.-S. Kim, Y. Lee, and H. Ahn, "A study on the metaverse: Focused on the application of news big data service and case study," *Journal of Korea Society of Digital Industry and Information Management*, vol. 17, no. 2, pp. 85–101, 2021, doi:10.17662/ksdim.2021.17.2.085.

[34] X. Niu and W. Feng, "Immersive entertainment environments-from theme parks to metaverse," in *Proc. International Conference on Human-Computer Interaction*. Springer, 2022, pp. 392–403, doi: 10.1007/978-3-031-05463-1_27.

[35] J. Thomason, "Metahealth-how will the metaverse change health care?" *Journal of Metaverse*, vol. 1, no. 1, pp. 13–16, 2021.

[36] A. Tobin. (2022) Insurance in the metaverse. [Online]. Available: https://clearsurance.com/blog/metaverse-insurance

[37] S. Nakamoto, "Bitcoin whitepaper," *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)*, 2008.

[38] H. Liu, X. Luo, H. Liu, and X. Xia, "Merkle tree: A fundamental component of blockchains," in *Proc. International Conference on Electronic Information Engineering and Computer Science (EIECS)*. IEEE, 2021, pp. 556–561, doi: 10.1109/EIECS53707.2021.9588047.

[39] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *Proc. IEEE international conference on systems, man, and cybernetics (SMC)*. IEEE, 2017, pp. 2567–2572, doi: 10.1109/SMC.2017.8123011.

[40] F. Saleh, "Blockchain without waste: Proof-of-stake," *The Review of financial studies*, vol. 34, no. 3, pp. 1156–1190, 2021, doi: 10.1093/rfs/hhaa075.

[41] N. Sánchez-Gómez, J. Torres-Valderrama, J. A. García-García, J. J. Gutiérrez, and M. Escalona, "Model-based software design and testing in blockchain smart contracts: A systematic literature review," *IEEE Access*, vol. 8, pp. 164 556–164 569, 2020, doi: 10.1109/ACCESS.2020.3021502.

[42] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Computing Surveys (CSUR)*, vol. 54, no. 8, pp. 1–41, 2021, doi: 10.1145/3471140.

[43] H. T. Vo, Z. Wang, D. Karunamoorthy, J. Wagner, E. Abebe, and M. Mohania, "Internet of blockchains: Techniques and challenges ahead," in *Proc. IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. IEEE, 2018, pp. 1574–1581, doi: 10.1109/Cybermatics_2018.2018.00264.

[44] N. Kannengießer, M. Pfister, M. Greulich, S. Lins, and A. Sunyaev, "Bridges between islands: Cross-chain technology for distributed ledger technology," 2020.

[45] K. Košt'ál, "Multi-chain architecture for blockchain networks," *Information Sciences & Technologies: Bulletin of the ACM Slovakia*, vol. 12, no. 2, pp. 8–14, 2020.

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

[47] J. Kwon and E. Buchman, "Cosmos whitepaper," *A Netw. Distrib. Ledgers*, 2019.

[48] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," *The Sovrin Foundation*, vol. 29, 2016.

[49] M. Sparkes. (2021) What is a metaverse. Doi: 10.1016/S0262-4079(21)01450-0.

[50] J. Fennimore. (2017) Roblox: 5 fast facts you need to know.

[51] O. Esteban, M. Ariel, J. Yemel, and A. Manuel, "Decentraland white paper," Technical Report. Decentraland, Tech. Rep., 2017.

[52] R. Games, "Grand theft auto v," *Retrieved February*, vol. 18, p. 2008, 2008.

[53] J. Kim, "The institutionalization of youtube: From user-generated content to professionally generated content," *Media, culture & society*, vol. 34, no. 1, pp. 53–67, 2012, doi: 10.1177/0163443711427199.

[54] E. Ordano, A. Meilich, Y. Jardi, and M. Araoz, "Decentraland: A blockchain-based virtual world," in *Technical Report*. Decentraland, 2017.

[55] W. Wright, D. Schroh, P. Proulx, A. Skaburskis, and B. Cort, "The sandbox for analysis: concepts and methods," in *Proc. SIGCHI conference on Human Factors in computing systems*, 2006, pp. 801–810, doi: 10.1145/1124772.1124890.

[56] T. Sandbox. (2020) The sandbox assets — ugc in a blockchain metaverse. [Online]. Available: https://medium.com/sandbox-game/the-sandbox-assets-ugc-in-a-blockchain-metaverse-87ce2d37ece6

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

[58] N. Rubio-Licht. (2021) The metaverse real-estate boom is on. [Online]. Available: https://www.protocol.com/bulletins/republic-realm-sandbox-real-estate

[59] R. Frank. (2022) Metaverse real estate sales top $500 million, and are projected to double this year. [Online]. Available: https://www.cnbc.com/2022/02/01/metaverse-real-estate-sales-top-500-million-metametric-solutions-says.html

[60] M. Mishra. (2022) Acura shows us how to use the metaverse and nfts to sell cars, raise awareness. [Online]. Available: https://kqeducationgroup.com/acura-enters-the-metaverse-with-integra-nft/

[61] K. D. Squire, "From virtual to participatory learning with technology during covid-19," *E-Learning and Digital Media*, vol. 19, no. 1, pp. 55–77, 2022, doi: 10.1177/20427530211022926.

