applied sciences

MDPI

Review

Blockchain Integration in the Era of Industrial Metaverse

Dimitris Mourtzis *, John Angelopoulos and Nikos Panopoulos

Laboratory for Manufacturing Systems and Automation, Department of Mechanical Engineering and Aeronautics, University of Patras, 26504 Rio Patras, Greece
* Correspondence: mourtzis@lms.mech.upatras.gr

Abstract: Blockchain can be realized as a distributed and decentralized database, also known as a "distributed ledger," that is shared among the nodes of a computer network. Blockchain is a form of democratized and distributed database for storing information electronically in a digital format. Under the framework of Industry 4.0, the digitization and digitalization of manufacturing and production systems and networks have been focused, thus Big Data sets are a necessity for any manufacturing activity. Big Data sets are becoming a useful resource as well as a byproduct of the activities/processes taking place. However, there is an imminent risk of cyberattacks. The contribution of blockchain technology to intelligent manufacturing can be summarized as (i) data validity protection, (ii) inter- and intra-organizational communication organization, and (iii) efficiency improvement of manufacturing processes. Furthermore, the need for increased cybersecurity is magnified as the world is heading towards a super smart and intelligent societal model, also known as "Society 5.0," and the industrial metaverse will become the new reality in manufacturing. Blockchain is a cutting-edge, secure information technology that promotes business and industrial innovation. However, blockchain technologies are bound by existing limitations regarding scalability, flexibility, and cybersecurity. Therefore, in this literature review, the implications of blockchain technology for addressing the emerging cybersecurity barriers toward safe and intelligent manufacturing in Industry 5.0 as a subset of Society 5.0 are presented.

Keywords: blockchain; metaverse; cybersecurity

Citation: Mourtzis, D.; Angelopoulos, J.; Panopoulos, N. Blockchain Integration in the Era of Industrial Metaverse. *Appl. Sci.* **2023**, *13*, 1353. https://doi.org/10.3390/app13031353

Academic Editor: Roberto Saia

Received: 22 December 2022
Revised: 12 January 2023
Accepted: 18 January 2023
Published: 19 January 2023

1. Introduction

Blockchain technology can be defined as a growing list of records, which are known as blocks. The innovation of blockchain technology, beyond the creation and maintenance of a continuous list of records, is the improvement of digital transaction security and anonymity based on the implementation of cryptography algorithms. For a peer to insert a new block into the blockchain, that specific block must be followed by a cryptographic hash (i.e., a unique code) that is connected to the preceding block. Each new block consists of two key parts, namely the block header and the block body. The structure of the block header includes the version number, a timestamp, a target hash bit of the current block, a nonce, the hash value of the previous block, and a Merkel root. The detailed data of transactions are stored in the block body. More specifically, additional attributes, such as a timestamp, and transaction data are also included in the new block, thus ensuring the continuity of the information. Consequently, it becomes apparent that the blockchain is by definition resistant to modification of its data. Timestamping and hashing processes are required before a new block is added to the chain; thus, the data of the blockchain can be traced back and are transparent to everyone who participates in the blockchain. Essentially, the blockchain can also be considered a distributed, shared database. In Figure 1, the operating principle of the blockchain for the addition of new blocks is described.

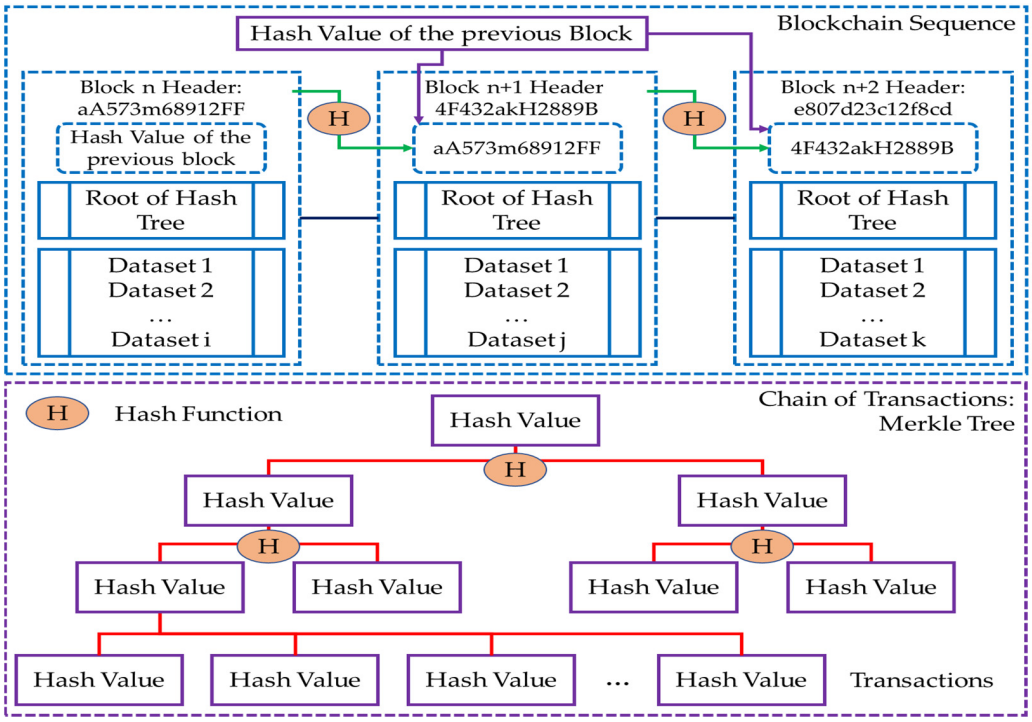

Figure 1. The operating principle of blockchain.

One of the most important processes that take place in the blockchain is "mining." The term "mining" is loosely defined by many as the process of creating, i.e., digitally generating, new cryptocurrency coins.

However, it is a much more involving process that is used for the validation of digital transactions and thus the creation of new blocks in the chain, i.e., the digital and distributed ledger. One of the most important processes in the blockchain is the admission of the required rights to the miners in order to add a new block and consequently to create the latest version of the blockchain. Therefore, whenever a new block is added to the chain, a new link is created starting from the initial block, the so-called "genesis block," creating a continuous history of transactions. The mining operation is accompanied by the consensus agreement process, which is investigated in the following paragraphs. The consensus process is required since the digital ledger lacks a centralized authority. Consequently, the miners are rewarded for their work securing the network with the provision of new digital coins (cryptocurrency).

The infrastructure of the blockchain can be realized as a six-layer framework (Figure 2), namely (i) application, (ii) contract, (iii) incentive, (iv) consensus, (v) network, and (vi) data layers. More specifically, in the application layer, a plethora of application scenarios are included. Then, the contract layer compiles the necessary algorithmic backend, e.g., code scripts, algorithms, and smart contracts. The incentive layer is used in conjunction with the consensus layer to ensure the reward of each node for the work accomplished on the network. The latter can be realized by the issuance of tokens to the miners after the completion of their task. Among the most important layers is the consensus layer, which encapsulates the consensus mechanism. The consensus mechanism is important in the current blockchain implementations (i.e., permissioned blockchains) since it provides the necessary framework for all the participants of the blockchain (i.e., the nodes) to achieve agreement. It is stressed that two types of blockchain exist considering the admittance of new nodes: permissioned and permissionless blockchain [1–3]. The network layer consists of the networking functionalities required for the communication between the nodes, the data exchange framework, and the data verification framework. Finally, the

data layer encapsulates the data included in the blocks and supports the encryption and timestamp processes.

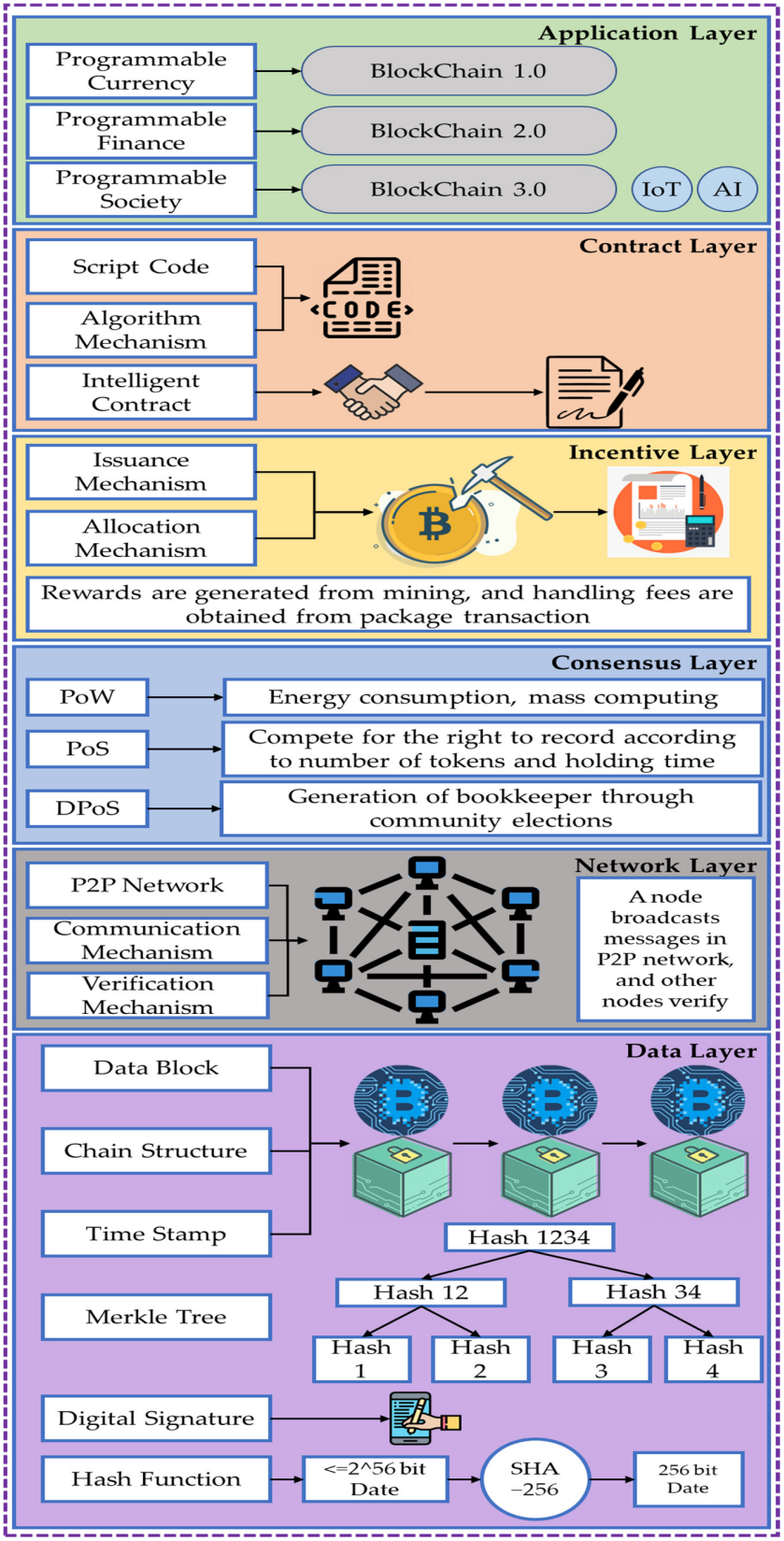

Figure 2. Layered infrastructure of blockchain.

Based on the above-mentioned, this review paper investigates several challenges and research directions of blockchain integration in the metaverse. The key challenges and contributions of the presented research work are listed below:

- Significant technical challenges still need to be addressed:
  - Cybersecurity issues;
  - Energy consumption of blockchain;
  - Interoperability.
- Regulatory challenges protecting human rights:
  - Privacy issues;
  - Web 3.0's copyright promises to support the creator economy by ensuring the fair use of assets;
  - Enforceability of regulatory frameworks.
- Economic challenges for a successful metaverse:
  - Stability of tokens, currencies, and blockchain systems;
  - The high concentration of financial players and institutions in the metaverse.
- Ethical challenges for a human-centric metaverse:
  - What ethical standards and limitations will govern this new cyber-physical metaverse, where identity will be a fluid concept and regulatory oversight will be weak?
- 5G technology opportunities:
  - Immersion;
  - Immediacy;
  - Consistency.
- Blockchain-as-a-service and application programming interface (API) opportunities.

2. Historical Evolution of the Blockchain

In the following Figure 3, the key milestones achieved from the mid-seventies up to 2019 are illustrated. This serves as an indication of the importance of cryptography as well as the development of algorithms and frameworks for the improvement of security in data transmission for digital transactions.

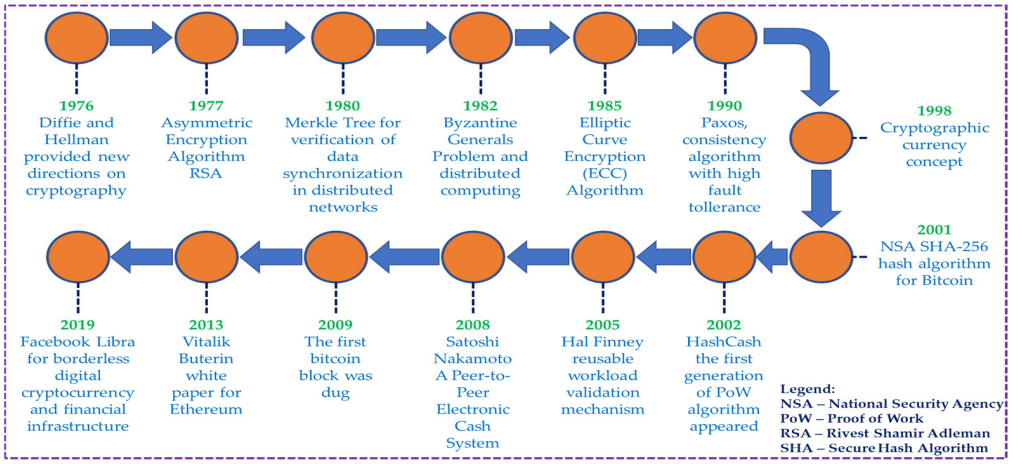

Figure 3. Historical evolution of blockchain: key milestones.

In the timeline presented in Figure 3, the cornerstone algorithmic developments regarding blockchain are illustrated. However, as it will be discussed in greater detail in the next section, five distinct evolutions for blockchain can be extracted in parallel to the Industrial Revolution. In the following paragraph, the blockchain revolutions are presented, discussed, and compared with each other to highlight the key accompanying

technological advances. In Figure 4, the historical evolution of blockchain is illustrated from the perspective of five distinct eras. In the illustration, the chronological boundaries are also set to facilitate the reader's comprehension of the evolution of blockchain along the technological, industrial, and societal evolution through the years.

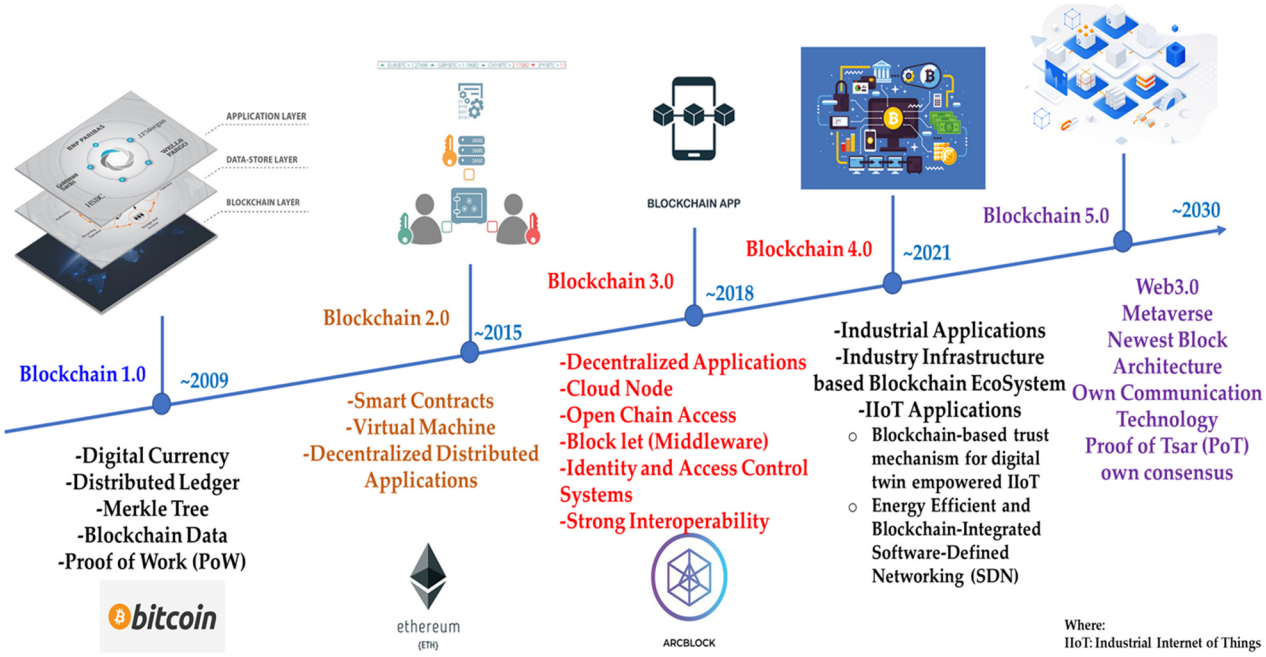

Figure 4. Evolution from Blockchain 1.0 up to Blockchain 5.0.

2.1. Blockchain 1.0

In the early 1990s, research efforts were focused on the design and development of suitable frameworks for the digitization of transactions in an attempt to facilitate transactions in industries and institutions. The Blockchain 1.0 era is dated from 2008 to 2013. The research efforts yielded interesting results in the field of cryptocurrencies, so that users from both parties can trade without the need for traditional centralized systems [4]. However, one of the key issues following the introduction of digital transactions and cryptocurrencies is double spending. Double spending induces additional risks of fraudulent activities.

Consequently, the first generation of blockchain, i.e., Blockchain 1.0, evolved on the principle of Digital Ledger Technology (DLT), which has enabled all the participants of a distributed network to keep track of a common record and thus eliminate certain challenges, such as double spending [5]. As a result, Bitcoin, the first type of cryptocurrency, has been developed and released by Satoshi Nakamoto in 2008, based on the principle of decentralization, promising security, verifiability, and efficiency of digital transactions [6]. Taking into consideration the above-mentioned, the key benefits of Blockchain 1.0 can be summarized as follows:

- Enhanced network reliability is achieved by masking the identity of users or organizations, thus increasing the privacy of users.
- Transparent communication between the network participants is possible as long as the users satisfy the conditions of the consensus mechanism.
- Operation costs are reduced due to the use of a decentralized and distributed network versus the higher cost of conventional systems.

In Figure 5, the workflow of bitcoin transactions between two users is illustrated based on the framework of blockchain technology. The concept illustrated below involves the most simple form of transaction, i.e., the transfer of cryptocurrency from user X to user Y.

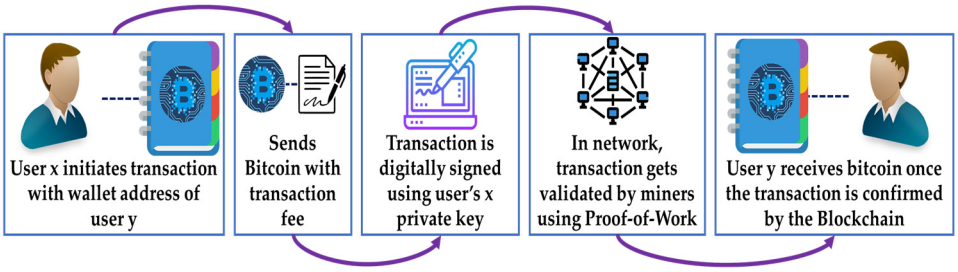

Figure 5. Peer-to-peer transactions in bitcoin.

Despite the added value in digital transactions, the first generation of blockchain has unveiled some key challenges requiring further elaboration [7]. Among these challenges are:

- For the validation of transactions, miners are obliged to work simultaneously in order to solve a cryptographic puzzle and adhere to the principles of the Proof of Work (PoW) consensus mechanism. By extension, multiple computing resources and increased computational time are required. Therefore, PoW is not efficient enough.
- Due to the increased computational time and computational resources required, delays in the execution of transactions are induced in the system, which leads to a less-than-optimal user experience.
- Security risks are still present, as there might be corrupt miners within the network who try to corrupt the ledger in an attempt to extract additional revenue/rewards.

2.2. Blockchain 2.0

The second generation of blockchain, i.e., Blockchain 2.0, is dated from 2013 to 2015. The technological advancements of the second generation have been focused on tackling the challenges that emerged during the first era. The key issues are the increased utilization of resources, increased computational time, and poor network scalability. In an attempt to tackle the above-mentioned, a new solution, also known as smart contracts, has been introduced. The implementation of smart contracts works in conjunction with the PoW consensus mechanism [8]. As indicated in the research work of Saini et al., in 2021 [9], the smart contract can be realized as a self-executable code that is part of the blockchain, to eliminate the risk of interruption. However, it has to be stressed that smart contracts should not be compared with or confused with traditional contracts. In the following Table 1, a comparative analysis between the two types of contracts is presented to highlight their similarities and key differences.

Table 1. Comparison of a traditional contract versus a smart contract.

Parameter	Traditional Contract	Smart Contract
Documents required	Several legal documents required	None
Transaction settlement time	Several hours	$\leq$60 s
Availability	Time-consuming	Easily and readily available
Processing method	Manual	Automatic
Security	Limited	Cryptographic security
Transaction cost	Expensive	Virtually free
Signature	Manual	Digital
Operation mode	Manual	Automatically triggered

From reference [10], a new blockchain platform, also known as the Ethereum platform, that exploits smart contracts, was developed in 2015 (Figure 6). Specifically, on the Ethereum platform, Solidity is utilized for the scripting of the smart contracts, which is a high-level object-oriented programming language. The cryptocurrency used on the Ethereum platform is ether.

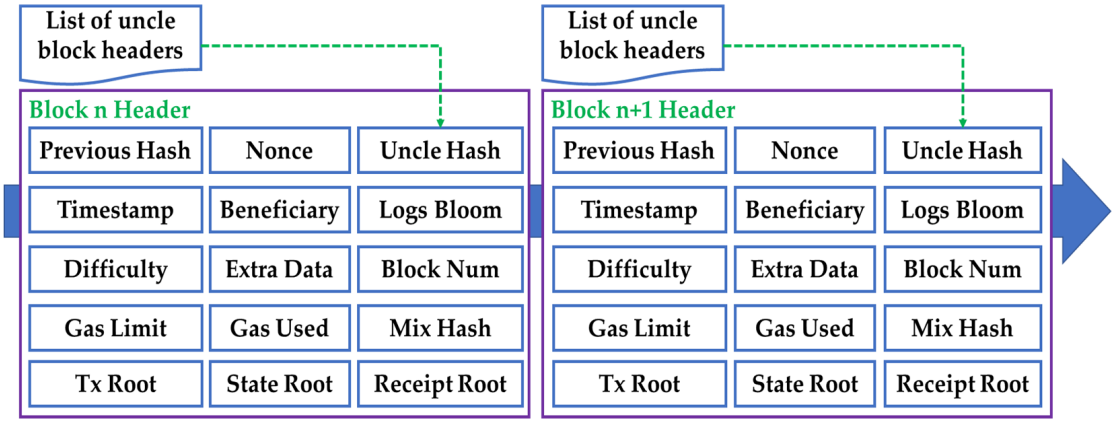

Figure 6. Example of block data structure for the Ethereum blockchain.