[62] 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 Conference on Consumer Electronics (GCCE)*. IEEE, 2018, pp. 585–587, doi: 10.1109/GCCE.2018.8574479.

[63] B. Tackmann, "Secure event tickets on a blockchain," in *Data privacy management, Cryptocurrencies and Blockchain technology*. Springer, 2017, pp. 437–444, doi: 10.1007/978-3-319-67816-0_26.

[64] Kalki. (2021) Decentral games – a virtual casino on decentraland (fundamental analysis). [Online]. Available: https://coinsutra.com/decentral-games/

[65] I. Arribas, D. Arroyo, and D. Reshef Kera, "Sandbox for minimal viable governance of blockchain services and daos: Claudia," in *Proc. International Congress on Blockchain and Applications*. Springer, 2020, pp. 24–30, doi: 10.1007/978-3-030-52535-4_3.

[66] G. Park. (2020) Silicon valley is racing to build the next version of the internet. fortnite might get there first. [Online]. Available: https://www.washingtonpost.com/video-games/2020/04/17/fortnite-metaverse-new-internet/

[67] J. Burke. (2021) Metafi: Defi for the metaverse. [Online]. Available: https://outlierventures.io/research/metafi-defi-for-the-metaverse/

[68] D. Parmar. (2022) 12 best crypto lending platforms in 2022. [Online]. Available: https://geekflare.com/finance/best-cryptocurrency-lending-platforms/
[69] L. Sáez and X. Shi, "Liquidity pools, risk sharing, and financial contagion," *Journal of Financial Services Research*, vol. 25, no. 1, pp. 5–23, 2004, doi: 10.1023/B:FINA.0000008662.59653.33.
[70] T. Chen, Z. Li, H. Zhou, J. Chen, X. Luo, X. Li, and X. Zhang, "Towards saving money in using smart contracts," in *Proc. IEEE/ACM 40th international conference on software engineering: New ideas and emerging technologies results (ICSE-NIER)*. IEEE, 2018, pp. 81–84.
[71] V. V. Bhandarkar, A. A. Bhandarkar, and A. Shiva, "Digital stocks using blockchain technology the possible future of stocks?" *International Journal of Management (IJM)*, vol. 10, no. 3, 2019.
[72] H. Al-Shaibani, N. Lasla, and M. Abdallah, "Consortium blockchain-based decentralized stock exchange platform," *IEEE Access*, vol. 8, pp. 123 711–123 725, 2020, doi: 10.1109/ACCESS.2020.3005663.
[73] A. Norta, "Creation of smart-contracting collaborations for decentralized autonomous organizations," in *Proc. International Conference on Business Informatics Research*. Springer, 2015, pp. 3–17, doi: 10.1007/978-3-319-21915-8_1.
[74] A. K. Kar and L. Navin, "Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature," *Telematics and Informatics*, vol. 58, p. 101532, 2021, doi: 10.1016/j.tele.2020.101532.
[75] R. Brophy, "Blockchain and insurance: a review for operations and regulation," *Journal of financial regulation and compliance*, vol. 28, no. 2, pp. 215–234, 2019, doi: 10.1108/JFRC-09-2018-0127.
[76] S. Kumar and A. Kumar, "Addressing transparency vis-a-vis privacy in portability of health insurance through blockchain," in *Innovations in Information and Communication Technologies (IICT-2020)*. Springer, 2021, pp. 407–411, doi: 10.1007/978-3-030-66218-9_48.
[77] N. Zagalo and L. Morgado, "Virtual worlds and metaverse platforms: Nevv communication and identity paradigms," 2012.
[78] A. Josang, J. Fabre, B. Hay, J. Dalziel, and S. Pope, "Trust requirements in identity management," in *Proc. Australasian workshop on Grid computing and e-research-Volume 44*. Citeseer, 2005, pp. 99–108.
[79] D. W. Chadwick, "Federated identity management," in *Foundations of security analysis and design V*. Springer, 2009, pp. 96–120, doi: 10.1007/978-3-642-03829-7_3.
[80] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, 2018, doi: 10.1016/j.cosrev.2018.10.002.
[81] A. Josang and S. Pope, "User centric identity management," in *Proc. AusCERT Asia Pacific information technology security conference*, vol. 77. Citeseer, 2005.
[82] J. Jensen, "Federated identity management challenges," in *Proc. Seventh International Conference on Availability, Reliability and Security*. IEEE, 2012, pp. 230–235, doi: 10.1109/ARES.2012.68.
[83] W. W. W. Consortium *et al.*, "Verifiable credentials data model 1.0: Expressing verifiable information on the web," *https://www.w3.org/TR/vc-data-model/?#core-data-model*, 2019.
[84] Z. A. Lux, D. Thatmann, S. Zickau, and F. Beierle, "Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials," in *Proc. 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 2020, pp. 71–78, doi: 10.1109/BRAINS49436.2020.9223292.