Similarly, the key implications of the adoption of Blockchain 2.0 can be summarized in [11]:

- The addition of Ethereum to Blockchain 2.0 has extended its usability for financial organizations as a result of its enhanced security and privacy.
- The level of transparency in the communication between users has been enhanced by the integration of smart contracts.
- By integrating smart contracts, an increased data rate for digital transactions can be achieved.

In Figure 7, a typical workflow and the steps and processes involved in a smart contract between two peers are illustrated. As can be seen from the illustration, the exchange of the assets is efficiently performed, and if only, then the smart contract conditions are satisfied.

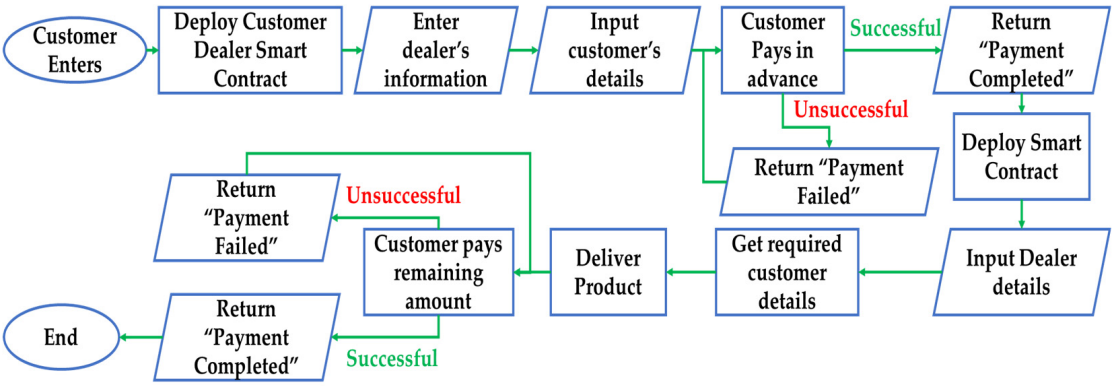

Figure 7. Smart contract execution between peers.

2.3. Blockchain 3.0

Considering the discussion of the two previous blockchain generations, it can be concluded that the key issue in the network is a lack of scalability. The utilization of the PoW mechanism requires excessive computational time and resources. Consequently, in the new era of blockchain, i.e., Blockchain 3.0, new techniques have been introduced, such as sharding and decentralized applications (DApps). The third era of blockchain is chronologically placed between 2015 and 2017. However, it is stressed that the concept of smart contracts has been preserved. DApps mainly work in the backend to provide the network users and applications with the necessary connectivity with the smart contract in a distributed manner; thus, the operation of a centralized server is no longer required in the blockchain network [12]. Alternatively, sharding resembles a new technique that can be used for the improvement of network scalability. More specifically, sharding is used to split the existing network into a cluster of smaller networks/groups. Furthermore, in Blockchain

3.0, the consensus mechanisms have also been revised. Towards this direction, instead of relying solely on the implementation of the PoW mechanism, additional mechanisms, such as Proof of Stake (PoS), Proof of History (PoH), Proof of Activity (PoA), and Proof of Authority (PoA), have been investigated. A list of the available consensus mechanisms available to date is presented in Figure 8. Ultimately, the combination of the consensus mechanisms and the sharding technique targets the enhancement of user privacy and the improvement of trust. Consequently, intrusions targeted at the identification of the transaction's identity are more easily blocked since they are processed by different blocks.

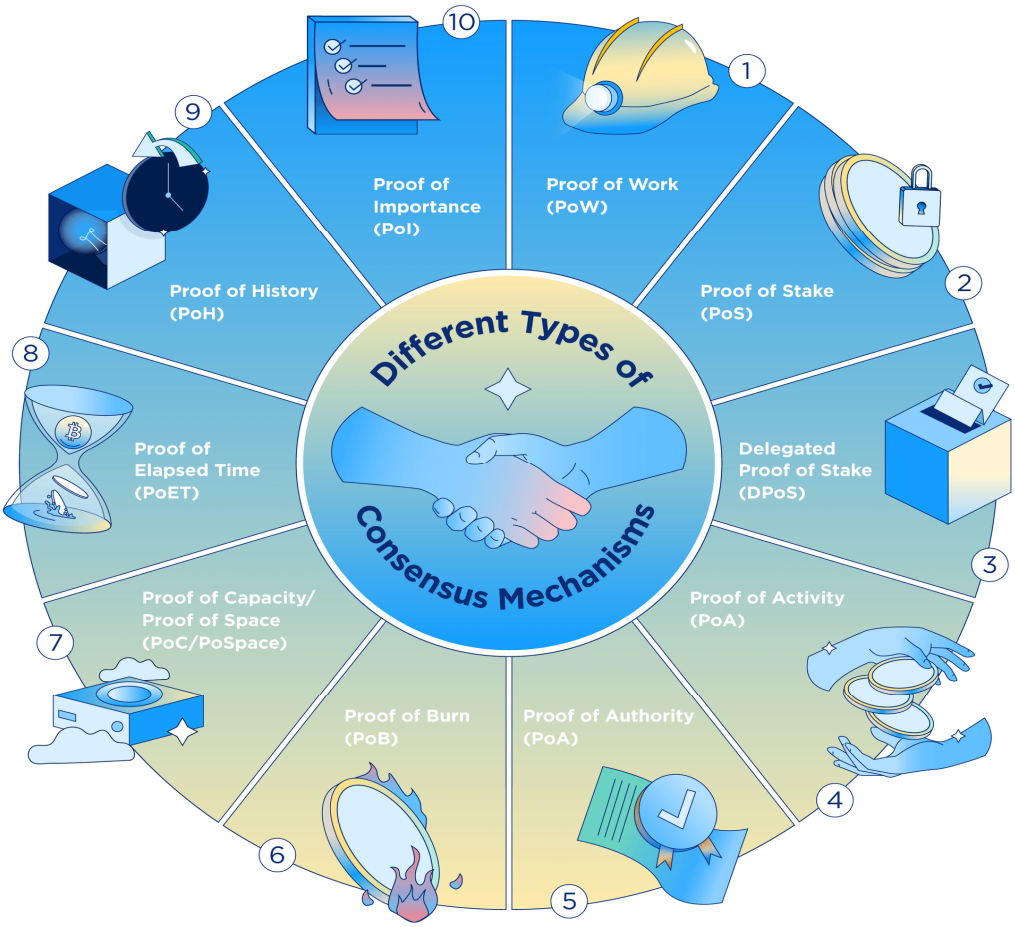

Figure 8. Consensus Mechanisms in Blockchain Technology [13].

The backbone of all cryptocurrency blockchains is formed by consensus mechanisms. Essentially, consensus mechanisms are responsible for the security issues of the blockchain. In order to ensure that every node participating in a blockchain network agrees on a singular version of the ledger, consensus mechanisms are necessary. Consensus mechanisms can be realized as a set of rules that facilitate the protection of networks from malicious behavior and cyberattacks. There are several types of consensus mechanisms, which mainly differ in the energy requirements, the security level they offer, and the scalability level. In the following paragraphs, the most common consensus mechanisms are presented and discussed.

2.3.1. Proof of Work (PoW)

The first consensus mechanism ever implemented on the blockchain is the so-called Proof of Work (PoW). PoW is considered the most reliable and secure mechanism so far implemented on the blockchain, despite the underlying scalability issues. Regarding mining, PoW offers equally to all users the capability to "mine" a new block in the network.

Consequently, the pool of miners competes against each other in order to solve very complex cryptographic mathematical problems. The miner who wins is the first to calculate a 64-digit hexadecimal number, i.e., the hash number, thus granting the miner the necessary rights to verify the transaction on the ledger and award them with cryptocurrency tokens. Consequently, PoW requires large amounts of computational resources and energy for the creation and addition of new blocks, and by extension, the operating costs are high.

2.3.2. Proof of Stake (PoS)

In a Proof of Stake (PoS) system, the miners are required to pledge a certain number of tokens from their account, also known as "staking," so that they can be randomly selected as validators. The selection of the miners is dependent on the amount of cryptocurrency available. In comparison to PoW, PoS only rewards the miner with transaction fees instead of additional cryptocurrency. Considering the operating principle of PoS vs. PoW, the former is more environmentally friendly since the miner's computational resources are not the highest criterion. Furthermore, PoS is more resistant to 51% of attacks. It becomes apparent that PoS is profitable for miners/users who possess a higher number of tokens, which by extension can lead to centralization, which is generally not wanted in blockchain networks.

2.3.3. Delegated Proof of Stake (DPoS)

This consensus mechanism can be considered a revision of PoS. The revision is about the selection of candidate miners, which is based on a network voting system. The users of the network are provided with the rights to vote for the suitable nodes, which have the necessary credentials for producing new blocks. Voters gain their right to vote by adding their tokens to a staking pool. Each vote is weighted based on the stake size the user has put in the stake pool. Whenever a digital transaction is verified, the elected witnesses are rewarded, and they are responsible for sharing the reward with their voters. Considering that voters pledge an amount of their tokens and then vote on the suitability of nodes to contribute to the blockchain process, DPoS is a more democratic and efficient consensus mechanism than its predecessor.

2.3.4. Proof of Activity (PoA)

From the combination of PoW and PoS mechanisms, the Proof of Activity (PoA) mechanism has been derived. Following the mining process of PoW, in PoA, the pool of miners competes in order to solve a difficult mathematical problem and rely on their computational resources. As soon as a block has been mined, the PoS mechanism is employed so that the details of the new block are shared with the rest of the network. Subsequently, a group of randomly selected validators is responsible for signing off on the hash and ultimately validating the addition of the new block. In a similar fashion, in PoA, the possibility of a validator being selected is affected by the validator's total holds, and the rewards are shared between the miners and the validators.

2.3.5. Proof of Authority (PoA)

In blockchains implementing the Proof of Authority (PoA) consensus mechanism, validators are selected based on their reputation ranking. In PoA, validators are not based on cryptocurrency coins; instead, they use their reputation in order to gain the necessary rights required for the block validation. PoA is differentiated from the mechanisms discussed so far since the identity of the validator is revealed to the network. Another advantage of the PoA mechanism is its minimal computing power requirements, which makes it a suitable solution for private networks.

2.3.6. Proof of Burn (PoB)

Another alternative consensus mechanism to the PoW that is more sustainable is the so-called Proof of Burn (PoB). The innovation of the PoB relies on the process of burning a predefined number of tokens in order to provide the miner with the necessary block

mining rights. However, the burning process has to be verifiable. For example, miners send the tokens to a predefined address, from where they cannot be recovered or spent. By increasing the number of tokens burned, the possibility of a miner being selected increases. However, it is stressed that burnt coins cannot be retrieved and sold by their owners. As a result, this method promotes the long-term commitment of miners to the network. However, investing coins through the process of "burning" leads to a currency shortage, which in turn facilitates limiting inflation.

2.3.7. Proof of Capacity/Proof of Space (PoC/PoSpace)

Proof of Capacity (PoC), which is also known as Proof of Space (PoSpace), is based on the utilization of a mining algorithm in which the main selection criterion is the available space on the miner's hard drive, for granting the mining rights to the miners, instead of making suggestions based on the available computational power or coins staked. In PoC, all the possible hashes are generated beforehand by the miners as part of the plotting process. Due to the limited specialized equipment required, PoC is suitable for commercial use by individuals who are willing to participate in the network. Consequently, PoSpace is a good alternative since fewer energy resources are required and it is based on a more decentralized framework.

2.3.8. Proof of Elapsed Time (PoET)

Proof of Elapsed Time (PoET) promotes trusted computing in order to enforce the implementation of the random waiting times methodology for the creation of new blocks on the network, and it has been mainly implemented on permissioned blockchain platforms. In 2016, Intel developed PoET based on specialized CPU instructions, also known as software guard extensions (SGX). In PoET, the miners are randomly assigned waiting times. As soon as a node is assigned a waiting time, it goes into standby mode. Consequently, the node with the shortest waiting time is granted mining rights. The principle of randomization applied to PoET helps ensure equality and fairness in the selection of miners within the network.

2.3.9. Proof of History (PoH)

Proof of History (PoH) is based on the provision of proof of historical events. PoH has been developed by Solana. Its distinguishing characteristic is the ability to build timestamps into the blockchain network itself, based on the utilization of a sequential-hashing verifiable delay function (VDF) SHA-256. The output of a transaction is used as the input for the next hash, thus creating a continuum of transactions, i.e., a continuum of historical events. Among the key implications of PoH is that VDF can only be executed by a single CPU core, making it a more environmentally friendly mechanism and reducing computational time and resources.

2.3.10. Proof of Importance (PoI)

Proof of Importance (PoI) can be realized as a combinatorial consensus mechanism that is based on several criteria for the selection of miners, such as network activity, the number and size of transactions within a timeframe of thirty days, and cryptocurrency vested. Based on the above-mentioned criteria, a score is automatically calculated for each node, which is later used for selecting the appropriate miner. In comparison to PoS, PoI utilizes additional metrics, thus eliminating the tendency to inherently reward richer users. This is accomplished by considering the contribution of the user to the blockchain network.

Another innovation introduced under the framework of Blockchain 3.0 is the elimination of miners as well as the transaction fee required for the validation of the transactions. The above-mentioned have been replaced by an integrated mechanism, which is also facilitating the reduction of transaction costs [14,15]. The key difference from the transition from Blockchain 2.0 to Blockchain 3.0 is focused on the adaptation of additional consensus mechanisms (see Figure 8) along with the introduction of DApps for making smart contracts even more visible and accessible to the network users [16].

So far, in the previous paragraphs, the innovations of Blockchain 3.0 in contrast to the previous generations have been discussed. Despite the increasing integration of blockchain in a plethora of industries and organizations, innovative digital technologies, such as AI, have not been integrated. Another limitation is that in Blockchain 3.0, consensus mechanisms are more complex and must be implemented along with smart contracts.

2.4. Blockchain 4.0

So far, the previous blockchain generations have not yet adequately achieved the industrial goals; thus, the needs of industries relevant to the technological pillars and advancements of Industry 4.0 are still open for further development [17]. For example, to achieve the required level of industrial automation, a new generation of blockchain is required. The key requirements of Industry 4.0 are the integration of cybersecurity and innovative technologies such as supply chain management [18], the Internet of Things (IoT), and AI. Therefore, the introduction of a new blockchain era, under the name "Blockchain 4.0," following the technological advances to serve businesses with enhanced privacy, security, transparency, and data integrity is required [19]. As a result, InterValue has been utilized for the creation of a Blockchain 4.0 platform. The main target of InterValue with Blockchain 4.0 is to create an improved version of a Directed Acyclic Graph (DAG) with improved scalability, usability, and reliability [20,21].

Blockchain 4.0 applications and their application in various industrial sectors have been discussed in several publications due to the improvements versus its previous generations in terms of scalability, interoperability, and transaction rate [22]. Growing technologies such as blockchain and software-defined networking (SDN) can be used to build secure systems and guarantee secure network connectivity [23]. As a result, in the near future, improvements regarding aspects such as scalability, security, and transparency of the blockchain network are to be expected for industrial implementations.

Based on the discussion in the previous paragraphs regarding the discrete evolutions of blockchain, the following comparative table (Table 2) has been compiled in order to explicitly highlight the key implications of the blockchain evolutions, taking into consideration various parameters, among them the key technology used, the consensus mechanism, the data rate for the completion of digital transactions, etc.

Table 2. Comparative analysis of blockchain evolutions.

Parameter	Blockchain 1.0	Blockchain 2.0	Blockchain 3.0	Blockchain 4.0
Underlying technology	Distributed ledger technology (DLT)	Smart contracts	Decentralized Applications (DApps)	Blockchain with AI
Consensus mechanism	Proof of Work	Delegated Proof of Work	Proof of Stake, Proof of Authority	Proof of Integrity
Validation	By miners	Through smart contracts and miners	In-built verification mechanism via DApps	Automated verification via sharing
Scalability	Non-scalable	Poorly scalable	Scalable	Highly scalable
Intercommunication	Not possible	Not possible	Possible	Possible
Data rate	7 TBS	15 TBS	1000 s of TBS	10^6 TBS
Cost	Expensive	Cheaper	More cheaper	Cost effective
Energy consumption	Highest	Moderate	Energy efficient	Highly efficient
Example	Bitcoin	Ethereum	IOTA, Cardano, Anion	SEELE, Unibright
Application	Financial sector	Non-financial sector	Business platforms	Industry 4.0

3. Beyond the Current Implementations—Blockchain 5.0

Considering the discussion of the previous section, the past blockchain generation provided various benefits by exploiting key digital technologies. During the last decades and through the various blockchain eras discussed earlier, it has become evident that research efforts are focused on key aspects, such as the cost efficiency of this technology as well as the speed of transaction execution/completion measured in terms of data rate. In the last few years, energy efficiency has been among the top requirements since cryptocurrency mining has formed a growing global community with companies creating miner farms. Such miner farms, in pursuit of awards, solve complex cryptographic puzzles, which require tremendous computational power and time. To put this in perspective, the Bitcoin community consumes approximately one hundred and fifty terawatt-hours of electrical power annually, which exceeds the power consumption of an entire country with a forty-five million population. In addition, carbon dioxide emissions (CO_2) are estimated to be sixty-five megatons annually [24–26]. However, the fifth era of blockchain also focuses on matters such as scalability, economic reliability, security, transparency, and confidentiality. The economic reliability and stability of such ecosystems create disbelief in companies towards the integration of blockchain in their business operations model [27,28]. The first commercial implementation of Blockchain 5.0, to the best of our knowledge, is Relictum Pro [29] (Figure 9). The key concept of Relictum Pro is the creation of a network that supports the setup of multiple smart contracts for the execution of transactions, which is expected to outperform competitor solutions in terms of security.

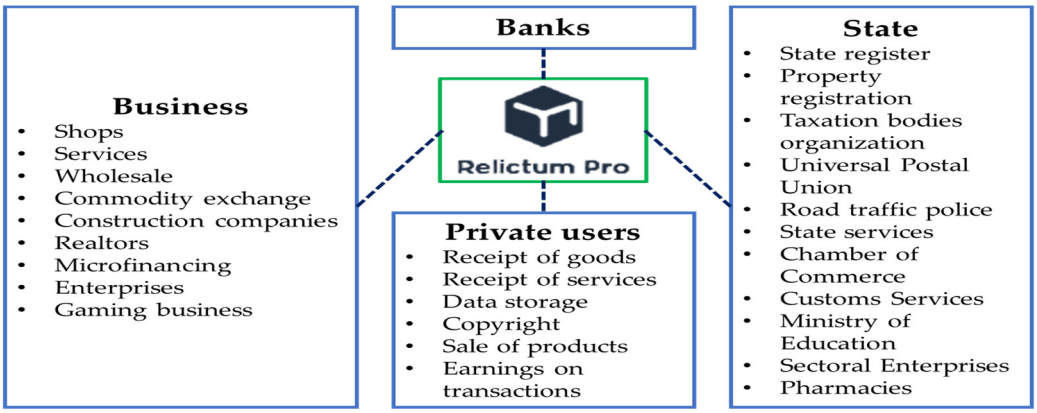

Figure 9. Relictum Pro Framework.

Currently, Relictum Pro is being utilized by several organizations on a worldwide scale, which are focusing on enhancing the features of Blockchain 5.0. This is of great importance since Blockchain 5.0 is superior to its predecessors for the reasons displayed below:

- User digital transactions are stored in a single system in order to ensure data confidentiality for information related to health care or governance.
- Features of advanced digital technologies, such as AI, are exploited for the creation of secure and reliable smart contracts in the network.
- Improvement of industrial performance with the implementation of complex projects with Blockchain 5.0.

3.1. Blockchain and Education

More specifically, the concept of blockchain was coined by Haber and Stornetta, who presented interesting research back in 1991 on how to timestamp digital documents [29]. Since then, the domain of cryptography has been further elaborated, resulting in the current form of blockchain [30,31]. Recent investigations have revealed that the modern industrial world is shifting towards the implementation of the blockchain ecosystem in an attempt to improve transparency of systems, avoid fraudulent activities, and increase

visibility [12,32]. Although blockchain technology is not new, it remains in its infancy, thus there is room for further development of both the techniques (i.e., algorithms) and the required infrastructure for the seamless integration of such technologies [33]. Several frameworks based on blockchain are presented in a multitude of fields [34–37]. Specifically, the applications are related to fields such as security on the Internet of Things (IoT), smart grids, smart cities, etc. It becomes obvious that this technology can benefit many different fields by ensuring data integrity and financial transactions. Additionally, the environment in which higher education institutions (HEIs) operate is more challenging and competitive. During this digitalization era, HEIs are under increasing pressure to respond to ongoing economic, political, and social change, including rising student demand in specific disciplines, embedding workplace attributes in graduates, and ensuring that the quality of learning programs is both nationally and globally relevant [38]. Furthermore, rising levels of fraud and corruption involving higher education degrees and credentials decrease trust levels in the educational system. Thus, a wide range of stakeholders (including academia, the private and public sectors, government administration, industrial researchers, etc.) anticipate that HEIs will adapt to the growing regulatory demands for accountability and transparency [39].

As a result, higher education will inevitably adopt blockchain technology. More specifically, several countries, among them the United States of America and the UK, have already implemented such platforms in an attempt to facilitate educating personnel and students about tracking academic progress and achievements [40,41]. Similarly, in a recent analysis presented in [42], the main areas of contribution of the above-mentioned technology in higher education are analyzed. The authors in reference [43] have focused on the challenges arising in the domain of academic credentialing and have also designed a four-layer architecture in order to evaluate educational credentialing frameworks that have been integrated with blockchain technology. Similarly, Zhang et al., in 2020 [44], investigated the integration of blockchain as a medium for improving data management in higher education by taking advantage of the advanced cryptographic techniques used as well as the decentralization of authority within the network. Considering the above-mentioned, the following challenges emerge regarding blockchain integration in higher education:

1. Reduction of costly academic bureaucracy;
2. Laggs in technology adoption;
3. Democratization and automation of higher education.

Towards this direction, Mourtzis et al., in 2020 [45], proposed a framework integrating blockchain functionalities, aiming at the promotion of collaboration between academia, research organizations, and industrial companies. In the presented framework, the principles of smart contracts have been adopted in order to enable all stakeholders to create digital portfolios of their achievements and digitally ensure the integrity of their academic profiles. One of the key implications of the presented research work is the provision of a framework for the establishment of a common/shared, and decentralized accreditation system for academic students, which ensures that their academic work can be easily recognized in the highly competitive global job market.