[85] Q. Stokkink and J. Pouwelse, "Deployment of a blockchain-based self-sovereign identity," in *Proc. IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. IEEE, 2018, pp. 1336–1342, doi: 10.1109/Cybermatics_2018.2018.00230.
[86] U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity," *Journal of cryptology*, vol. 1, no. 2, pp. 77–94, 1988, doi: 10.1007/BF02351717.
[87] N. Kulabukhova, "Zero-knowledge proof in self-sovereign identity," in *Proc. 27th Int. Symp. Nucl. Electron. Comput.(NEC)*, 2019, pp. 381–385.
[88] Y. Liu, Q. Lu, H.-Y. Paik, and X. Xu, "Design patterns for blockchain-based self-sovereign identity," in *Proc. European Conference on Pattern Languages of Programs 2020*, 2020, pp. 1–14, doi: 10.1145/3424771.3424802.
[89] E. Bandara, X. Liang, P. Foytik, S. Shetty, and K. De Zoysa, "A blockchain and self-sovereign identity empowered digital identity platform," in *Proc. International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2021, pp. 1–7, doi: 10.1109/ICCCN52240.2021.9522184.
[90] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Information Processing & Management*, vol. 58, no. 2, p. 102468, 2021, doi: 10.1016/j.ipm.2020.102468.
[91] U. Cali, M. S. Ferdous, E. Karaarslan, S. N. G. Gourisetti, and M. Mylrea, "Ssi meets metaverse for industry 4.0 and beyond," 2022.
[92] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for iot," *Computers & Security*, vol. 78, pp. 126–142, 2018, doi: 10.1016/j.cose.2018.06.004.
[93] 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 Transactions on Services Computing*, vol. 13, no. 2, pp. 241–251, 2020, doi: 10.1109/TSC.2020.2964537.
[94] V. Almeida, F. Filgueiras, and D. Doneda, "The ecosystem of digital content governance," *IEEE Internet Computing*, vol. 25, no. 3, pp. 13–17, 2021, doi: 10.1109/MIC.2021.3057756.
[95] A. Sims, "Decentralised autonomous organisations: Governance, dispute resolution and regulation," *Dispute Resolution and Regulation (May 31, 2021)*, 2021, doi: 10.2139/ssrn.3971228.
[96] D. Kraus, T. Obrist, and O. Hari, *Blockchains, smart contracts, decentralised autonomous organisations and the law*. Edward Elgar Publishing, 2019.
[97] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE Access*, vol. 7, pp. 24 477–24 488, 2019, doi: 10.1109/ACCESS.2019.2895670.
[98] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in *Proc. International conference on financial cryptography and data security*. Springer, 2017, pp. 357–375, doi: 10.1007/978-3-319-70972-7_20.
[99] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Future Generation Computer Systems*, vol. 105, pp. 13–26, 2020, doi: 10.1016/j.future.2019.11.005.
[100] 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, 2021, doi: 10.3390/s21175874.
[101] 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. 115 304–115 316, 2019, doi: 10.1109/ACCESS.2019.2935895.
[102] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory," *Prob. Contr. Inform. Theory*, vol. 15, no. 2, pp. 157–166, 1986.
[103] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtỳsson, "Blockchain-based e-voting system," in *Proc. IEEE 11th international conference on cloud computing (CLOUD)*. IEEE, 2018, pp. 983–986, doi: 10.1109/CLOUD.2018.00151.
[104] H. Yi, "Securing e-voting based on blockchain in p2p network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–9, 2019, doi: 10.1186/s13638-019-1473-6.
[105] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A trustless privacy-preserving reputation system," in *Proc. IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer, 2016, pp. 398–411, doi: 10.1007/978-3-319-33630-5_27.
[106] D. Liu, A. Alahmadi, J. Ni, X. Lin, and X. Shen, "Anonymous reputation system for iiot-enabled retail marketing atop pos blockchain," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3527–3537, 2019, doi: 10.1109/TII.2019.2898900.
[107] Z. Abubaker, A. U. Khan, A. Almogren, S. Abbas, A. Javaid, A. Radwan, and N. Javaid, "Trustful data trading through monetizing iot data using blockchain based review system," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 5, p. e6739, 2022, doi: 10.1002/cpe.6739.
[108] 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 Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4434–4449, 2021, doi: 10.1109/TNSM.2021.3098439.
[109] 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," *Applied Energy*, vol. 295, p. 117056, 2021, doi: 10.1016/j.apenergy.2021.117056.
[110] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, "Consortium blockchains: Overview, applications and challenges," *Inter-*

national Journal On Advances in Telecommunications, vol. 11, no. 1&2, pp. 51–64, 2018.