3.2. Blockchain and Digital Twin

Under the light of Industry 4.0, nine pillar technologies have been developed and researched. Among them, simulation as a whole and advanced simulation technologies and techniques, such as digital twins, have been at the center of attention [46]. Based on the illustration of the keyword network presented in Figure 10, it can be realized that blockchain technology is highly intertwined with the pillar technologies of Industry 4.0, including the digital twin, the Internet of Things (IoT), and Big Data analytics. Alternatively, the "digital twin," as an umbrella term for advanced simulation technologies and techniques, is highly dependent on Big Data analytics and the direct connection of the physical system with its digital twin. Therefore, new challenges arise regarding the network architecture design to be adopted for information technology, data inference, privacy, and security, as well as

trust beyond the physical boundaries of the company. As a result, blockchain technology can be efficiently implemented along with digital twins to achieve a greater degree of data security and privacy. Furthermore, due to the decentralized features of the distributed ledger, stronger bonds (i.e., trust) with the stakeholders of the supply chain network can be established [47]. In addition, emerging technologies such as blockchain and digital twins are crucial to the industry 5.0 revolution's rapid growth and employment [48]. It is challenging to optimize the network and make the most of scarce resources to enable secure transmission given the rising number of industrial IoT nodes. A digital twin can be realized as a closed-loop control system between the physical object and its digital representation, which is entirely dependent on the constant bilateral data exchange enabled by the utilization of sensing systems. Sasikumar et al., in 2023 [47], combined a digital twin with a distributed network (employing blockchain functionalities) in an attempt to enhance Industrial Internet of Things (IIoT) applications. Among the key contributions of this research work is the presentation of a Proof of Authority (PoA) trust mechanism for the Internet of Things (IIoT).

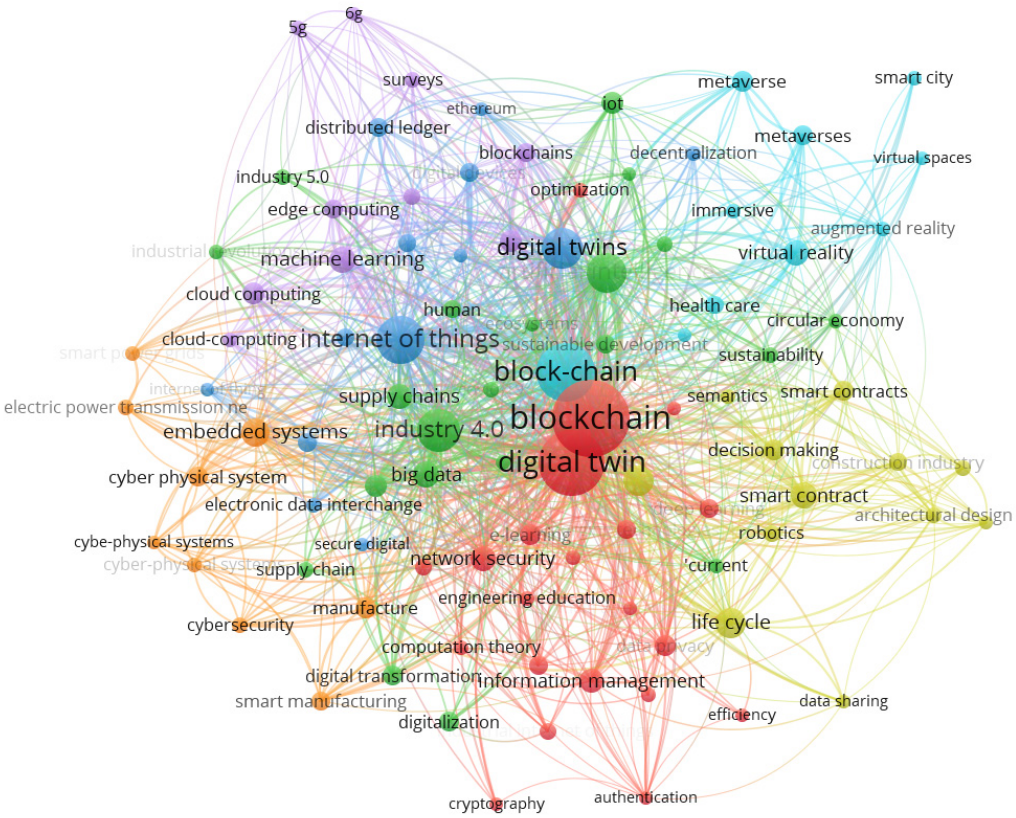

Figure 10. Keyword network for "blockchain," "digital," and "twin."

Inarguably, the global pandemic caused by COVID-19 has stressed not only manufacturing systems but also severely affected supply chains. More specifically, through the last two years, it became more than evident that existing infrastructure and techniques used for the operation and management of supply chains are fragile, have a low level of flexibility, and are very susceptible to failure due to external disturbances [49,50]. However, global production networks as well as global supply networks could benefit from the integration of blockchain, improving their resilience as a result of increased data access accompanied by increased privacy and security [51]. Another aspect covered in the above-mentioned publications is the traceability of products and resources through the information shared by the distributed ledger [52].

An alternative approach to the integration of blockchain technology in digital twins has been proposed by Huang et al., in 2020 [53]. Besides the operational strategy of the company,

it is of equal importance for companies to have better insights throughout the entire lifecycle of their products. Therefore, with the utilization of blockchain, it becomes evident that issues regarding data management and storage, access, and sharing can be tackled with the implementation of a distributed network, the operation of a distributed ledger, and the application of a consensus mechanism between the different parties involved.

3.3. Data Management and Cybersecurity

Despite the notable technological advances presented in the available literature, the challenge of cyber-security is still open regarding blockchain implementations [54,55] (Figure 11). Following the content of the previous section regarding the various consensus mechanisms, it can be concluded that the implementation of a vulnerable consensus mechanism can make a system prone to severe cyberattacks (e.g., a 51% attack, a routine attack, a phishing attack, etc.), thus jeopardizing the operation of the entire blockchain network [56].

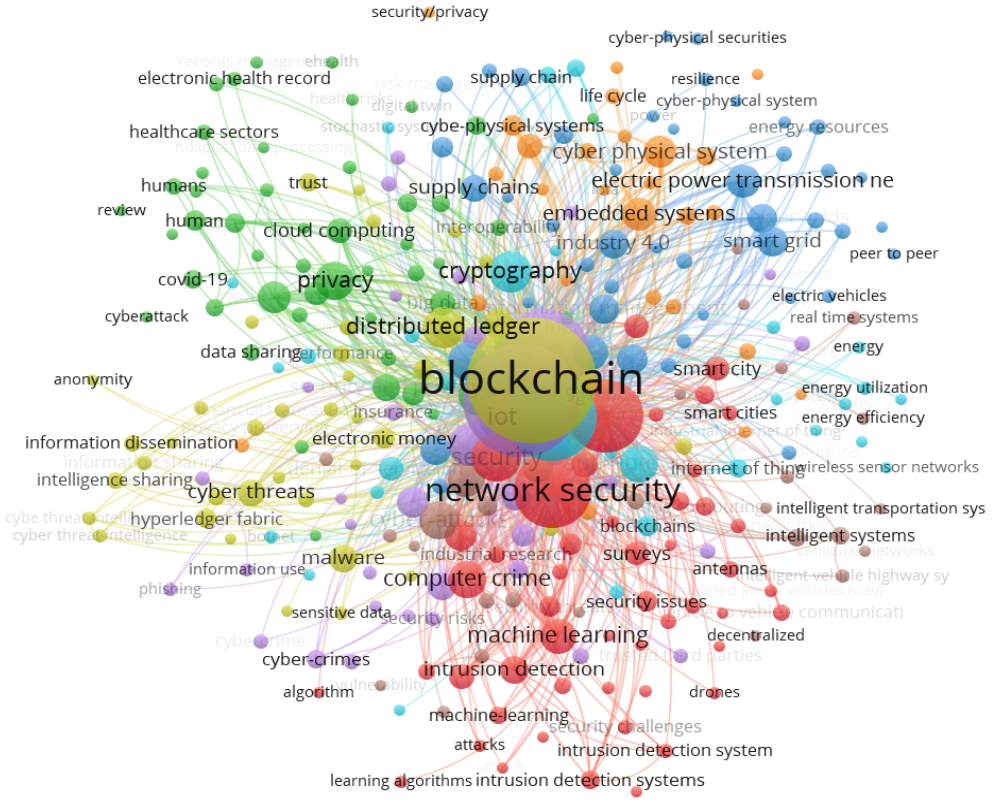

Figure 11. Keyword network for "blockchain" and "cybersecurity."

4. Blockchain in the Era of Society 5.0

Society 5.0 is inherently a technology-driven evolution of Industry 4.0 and the generalization of the upcoming Industry 5.0 (Figure 12). More specifically, three critical areas are targeted: human centricity, resilience, and sustainability of the systems and networks. Ultimately, the goal is to create what has been conceived as a super-smart and intelligent society. Industry 4.0 has its origins in six technological pillars: the digital society, sustainable energy, intelligent mobility, healthy living, civil security, and technology at work. These pillars appeared to have a positive impact on the community. Society 5.0 presumes to consist of the hunting, the agricultural, the industrial, the information (where they collect the successive industrial revolutions and the current fourth), and a fifth that integrates the online with the offline, or what it means, information or cyberspace, with the real physical world in a sustainable way [57,58].

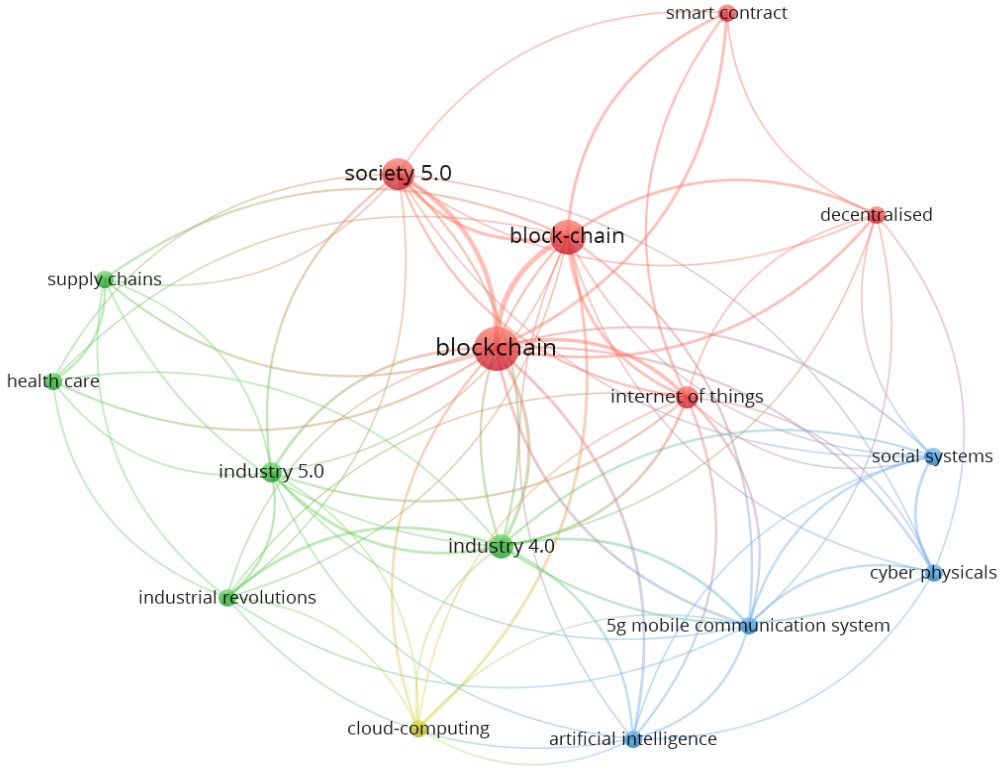

Figure 12. Keyword network for "blockchain" and "Society 5.0."

The main theme of Industry 4.0 is the digitization and digitalization of manufacturing and production systems and networks for the creation of insights and intelligence. During the last decade, an exponential technological advance has been noted, which has laid the foundations for an entirely new level of automation and the realization of Society 5.0. The ecosystem known as "Society 5.0" will promote economic, environmental, social, and political sustainability while putting a strong emphasis on people and the creation of added value. It is a notion that expands beyond the business model of Industry 4.0 [57,59].

With the integration of technologies introduced in Industry 4.0, such as cloud computing, IoT, and artificial intelligence, next-generation machine communications can become a reality. Therefore, challenges in security, connectivity, centralization, lack of latency, lack of accuracy, hardware capabilities, etc., will emerge [60].

5. Blockchain Integration in Metaverse

The developments and technological advancements presented in the previous paragraphs in the field of blockchain technology have led many businesses to experiment with the design and development of proprietary blockchain platforms (Figure 13). The objective of the metaverse is the provision of a scalable, safe, and user-friendly blockchain platform. Furthermore, the metaverse also focuses on the creation of digital assets and smart contracts. Within the metaverse environment, users are provided with the necessary tools required for the creation and release of digital assets using what is also known as the metaverse Digital Asset System. Smart contracts, which pose a major theme in blockchain, can be utilized within the metaverse in order to enable users to easily, safely, and legally transfer digital assets. The decentralized nature of blockchain aligns well with the metaverse, enabling the creation and operation of a virtual economy. Especially with the use of various kinds of utility tokens and NFTs (non-fungible tokens). With the use of NFTs, a user's digital assets can be shielded from copying and hacking. However, in order to achieve successful integration of blockchain in the metaverse, the issue of double spending remains an open challenge. The metaverse originated as a medium for the co-existence of a virtual and physical world.

Therefore, one challenge emerging is the ability to trade and invest irreplaceable tokens for real/physical money. Advantages to utilizing the metaverse include the following:

- Investing in financial products and services now has a lower barrier to entry.
- Assisting individuals in monetizing their work and experiences (such as gaming) in order to compensate for income losses due to inflation and the pandemic.
- Reducing costs and increasing transaction efficiency by eliminating middlemen in procedures such as money transfers.
- Creating interest from a diverse range of demographic groups outside of the traditional financial sector and presenting novel concepts and opportunities.
- Managing community-involved and connected projects.

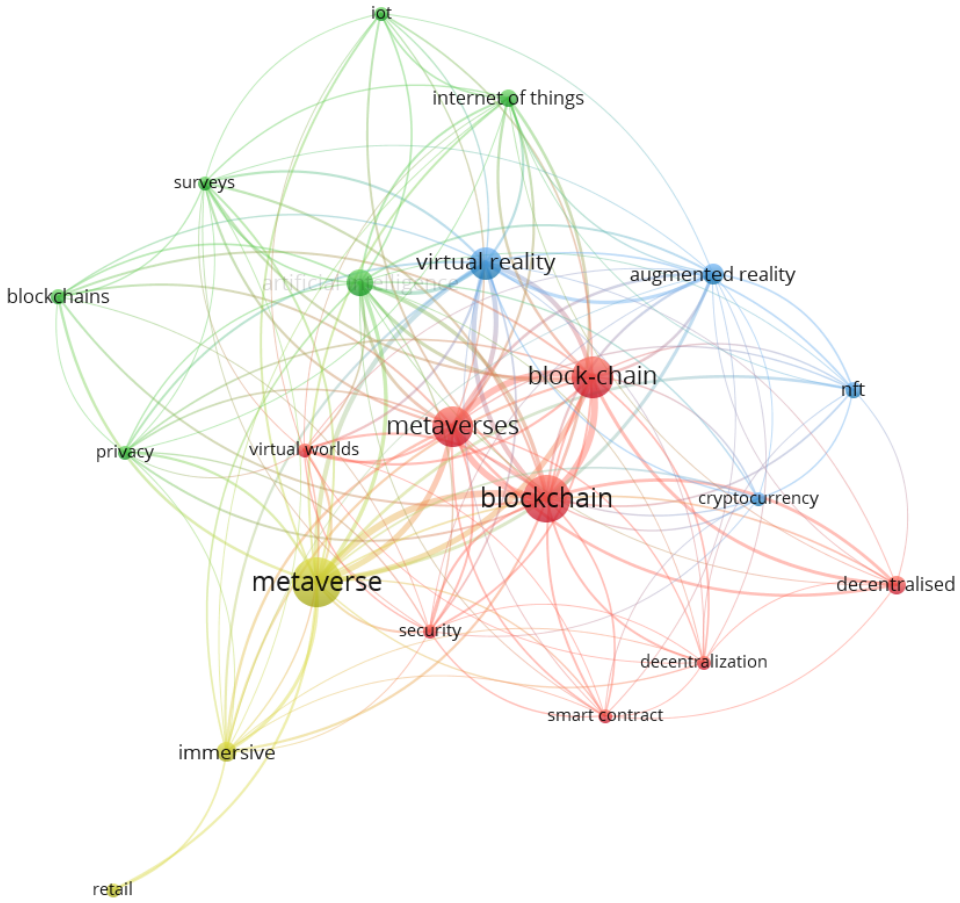

Figure 13. Keyword network for "blockchain" and "metaverse."

In the research work of Yang et al., published in 2021 [58], the authors have performed a comprehensive literature review on the integration of blockchain technology in the upcoming metaverse. Furthermore, a plethora of applications are provisioned in order to setup an economic ecosystem within the metaverse, such as applications for office work, social networking applications, non-fungible token (NFT) marketplaces, etc. Another aspect that must be further elaborated in the near future is the development of suitable security and privacy frameworks in the metaverse, which could minimize users' privacy violations, identity theft, and/or any other kind of fraudulent activity. Furthermore, another requirement for future development is the design and development of metaverse-oriented cryptography mechanisms for privacy preservation.

5.1. Technical Framework for the Blockchain in Metaverse

In the following paragraphs, the most recent and pertinent blockchain-based methods are investigated, along with their suitability for integration into the metaverse. The methods

are examined from a technical point of view, covering cornerstone aspects including, among others: (i) data storage, (ii) collection, (iii) interoperability, (iv) sharing, and (v) privacy protection framework. Following the presentation and discussion of the above-mentioned methods, the authors also propose a conceptual framework, which is illustrated in Figure 14.

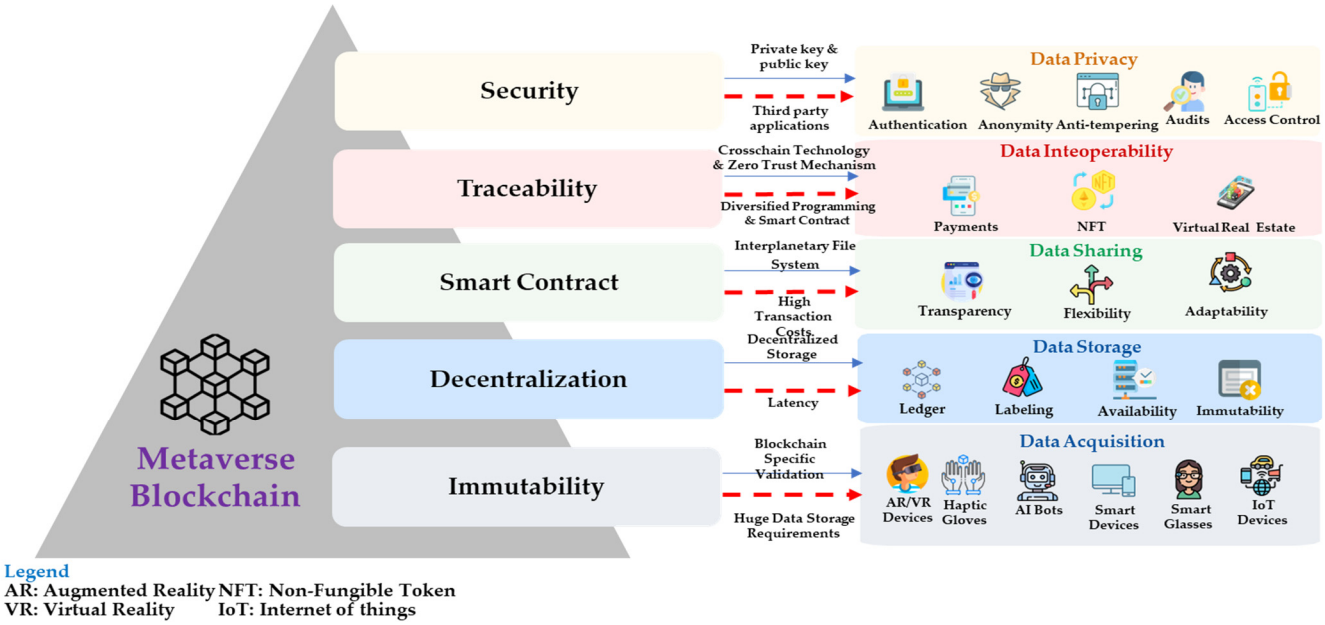

Figure 14. Blockchain for technical aspects in metaverse.

5.1.1. Data Acquisition

Data acquisition is a significant process in the ecosystem of the metaverse. Whenever a user makes financial transactions, it is inevitable that sensitive user information, such as bank and credit card information, will be shared. Beyond the financial aspect, the users also share other types of sensitive information, which are prerequisites for the creation of their digital avatars, namely biometric data and hand gestures [60]. Furthermore, data acquisition contributes towards the training of AI and ML algorithms that can facilitate a variety of applications, such as the creation of digital products, the implementation of automated recommendation systems, the support of decision-making, and metaverse marketing [61]. As a result, enormous sets of heterogeneous data will be produced in the metaverse [62]. One of the tools used in the metaverse for data collection will be web forms filled out by the users. Bots will obtain users' social security numbers and other necessary authentication information, including personal information [63]. Additionally, a high-definition camera will gather data regarding the physical characteristics of the metaverse users. Finally, the utilization of XR devices will be advantageous to the users in regards to the exploration of the metaverse. The utilization of such devices will also be expanded for compiling data regarding user behavior [64].

Challenges of Data Acquisition in the Metaverse

The metaverse will produce vast amounts of unstructured, real-time data through decentralized applications. Acquiring the vast amounts of data being generated poses a difficult challenge. Building metaverse applications such as recommender systems will make data assurance or integrity crucial [65]. The quality of the data may also be impacted by the acquisition of duplicate and inaccurate data [66].

Blockchain Contribution

The adoption of blockchain technology will make it simpler for applications such as social networking to acquire real data in the metaverse. The distributed ledger of the

metaverse will make it possible to trace data in the metaverse and validate transaction records. Data acquisition is therefore resistant to attacks because the majority of nodes in the ledger must consent before any changes to the data in the metaverse can be made [67]. All gathered data in the metaverse are validated using a blockchain-specific process that is driven by consensus mechanisms [68]. The probability of producing a duplicate block is almost zero, ensuring that there will be no duplication during the data acquisition process. The data obtained through blockchain-enabled acquisition systems in the metaverse will be accurate because every block in the blockchain has been authorized [69,70].

Challenge/Limitation

Blockchain transactions may take much longer to complete (e.g., a few days). Consequently, the network has a limited number of users, and transaction fees are higher than usual [71]. The necessity of copying the data collected in a blockchain along the chain raises the need for storage. Storage space requirements increase as data collection increases [72].

5.1.2. Data Storage

In a fully implemented metaverse, enormous amounts of data will be produced, placing a significant burden on the real world's capacity to process that information. Thus, data storage will be a significant challenge [64].

Challenges of Data Storage in the Metaverse

In the metaverse, a digital reality coexists with the real world. The metaverse will produce a vast amount of data as more people enter the virtual worlds, and as a result, huge amounts of data files will be produced. As soon as the metaverse is fully operational, the ability of the physical world to store data will be stretched to the breaking point. Therefore, deploying metaverse applications such as gaming, entertainment, real estate, healthcare, etc. will present a significant challenge in terms of data storage [70]. The provision of biometric data, vocal inflections, and vital signs that depend on sensitive data by the metaverse is put at risk by the high likelihood of data loss [73] and corruption in centralized applications [74].