[111] J. Lee, B. Lee, J. Jung, H. Shim, and H. Kim, "Dq: Two approaches to measure the degree of decentralization of blockchain," *ICT Express*, vol. 7, no. 3, pp. 278–282, 2021, doi: 10.1016/j.icte.2021.08.008.

[112] M. Satyanarayanan, "A survey of distributed file systems," *Annual Review of Computer Science*, vol. 4, no. 1, pp. 73–104, 1990, doi: 10.1146/annurev.cs.04.060190.000445.

[113] M. Dowling, "Is non-fungible token pricing driven by cryptocurrencies?" *Finance Research Letters*, vol. 44, p. 102097, 2022, doi: 10.1016/j.frl.2021.102097.

[114] R. Kumar, N. Marchang, and R. Tripathi, "Distributed off-chain storage of patient diagnostic reports in healthcare system using ipfs and blockchain," in *Proc. International Conference on COMmunication Systems & NETworkS (COMSNETS)*. IEEE, 2020, pp. 1–5, doi: 10.1109/COMSNETS48256.2020.9027313.

[115] 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 Transactions on Services Computing*, vol. 12, no. 5, pp. 762–771, 2018, doi: 10.1109/TSC.2018.2853167.

[116] W. Liang, Y. Fan, K.-C. Li, D. Zhang, and J.-L. Gaudiot, "Secure data storage and recovery in industrial blockchain network environments," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6543–6552, 2020, doi: 10.1109/TII.2020.2966069.

[117] G. Bansal, K. Rajgopal, V. Chamola, Z. Xiong, and D. Niyato, "Healthcare in metaverse: A survey on current metaverse applications in healthcare," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2022.3219845.

[118] 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. 118 943–118 953, 2019, doi: 10.1109/ACCESS.2019.2937685.

[119] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *Proc. 2016 2nd international conference on open and big data (OBD)*. IEEE, 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.

[120] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "Bbds: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017, doi: 10.3390/info8020044.

[121] S. Huang, G. Wang, Y. Yan, and X. Fang, "Blockchain-based data management for digital twin of product," *Journal of Manufacturing Systems*, vol. 54, pp. 361–371, 2020, doi: 10.1016/j.jmsy.2020.01.009.

[122] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of iot data," in *Proc. 2017 on cloud computing security workshop*, 2017, pp. 45–50, doi: 10.1145/3140649.3140656.

[123] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for iot data," in *Proc. IEEE International Conference on Web Services (ICWS)*, 2017, pp. 468–475, doi: 10.1109/ICWS.2017.54.

[124] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, and S. Chen, "The blockchain as a software connector," in *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*. IEEE, 2016, pp. 182–191, doi: 10.1109/WICSA.2016.21.

[125] A. Hassan, M. Ali, R. Ahammed, M. M. Khan, N. Alsufyani, A. Alsufyani *et al.*, "Secured insurance framework using blockchain and smart contract," *Scientific Programming*, vol. 2021, 2021, doi: 10.1155/2021/6787406.

[126] P. Tasca, "Insurance under the blockchain paradigm," in *Business transformation through blockchain*. Springer, 2019, pp. 273–285, doi: 10.1007/978-3-319-98911-2_9.

[127] E. Culliford. (2021) Who is building the metaverse? [Online]. Available: https://www.reuters.com/technology/whos-building-metaverse-2021-11-01/

[128] (2021) ISO/IEC 23005 MPEG-V Standards. Interfacing with Virtual Worlds. [Online]. Available: https://mpeg.chiariglione.org/standards/mpeg-v

[129] (2021) IEEE 2888 standards. Interfacing Cyber and Physical World. [Online]. Available: https://sagroups.ieee.org/2888/

[130] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, and E. Dutkiewicz, "Metachain: A novel blockchain-based framework for metaverse applications," in *Proc. IEEE 95th Vehicular Technology Conference:(VTC2022-Spring)*. IEEE, 2022, pp. 1–5, doi: 10.1109/VTC2022-Spring54318.2022.9860983.

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

[132] R. Belchior, A. Vasconcelos, M. Correia, and T. Hardjono, "Hermes: Fault-tolerant middleware for blockchain interoperability," *Future Generation Computer Systems*, vol. 129, pp. 236–251, 2022, doi: 10.1016/j.future.2021.11.004.

[133] M. Herlihy, "Atomic cross-chain swaps," in *Proc. ACM symposium on principles of distributed computing*, 2018, pp. 245–254, doi: 10.1145/3212734.3212736.

[134] L. Deng, H. Chen, J. Zeng, and L.-J. Zhang, "Research on cross-chain technology based on sidechain and hash-locking," in *Proc. International conference on edge computing*. Springer, 2018, pp. 144–151, doi: 10.1007/978-3-319-94340-4_12.

[135] B. Pillai, K. Biswas, and V. Muthukkumarasamy, "Cross-chain interoperability among blockchain-based systems using transactions," *The Knowledge Engineering Review*, vol. 35, 2020, doi: 10.1017/S0269888920000314.

[136] T. Hardjono, A. Lipton, and A. Pentland, "Toward an interoperability architecture for blockchain autonomous systems," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1298–1309, 2019, doi: 10.1109/TEM.2019.2920154.

[137] Z. Liu, Y. Xiang, J. Shi, P. Gao, H. Wang, X. Xiao, B. Wen, and Y.-C. Hu, "Hyperservice: Interoperability and programmability across heterogeneous blockchains," in *Proc. 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 549–566, doi: 10.1145/3319535.3355503.

[138] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable cities and society*, vol. 39, pp. 283–297, 2018, doi: 10.1016/j.scs.2018.02.014.

[139] G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate, and M. Maffei, "Anonymous multi-hop locks for blockchain scalability and interoperability," *Cryptology ePrint Archive*, 2018.

[140] L. Lab. Second life terms and conditions. [Online]. Available: https://www.lindenlab.com/legal/second-life-terms-and-conditions

[141] D. Kuhn. (2022) What you own when you own an nft. [Online]. Available: https://www.coindesk.com/layer2/2022/01/17/what-you-own-when-you-own-an-nft/

[142] Blizzard. (2022) Trading items and services for real money. [Online]. Available: https://us.battle.net/support/en/article/269874

[143] K. Games. (2022) Archeage bans accounts for real money trade. [Online]. Available: https://mmohaven.com/blog/2022/02/04/archeage-bans-accounts-for-real-money-trade/

[144] J. Bruene. (2006) Truly virtual banking in second life. [Online]. Available: https://finovate.com/virtual-banking-second-life/

[145] T. Janckus. (2018) Offensive and illegal content online threatens adults as well as children. [Online]. Available: https://www.delfi.lt/en/politics/offensive-and-illegal-content-online-threatens-adults-as-well-as-children.d?id=79577539

[146] SEC. (2021) Sec charges three media companies with illegal offerings of stock and digital assets. [Online]. Available: https://www.sec.gov/news/press-release/2021-175

[147] J. R. Schlimgen, "Virtual world, real taxes: A sales and use tax adventure through second life starring dwight schrute," *Minn. JL Sci. & Tech.*, vol. 11, p. 877, 2010.

[148] M. Phadtare. (2022) Crypto currency and its taxation in different countries. [Online]. Available: https://regtechtimes.com/cryptocurrency-taxation-in-different-countries/

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

[150] H. R. Hasan and K. Salah, "Combating deepfake videos using blockchain and smart contracts," *IEEE Access*, vol. 7, pp. 41 596–41 606, 2019, doi: 10.1109/ACCESS.2019.2905689.

[151] M. Antolin. (2022) What is proof-of-authority? [Online]. Available: https://www.coindesk.com/learn/what-is-proof-of-authority/

[152] J. Yao, S. Lee, and S. Nam, "Privacy preserving drm solution with content classification and superdistribution," in *Proc. 6th IEEE Consumer Communications and Networking Conference*. IEEE, 2009, pp. 1–5, doi: 10.1109/CCNC.2009.4784776.

[153] Q. Chen, G. Srivastava, R. M. Parizi, M. Aloqaily, and I. Al Ridhawi, "An incentive-aware blockchain-based solution for internet of fake me-