Blockchain Contribution

A new block is created for every metaverse transaction [75]. As a result, data are stored throughout the chain as a copy of the original blocks, increasing data reliability and transparency in the metaverse [76]. When blockchain technology is used, many blocks will contribute to data distribution, increasing the amount of data that are available for use in metaverse applications such as vital monitoring and life support alerts. Data scientists in the metaverse can collaborate and work on data cleansing thanks to the decentralized nature of blockchain technology, which drastically reduces the time and costs involved in labeling data and getting datasets ready for analytics.

Challenge/Limitation

Data in the metaverse will be more able to withstand copying and tampering with the help of a consensus-based distributed ledger [77]. However, since any new data must be mirrored eight times throughout the entire chain, more study is needed to address the latency issue.

5.1.3. Data Sharing

Data exchange in the metaverse will be advantageous to all parties, including scientists and the public [78]. The metaverse of AR/VR and IoT devices will collect data that will be used to build personalized systems that respond to users' behavior. Businesses will be able to conduct data analytics through the metaverse by sharing information across applications. Shared data will be used to build products in the metaverse, evaluate advertising, personalize content, and establish content strategies [74].

Challenges of Data Sharing in the Metaverse

Due to high data mutability in the conventional sharing environment, there is also high latency and reduced data availability. In contrast to immutable data, scaling mutable data is difficult [79]. Numerous applications in the metaverse, including those in healthcare, traffic optimization, media, and entertainment, will produce vast amounts of data and operate mostly in real-time. When the demand for real-time data rises in a conventional data-sharing environment, data flexibility becomes a significant issue.

Blockchain Contribution

Blockchain technology can increase the transparency and accuracy of transactions in the metaverse for applications such as education and cryptocurrency exchange [80]. Furthermore, the data owner will also have total control over the data. Distributed ledger technology can also be useful for data audits. Blockchain consequently saves time and money by reducing the need for data validation [74]. Additionally, flexible data sharing will be enhanced by smart contracts. Typically, they are used to automate the execution of an agreement so that all parties can be sure of the result right away. Smart contracts can be programmed in a variety of ways thanks to blockchain technology [81].

Challenge/Limitation

The number of blocks has to grow along with the number of users in the metaverse, requiring the use of enormous computing resources [77]. As a result, users will pay a higher transaction cost for the verification of shared transactions. This problem needs to be solved by next-generation blockchains so that data can be shared effectively in the metaverse.

5.1.4. Data Interoperability

The main force behind the metaverse will be interoperability. The metaverse will enable communication and information exchange between a wide range of applications, including those in finance and healthcare. An identity standard is used to issue the user a special set of credentials that can be used in any virtual world [74].

Challenges of Data Interoperability in Metaverse

To participate in various realms, people must set up their accounts, avatars, hardware, and payment infrastructure. There are limited options for a user to move their digital assets, such as NFT and avatars, to another digital environment [70]. The interconnection between the virtual worlds will determine the possibility of using an application there. Applications in the digital world should be able to freely exchange information with one another, regardless of their location or the technology being used. The ability to manage the interactions between virtual worlds in an appropriate manner, which is a serious limitation of the conventional approach, is necessary for metaverse interoperability [82].

Blockchain Contribution

Cross-blockchain technology will make it possible for virtual worlds to communicate, minimizing the need for intermediaries in the metaverse [83].

Challenge/Limitation

The existence of numerous public blockchains in various virtual worlds that do not share a common language poses the biggest obstacle to cross-blockchain-enabled metaverse interoperability. It will be challenging to adapt because different platforms will offer varying degrees of smart contract capabilities. Furthermore, these virtual worlds use a wide range of transaction architectures and consensus mechanisms, which limits interoperability [84].

5.1.5. Data Privacy Preservation

Considering that Web 2.0 follows a centralized architecture, it becomes apparent that data privacy is becoming a concern. However, with the emergence of Web 3.0, the metaverse

will also become a reality, which can be briefly realized as the co-existence of the physical world and its digital twin, which will expand the scope and complexity of the Internet. In the literature, the challenge of how Web 2.0 will affect the defense of personal rights has not been addressed yet. The above-mentioned challenge is also pertinent to the upcoming Web 3.0. By extension, the issue of data privacy will become a first-priority challenge.

Privacy Preservation in the Metaverse and the Corresponding Challenges

Personally identifiable information (PII) is a source of concern for protecting the privacy of personal data. The initial stages of the metaverse ecosystem, where attackers can deceive users and steal sensitive data, will be challenging to adapt to. Another concern regarding the metaverse will be the simultaneous management and validation of large volumes of data [85].

Blockchain Contribution

Third-party intermediaries are prohibited in the blockchain-enabled metaverse from misusing or obtaining data from other parties. Consequently, with the integration of blockchain technology in the metaverse, users will gain full control over the access rights to their sensitive and personal data, thus controlling whenever and how their data are accessed by third parties [86].

Challenge/Limitation

Similar to the existing challenges of blockchain applications, within the metaverse environment, human error plays a key role since the security of the blockchain can be jeopardized. A common example might be the misplacement of a private key, which would put at great risk the users' data privacy in the metaverse. Since third-party applications frequently employ insufficient security measures, which compromise personal data, attackers can easily target them in the metaverse [19]. Thus, there is still fertile ground for further research into discovering new ways for integrating blockchain technology in the metaverse, targeting the protection and preservation of user data privacy.

5.2. Blockchain Case Studies in Metaverse

As the number of metaverse platforms grows, so does the number of blockchain case studies in metaverse that can be found in the literature. In terms of gaming, Illuvium, which will be released in beta in 2022, is another fantasy role-playing game with a graphically rich and immersive experience built on the Ethereum blockchain [87]. More specifically, a summary of typical blockchain use cases in the metaverse can be found in Table 3.

Table 3. Typical Blockchain use cases in Metaverse.

Case Study	Advantage	Ref.
Data Sharing	Verify the data review procedure.	[88]
	A flexible privacy protection system.	[89]
Data Storage	High-efficiency access to data.	[90]
	Identify and fix the storage capacity issue with the blockchain.	[91]
Virtual Economy Ecosystem	Support anonymous payment.	[92]
	Assume machine-to-machine (M2M) and Internet of Things (IoT) payments.	[93]
	Encourage a transparent environment for system participation.	[94]

5.3. Regulatory Challenges Protecting Human Rights in Metaverse

Three regulatory issues in the metaverse era stand out among others [95]:

(1) Privacy regulations;
(2) Copyright laws and regulations;
(3) Mechanisms to enforce regulatory regimes.

Regarding privacy, it is crucial to remember that public blockchains are truly public, meaning that everyone can see all transaction histories. While transactions can be made anonymous (using cryptographic hashes), assets, tokens, and electronic addresses of the wallets can still be seen. Anytime a specific address is intentionally, unintentionally, or in some other way connected to a specific person, the entire history of prior transactions can be made public. Therefore, it is impossible to guarantee the privacy of current or previous transactions. Despite this, transparency continues to be a valuable asset in the metaverse because it fosters greater trust among all actors, and there should be a good trade-off with privacy.

Next, Web 3.0 promises to support the creator economy by securing fair use of assets in terms of copyright. However, a rather unexpected NFT-related development has reopened the discussion on content rights in the metaverse. Notably, blockchains were viewed as the best way to prove the provenance of digital assets, allowing creators to track the use and sale of their creative works using specific addresses and cryptographic signatures. Anyone who has created cryptographic signatures, however, is aware that altering even a single bit in a large file will completely alter the hash. Therefore, a famous NFT would technically have a completely different asset as a result of an invisible pixel change. Thus, decisions about originality return to subjective interpretation, which is something we had hoped blockchains would help us avoid.

The enforceability of regulatory frameworks is another open question. Regulation violations in the Web 2.0 era were easily addressed: the regulator would issue a notice against the violating party, such as a specific company. However, since the metaverse is powered by a blockchain, which is a distributed computing infrastructure that is owned by millions of people, there is no such company in the Web 3.0 era.

As it regards the ethical challenges of the human-centric metaverse, an open question is, "What ethical standards and limitations will govern this new cyber-physical metaverse, where identity will be a fluid concept and regulatory oversight will be weak?"

What are the standards of conduct that society will accept in order to navigate and feel secure while interacting online? The "internet of senses" and haptic feedback will further enhance experiences. It has to be stressed that immersion will be much stronger in the metaverse than it is on the current internet. As such, the possibility of acquiring multiple identities in the metaverse poses fertile ground for new kinds of conflicts of which we are not yet aware. Thus, a solution should be to establish an international committee for such legal issues, similar to the newly established Coordinating Committee for the Governance of Artificial Intelligence (CCGAI) [96].

5.4. Comparison of Current Paper Versus the State of Knowledge

The contribution of this paper is highlighted in Table 4. Following the literature survey presented in the previous sections, only a few publications investigate the use of blockchain for applications in the metaverse. Thus, the impact of blockchain on enabling technologies is presented in our study, along with a variety of metaverse applications in which the integration of blockchain technology would improve their effectiveness. Furthermore, the contribution of this paper extends to the historical evolution of blockchain (timeline) as well as the integration of blockchain in the era of Society 5.0.

Table 4. Comparison of the contribution of this paper with the pertinent literature.

Topic	Current Paper	[97]	[98]	[58]	[76]	[99]	[100]
Blockchain Impact for Metaverse Enablers	X						
Technical Perspective of Metaverse	X		X	X	X		
Blockchain as an Enabling Technology for Metaverse	X	X	X	X	X	X	X
Applications of Blockchain	X	X	X	X	X		
Timeline of Blockchain Evolution	X						
Technical Perspective of Adoptable Blockchain Methods			X	X	X		
Blockchain for Society 5.0	X						

6. Concluding Remarks and Outlook

In the context of this research work, a literature review has been presented regarding blockchain integration starting from Industry 4.0 up to Society 5.0 and predictions regarding the metaverse. More specifically, the center of attention is the integration of cryptocurrency technologies in the fields of academia, societal aspects, industry, etc. Although so far there have been identified four blockchain eras, with one more upcoming in the near future, it has become apparent that blockchain technology is not yet fully developed, and there are several key issues requiring further elaboration. An important topic that must be covered in greater depth is the investigation of permissioned versus permissionless blockchains. As it has become apparent from the available literature, permissionless blockchain has not yet reached a satisfactory level of maturity in comparison with permissioned blockchain, which is a result of the different challenges for each of the types discussed above. Since 2019, permissionless blockchains have become widely accepted by society since individual users can use cryptocurrency in order to pay for goods and services.

Inarguably, the current global environmental and societal instability has led the United Nations (UN) to create a more sustainable and environmentally friendly future for the next generations. Consequently, a set of seventeen developmental goals have been discussed and published under the convention known as Sustainable Development Goals (SDG). Alternatively, as it has been indicated within the manuscript, blockchain should be further elaborated in order to become both more sustainable and environmentally friendly. However, the global community has offered an alternative point of view, which indicates that blockchain could be used in accordance with the SDGs for the benefit of the global community. The technological advancements presented in the previous paragraphs can facilitate global authorities by offering a framework for decentralized and global coordination and collective decision-making. Essentially, the need for such a decentralized and globalized governance model emerges. Therefore, goals have to be agreed upon for ensuring effective execution, which in this case are the SDGs. These goals must be followed by the objectives and measures associated with them. To achieve the above-mentioned goals, ownership, transparency, and accountability are required. To ensure that the objectives are satisfied, the development of an execution process is necessary. Therefore, without appropriate governance, execution cannot be guaranteed. On the contrary, with the implementation of poor governance strategies, the key concepts of blockchain platforms, i.e., democracy, decentralization, and transparency, are compromised.