dia things," *Information Processing & Management*, vol. 57, no. 6, p. 102370, 2020, 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," *Procedia Computer Science*, vol. 199, pp. 580–588, 2022, doi: 10.1016/j.procs.2022.01.071.
[155] Y. Amir and A. Wool, "Optimal availability quorum systems: Theory and practice," *Information Processing Letters*, vol. 65, no. 5, pp. 223–228, 1998, doi: 10.1016/S0020-0190(98)00017-9.
[156] W. Ku and C.-H. Chi, "Survey on the technological aspects of digital rights management," in *Proc. International Conference on Information Security*. Springer, 2004, pp. 391–403, doi: 10.1007/978-3-540-30144-8_33.
[157] S. Subramanya and B. K. Yi, "Digital rights management," *IEEE potentials*, vol. 25, no. 2, pp. 31–34, 2006, doi: 10.1109/MP.2006.1649008.
[158] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, 2015, doi: 10.1109/MC.2015.33.
[159] 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 International Conference on Services Computing (SCC)*. IEEE, 2018, pp. 193–200, doi: 10.1109/SCC.2018.00032.
[160] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaria, "To blockchain or not to blockchain: That is the question," *It Professional*, vol. 20, no. 2, pp. 62–74, 2018, doi: 10.1109/MITP.2018.021921652.
[161] J. Golosova and A. Romanovs, "The advantages and disadvantages of the blockchain technology," in *Proc. IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)*. IEEE, 2018, pp. 1–6, doi: 10.1109/AIEEE.2018.8592253.
[162] "IEEE Standard for Blockchain-based Digital Asset Management," Blockchain Standards Committee, IEEE Consumer Technology Society, Standard, Mar. 2022.
[163] N. Thompson. (2022) It's complicated: The relationship between crypto and nfts. [Online]. Available: https://www.coindesk.com/layer2/2022/03/07/its-complicated-the-relationship-between-crypto-and-nfts/
[164] W. A. Kaal, S. Evans, and H. Howe, "Digital asset valuation," *Available at SSRN 4033886*, 2022, doi: 10.2139/ssrn.4033886.
[165] T. Glas, *Asset Pricing and Investment Styles in Digital Assets: A Comparison with Traditional Asset Classes*. Springer Nature, 2022.
[166] S. Bernstrom, *Valuation: the market approach*. John Wiley & Sons, 2014.
[167] L. Kruschwitz and A. Löffler, *Discounted cash flow: a theory of the valuation of firms*. John Wiley & Sons, 2006.
[168] M. Ghaeli, "Price-to-earnings ratio: A state-of-art review," *Accounting*, vol. 3, no. 2, pp. 131–136, 2017, doi: 10.5267/j.ac.2016.7.002.
[169] I. Fisher, ""the equation of exchange," 1896-1910," *The American Economic Review*, vol. 1, no. 2, pp. 296–305, 1911.
[170] W. H. Buiter, "The fiscal theory of the price level: A critique," *The Economic Journal*, vol. 112, no. 481, pp. 459–480, 2002, doi: 10.1111/1468-0297.00726.
[171] V. Buterin. (2017) On medium-of-exchange token valuations. [Online]. Available: https://vitalik.ca/general/2017/10/17/moe.html
[172] W. Woo. (2017) Introducing nvt ratio (bitcoin's pe ratio), use it to detect bubbles. [Online]. Available: https://woobull.com/introducing-nvt-ratio-bitcoins-pe-ratio-use-it-to-detect-bubbles/
[173] J. Todaro. (2018) Valuing crypto assets using a dcf model. [Online]. Available: https://medium.com/@john_19547/valuing-crypto-assets-using-a-dcf-model-bc6297b0bd25
[174] N. Polyakova and T. Yakushkina, "Token valuation: Business perspective."
[175] A. Russell, "Cash flows in networks," *Management Science*, vol. 16, no. 5, pp. 357–373, 1970, doi: 10.1287/mnsc.16.5.357.
[176] 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 Networking and Applications*, vol. 14, no. 5, pp. 2665–2680, 2021, doi: 10.1007/s12083-020-01023-z.
[177] G. Caldarelli, "Understanding the blockchain oracle problem: A call for action," *Information*, vol. 11, no. 11, p. 509, 2020, doi: 10.3390/info11110509.
[178] S. Woo, J. Song, and S. Park, "A distributed oracle using intel sgx for blockchain-based iot applications," *Sensors*, vol. 20, no. 9, p. 2725, 2020.
[179] L. Lys and M. Potop-Butucaru, "Distributed blockchain price oracle," Ph.D. dissertation, LIP6, 2022.
[180] D. D. F. Maesa, P. Mori, and L. Ricci, "Blockchain based access control services," in *Proc. IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018, pp. 1379–1386, doi: 10.1109/Cybermatics_2018.2018.00237.
[181] 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. 38 431–38 441, 2019, doi: 10.1109/ACCESS.2019.2905846.
[182] 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 Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 942–954, 2020, doi: 10.1109/JSAC.2020.2980916.
[183] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an internet of things environment," *The Journal of Supercomputing*, vol. 73, no. 3, pp. 1152–1167, 2017, doi: 10.1007/s11227-016-1870-0.
[184] Y. Feng, W. Zhang, X. Luo, and B. Zhang, "A consortium blockchain-based access control framework with dynamic orderer node selection for 5g-enabled industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2840–2848, 2021, doi: 10.1109/TII.2021.3078183.
[185] S. Hu, Y.-C. Liang, Z. Xiong, and D. Niyato, "Blockchain and artificial intelligence for dynamic resource sharing in 6g and beyond," *IEEE Wireless Communications*, vol. 28, no. 4, pp. 145–151, 2021, doi: 10.1109/MWC.001.2000409.
[186] Z. Zhou, X. Chen, Y. Zhang, and S. Mumtaz, "Blockchain-empowered secure spectrum sharing for 5g heterogeneous networks," *IEEE Network*, vol. 34, no. 1, pp. 24–31, 2020, doi: 10.1109/MNET.001.1900188.
[187] G. O. Boateng, D. Ayepah-Mensah, D. M. Doe, A. Mohammed, G. Sun, and G. Liu, "Blockchain-enabled resource trading and deep reinforcement learning-based autonomous ran slicing in 5g," *IEEE Transactions on Network and Service Management*, vol. 19, no. 1, pp. 216–227, 2021, doi: 10.1109/TNSM.2021.3124046.
[188] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Low-latency federated learning and blockchain for edge association in digital twin empowered 6g networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 5098–5107, 2020, doi: 10.1109/TII.2020.3017668.
[189] S. Badruddoja, R. Dantu, Y. He, M. Thompson, A. Salau, and K. Upadhyay, "Trusted ai with blockchain to empower metaverse," in *Proc. Fourth International Conference on Blockchain Computing and Applications (BCCA)*. IEEE, 2022, pp. 237–244, doi: 10.1109/BCCA55292.2022.9922027.
[190] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4298–4311, 2020, doi: 10.1109/TVT.2020.2973651.
[191] B. Falchuk, S. Loeb, and R. Neff, "The social metaverse: Battle for privacy," *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 52–61, 2018, doi: 10.1109/MTS.2018.2826060.
[192] 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 International Conference on Blockchain (Blockchain)*. IEEE, 2022, pp. 71–78, doi: 10.1109/Blockchain55522.2022.00020.
[193] 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 Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2438–2455, 2019, doi: 10.1109/TDSC.2019.2952332.
[194] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, "Privacy-preserving blockchain-based federated learning for iot devices," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1817–1829, 2020, doi: 10.1109/JIOT.2020.3017377.
[195] 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 International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*. IEEE, 2017, pp. 468–477, doi: 10.1109/CCGRID.2017.8.
[196] M. Li, J. Weng, A. Yang, W. Lu, Y. Zhang, L. Hou, J.-N. Liu, Y. Xiang, and R. H. Deng, "Crowdbc: A blockchain-based decentralized framework for crowdsourcing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 6, pp. 1251–1266, 2018, doi: 10.1109/TPDS.2018.2881735.

[197] J. Chen, Z. Zhan, K. He, R. Du, D. Wang, and F. Liu, "Xauth: Efficient privacy-preserving cross-domain authentication," *IEEE Transactions on Dependable and Secure Computing*, 2021, doi: 10.1109/TDSC.2021.3092375.
[198] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in iot," in *Europe and MENA cooperation advances in information and communication technologies*. Springer, 2017, pp. 523–533, doi: 10.1007/978-3-319-46568-5_53.
[199] M. Chanson, A. Bogner, D. Bilgeri, E. Fleisch, and F. Wortmann, "Blockchain for the iot: privacy-preserving protection of sensor data," *Journal of the Association for Information Systems*, vol. 20, no. 9, pp. 1274–1309, 2019, doi: 10.17705/1jais.00567.
[200] 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, 2019, doi: 10.3390/s19020326.
[201] Omnimint. (2022) Japanese nft task force asks government to appoint web3 minister. [Online]. Available: https://content.collectorx.io/2022/04/news/japanese-nft-task-force-asks-government-to-appoint-web3-minister/
[202] P. Bond. (2022) Eu, south korea, japan announce metaverse regulation plans. [Online]. Available: https://www.hklaw.com/en/insights/publications/2022/09/eu-south-korea-japan-announce-metaverse-regulation-plans/
[203] S. Paul, J. I. Joy, S. Sarker, S. Ahmed, A. K. Das *et al.*, "Fake news detection in social media using blockchain," in *Proc. 7th International Conference on Smart Computing & Communications (ICSCC)*. IEEE, 2019, pp. 1–5, doi: 10.1109/ICSCC.2019.8843597.
[204] 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 Professional*, vol. 21, no. 4, pp. 16–24, 2019, doi: 10.1109/MITP.2019.2910503.
[205] Z. Shahbazi and Y.-C. Byun, "Fake media detection based on natural language processing and blockchain approaches," *IEEE Access*, vol. 9, pp. 128 442–128 453, 2021, doi: 10.1109/ACCESS.2021.3112607.
[206] S. Mackenzie, "Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial," *The British Journal of Criminology*, 2022, doi: 10.1093/bjc/azab118.
[207] P. N. Sureshbhai, P. Bhattacharya, and S. Tanwar, "Karuna: A blockchain-based sentiment analysis framework for fraud cryptocurrency schemes," in *Proc. IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2020, pp. 1–6, doi: 10.1109/ICCWorkshops49005.2020.9145151.
[208] W. Chen, X. Guo, Z. Chen, Z. Zheng, and Y. Lu, "Phishing scam detection on ethereum: Towards financial security for blockchain ecosystem." in *Proc. IJCAI*, 2020, pp. 4506–4512.
[209] H. Hu, Q. Bai, and Y. Xu, "Scsguard: Deep scam detection for ethereum smart contracts," in *Proc. IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2022, pp. 1–6, doi: 10.1109/INFOCOMWKSHPS54753.2022.9798296.
[210] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, "The energy consumption of blockchain technology: Beyond myth," *Business & Information Systems Engineering*, vol. 62, no. 6, pp. 599–608, 2020, doi: 10.1007/s12599-020-00656-x.
[211] R. Zhang and W. K. V. Chan, "Evaluation of energy consumption in block-chains with proof of work and proof of stake," in *Proc. Journal of Physics: Conference Series*, vol. 1584, no. 1. IOP Publishing, 2020, p. 012023, doi: 10.1088/1742-6596/1584/1/012023.
[212] N. Lasla, L. Al-Sahan, M. Abdallah, and M. Younis, "Green-pow: An energy-efficient blockchain proof-of-work consensus algorithm," *Computer Networks*, vol. 214, p. 109118, 2022, doi: 10.1016/j.comnet.2022.109118.
[213] C. Chenli, B. Li, Y. Shi, and T. Jung, "Energy-recycling blockchain with proof-of-deep-learning," in *Proc. IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2019, pp. 19–23, doi: 10.1109/BLOC.2019.8751419.
[214] X. Qu, S. Wang, Q. Hu, and X. Cheng, "Proof of federated learning: A novel energy-recycling consensus algorithm," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 8, pp. 2074–2085, 2021, doi: 10.1109/TPDS.2021.3056773.
[215] 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
[216] C. Heidorn. (2022) The 10 most expensive nfts ever sold. [Online]. Available: https://tokenizedhq.com/most-expensive-nft-sold/
[217] Y. Liu. (2021) Dodo research: Nft needs a pricing revolution. [Online]. Available: https://blog.dodoex.io/nft-needs-a-pricing-revolution-f0044b268ae5
[218] Wikipedia. (2021) Poly network exploit. [Online]. Available: https://en.wikipedia.org/wiki/Poly_Network_exploit
[219] 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
[220] E. L. Sidorenko, "Stablecoin as a new financial instrument," in *Proc. International Scientific Conference "Digital Transformation of the Economy: Challenges, Trends, New Opportunities"*. Springer, 2019, pp. 630–638, doi: 10.1007/978-3-030-27015-5_75.
[221] O. Analytica, "Terra stablecoin crash casts spotlight on ecosystem," *Emerald Expert Briefings*, no. oxan-es, doi: 10.1108/OXAN-ES270251.
[222] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, "Blockchain and scalability," in *Proc. IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. IEEE, 2018, pp. 122–128, doi: 10.1109/QRS-C.2018.00034.
[223] S. Farshid, A. Reitz, and P. Roßbach, "Design of a forgetting blockchain: A possible way to accomplish gdpr compatibility," in *Proc. 52nd Hawaii International Conference on System Sciences*, 2019.
[224] M. Florian, S. Henningsen, S. Beaucamp, and B. Scheuermann, "Erasing data from blockchain nodes," in *Proc. IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2019, pp. 367–376, doi: 10.1109/EuroSPW.2019.00047.
[225] 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 an MSc student at the Institut National de la Recherche Scientifique (INRS), University of Quebec, Montreal, QC, Canada. His research focuses on blockchain and enabling technologies for metaverse.

LONG BAO LE (S'04-M'07-SM'12) 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 at Massachusetts Institute of Technology (2008 to 2010) and University of Waterloo (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. His current research interests include smartgrids, radio resource management, network control and optimization, and emerging enabling technologies for 5G and beyond wireless systems. He is a co-author 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). Dr. Le was a member of the editorial board of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and IEEE COMMUNICATIONS SURVEYS AND TUTORIALS.

PLACE PHOTO HERE

DUSIT NIYATO (M'09–SM'15–F'17) received the B.E. degree from the King Mongkuk's 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 and, by courtesy, the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. He has published extensively in the area of wireless and mobile computing. He is an inventor of four U.S. and German patents. He has authored a few books, including Dynamic Spectrum Access and Management in Cognitive Radio Networks, Game Theory in Wireless and Communication Networks: Theory, Models, and Applications, and Wireless Device-to-Device Communications and Networks (Cambridge University Press). He is a Highly Cited Researcher, in 2017. He received the Best Young Researcher Award of the IEEE Communications Society (ComSoc) Asia Pacific and the IEEE Communications Society Fred W. Ellersick Prize Paper Award. He was a Guest Editor of the IEEE JSAC. He is also a Distinguished Lecturer of the IEEE Communications Society. He serves as an Area Editor for the IEEE TWC, a Senior Editor of the IEEE WIRELESS COMMUNICATIONS LETTERS, an Editor of the IEEE TCOM, the IEEE COMST, the IEEE TMC, and the IEEE TCCN.