Therefore, future research as a result of the presented literature review will be focused on the design and development of smaller, decentralized networks for key societal aspects. The aim will be the creation of a "blockchain of blockchains," which will facilitate unifying the information exchange between smaller networks and improving the decentralization of authority in an attempt to further minimize cybersecurity issues in conjunction with the implementation of state-of-the-art cryptographic algorithms.

Author Contributions: Conceptualization, D.M. and J.A.; investigation, J.A. and N.P.; resources, N.P.; writing—review and editing, J.A.; supervision, D.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Nomenclature

AI	Artificial Intelligence
AR	Augmented Reality
DApps	Digital Applications
DLT	Digital Ledger Technology
DOS	Denial Of Service
DPoS	Delegated Proof of Stake
HCI	Human-Computer Interaction
HEI	Higher Education
IoT	Internet of things
NFT	Non-Fungible Token
NSA	National Security Agency
PII	Personally Identifiable Information
PoA	Proof of Activity
PoA	Proof of Authority
PoB	Proof of Burn
PoC	Proof of Capability
PoET	Proof of Elapsed Time
PoH	Proof of History
PoI	Proof of Importance
PoS	Proof of Stake
PoSpace	Proof of Space
PoW	Proof of Work
RSA	Rivest Shamir Adleman
SDG	Sustainable Development Goals
SGX	Software Guard Extensions
SHA	Secure Hash Algorithm
VR	Virtual Reality

References

1. Politou, E.; Casino, F.; Alepis, E.; Patsakis, C. Blockchain mutability: Challenges and proposed solutions. *IEEE Trans. Emerg. Top. Comput.* **2019**, *9*, 1972–1986. [CrossRef]
2. Helliar, V.C.; Crawford, L.; Rocca, L.; Teodori, C.; Veneziani, M. Permissionless and permissioned blockchain diffusion. *Int. J. Inf. Manag.* **2020**, *54*, 102136. [CrossRef]
3. Peng, L.; Feng, W.; Yan, Z.; Li, Y.; Zhou, X.; Shimizu, S. Privacy preservation in permissionless blockchain: A survey. *Digit. Commun. Netw.* **2021**, *7*, 295–307. [CrossRef]
4. Akram, S.V.; Malik, P.K.; Singh, R.; Anita, G.; Tanwar, S. Adoption of blockchain technology in various realms: Opportunities and challenges. *Secur. Priv.* **2020**, *3*, 109. [CrossRef]
5. Bao, Q.; Li, B.; Hu, T.; Sun, X. A survey of blockchain consensus safety and security: State-of-the-art, challenges, and future work. *J. Syst. Softw.* **2023**, *196*, 111555. [CrossRef]
6. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, 21260.
7. Xu, M.; Chen, X.; Kou, G. A systematic review of blockchain. *Financ. Innov.* **2019**, *5*, 27. [CrossRef]
8. Badruddoja, S.; Dantu, R.; He, Y.; Upadhayay, K.; Thompson, M. Making smart contracts smarter. In Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, 3–6 May 2021; pp. 1–3. [CrossRef]
9. Saini, K.; Roy, A.; Chelliah, P.R.; Patel, T. Blockchain 2.O: A smart contract. In Proceedings of the International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 1–3 December 2021; pp. 524–528. [CrossRef]
10. Ethereum Official Website. Available online: https://ethereum.org/en/ (accessed on 20 November 2022).
11. Khandelwal, P.; Johari, R.; Gaur, V.; Vashisth, D. BlockChain technology based smart contract agreement on REMIX IDE. In Proceedings of the 8th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 26–27 August 2021; pp. 938–942. [CrossRef]
12. Raphael, J.; Steele, A. The Impact of Blockchain Technology on Audit 2020. Available online: https://www2.deloitte.com/us/en/pages/audit/articles/impact-of-blockchain-in-accounting.html (accessed on 18 November 2022).
13. Consensus Mechanisms in Blockchain: A Beginner's Guide. Crypto.com. Available online: https://crypto.com/university/consensus-mechanisms-in-blockchain (accessed on 20 November 2022).
14. Hafid, A.; Hafid, A.S.; Samih, M. Scaling Blockchains: A Comprehensive Survey. *IEEE Access* **2020**, *8*, 125244–125262. [CrossRef]

15. Zhang, P.; Zhou, M.; Zhen, J.; Zhang, J. Enhancing scalability of trusted blockchains through optimal sharding. In Proceedings of the 2021 IEEE International Conference on Smart Data Services (SMDS), Chicago, IL, USA, 5–10 September 2021; pp. 226–233. [CrossRef]
16. He, J.; Wang, G.; Zhang, G.; Zhang, J. Consensus mechanism design based on structured directed acyclic graphs. *Blockchain Res. Appl.* **2021**, *2*, 100011. [CrossRef]
17. Zhang, Q.; Jiang, X.; Zheng, Y. Blockchain adoption and gray markets in a global supply chain. *Omega* **2023**, *115*, 102785. [CrossRef]
18. Mourtzis, D. *Design and Operation of Production Networks for Mass Personalization in the Era of Cloud Technology*; Elsevier: Amsterdam, The Netherlands, 2022; pp. 1–393. [CrossRef]
19. Hassan, M.U.; Rehmani, M.H.; Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Gener. Comput. Syst.* **2019**, *97*, 512–529. [CrossRef]
20. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
21. Malik, S.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. TrustChain: Trust management in blockchain and IoT supported supply chains. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 184–193. [CrossRef]
22. Rahman, M.S.; Chamikara, M.; Khalil, I.; Bouras, A. Blockchain-of-blockchains: An interoperable blockchain platform for ensuring IoT data integrity in smart city. *J. Ind. Inf. Integr.* **2022**, *30*, 100408. [CrossRef]
23. Asaithambi, S.; Ravi, L.; Kotb, H.; Milyani, A.H.; Azhari, A.A.; Nallusamy, S.; Varadarajan, V.; Vairavasundaram, S. An Energy-Efficient and Blockchain-Integrated Software Defined Network for the Industrial Internet of Things. *Sensors* **2022**, *22*, 7917. [CrossRef]
24. Hinsdale, J. *Cryptocurrency's Dirty Secret: Energy Consumption*; State of the Planet; Columbia Climate School: New York, NY, USA, 2022.
25. Saingre, D.; Ledoux, T.; Menaud, J.M. Measuring performances and footprint of blockchains with BCTMark: A case study on Ethereum smart contracts energy consumption. *Clust. Comput.* **2022**, *25*, 2819–2837. [CrossRef]
26. Is This the End of Crypto? *The Economist.* Available online: https://www.economist.com/leaders/2022/11/17/is-this-the-end-of-crypto (accessed on 15 November 2022).
27. Start Your Crypto Journey with a Reliable Partner. Available online: https://relictum.pro/ (accessed on 15 November 2022).
28. Shen, P.; Li, S.; Huang, M.; Gao, H.; Li, L.; Li, J.; Lei, H. A survey on safety regulation technology of blockchain application and blockchain ecology. In Proceedings of the 2022 IEEE International Conference on Blockchain (Blockchain), Virtual Conference, 2–5 May 2022; pp. 494–499. [CrossRef]
29. Haber, S.; Stornetta, W.S. How to timestamp a digital document. *J. Cryptogr.* **1991**, *3*, 99–111. [CrossRef]
30. Cheng, Y.; Shaoqin, H. Research on blockchain technology in cryptographic exploration. In Proceedings of the 2020 International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE), Bangkok, Thailand, 30 October–1 November 2020; pp. 120–123. [CrossRef]
31. Touloupou, M.; Christodoulou, K.; Inglezakis, A.; Iosif, E.; Themistocleous, M. Towards a framework for understanding the performance of blockchains. In Proceedings of the 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 27–30 September 2021; pp. 47–48. [CrossRef]
32. Li, Z.; Tian, Z.; Wang, L.; Zhong, Y.R. Chapter 12—Blockchain-enabled product lifecycle management. In *Design and Operation of Production Networks for Mass Personalization in the Era of Cloud Technology*; Mourtzis, D., Ed.; Elsevier: Amsterdam, The Netherlands, 2022; pp. 349–379. [CrossRef]
33. Chen, G.; Xu, B.; Lu, M.; Chen, N.S. Exploring blockchain technology and its potential applications for education. *Smart Learn. Environ.* **2018**, *5*, 1. [CrossRef]
34. Hasankhani, A.; Hakimi, S.M.; Miadreza, S.; Asadolahi, H. Blockchain technology in the future smart grids: A comprehensive review and frameworks. *Int. J. Electr. Power Energy Syst.* **2021**, *129*, 106811. [CrossRef]
35. Krishna, B.; Rajkumar, P.; Velde, V. Integration of blockchain technology for security and privacy in internet of things. *Mater. Today Proc.* **2021**, 196–209. [CrossRef]
36. Majeed, U.; Khan, L.U.; Yaqoob, I.; Kazmi, S.M.A.; Salah, K.; Hong, C.S. Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. *J. Netw. Comput. Appl.* **2021**, *181*, 103007. [CrossRef]
37. Sanka, A.I.; Irfan, M.; Huang, I.; Cheung, R.C.C. A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Comput. Commun.* **2021**, *169*, 179–201. [CrossRef]
38. Aldowah, H.; Al-Samarraie, H.; Wan Mohamad, F. Educational data mining and learning analytics for 21st century higher education: A review and synthesis. *Telemat. Inform.* **2019**, *37*, 13–49. [CrossRef]
39. Chapman, D.; Samira, L. Degrees of integrity. The threat of corruption in higher education. *Stud. High. Educ.* **2016**, *41*, 247–268. [CrossRef]
40. Yakovenko, I.; Kulumbetova, L.; Subbotina, I.; Zhanibekova, G.; Bizhanova, K. The Blockchain technology as a catalyst for digital transformation of education. *Int. J. Mech. Eng. Technol. (IJMET)* **2019**, *10*, 886–897.
41. Zou, Y.; Meng, T.; Zhang, P.; Zhang, W.; Li, H. Focus on blockchain: A comprehensive survey on academic and application. *IEEE Access* **2020**, *8*, 187182–187201. [CrossRef]

42. 4 Ways Blockchain Will Transform Higher Education, Gartner. Available online: https://www.gartner.com/smarterwithgartner/4-ways-blockchain-will-transform-higher-education (accessed on 25 November 2022).
43. Ziyi Li, Z.; Joseph, L.K.; Yu, J.; Gasevic, D. Blockchain-based solutions for education credentialing system: Comparison and implications for future development. In Proceedings of the 2022 IEEE International Conference on Blockchain (Blockchain), Virtual Conference, 2–5 May 2022; pp. 79–86. [CrossRef]
44. Zhang, L.; Ma, Z.; Ji, X.; Wang, C. Blockchain: Application in the system of teaching informatization management of higher education. In Proceedings of the 2020 3rd International Conference on Smart BlockChain (SmartBlock), Zhengzhou, China, 23–25 October 2020; pp. 185–190. [CrossRef]
45. Mourtzis, D.; Angelopoulos, J.; Panopoulos, N. Blockchain in engineering education: The teaching factory paradigm. In Proceedings of the Conference on Learning Factories (CLF), Graz, Austria, 1–2 July 2021. [CrossRef]
46. Mourtzis, D. Simulation in the design and operation of manufacturing systems: State of the art and new trends. *Int. J. Prod. Res.* **2020**, *58*, 1927–1949. [CrossRef]
47. Sasikumar, A.; Subramaniyaswamy, V.; Ketan, K.; Indragandhi, V.; Logesh, R.; Ganeshsree, S.; Ajith, A. Blockchain-based trust mechanism for digital twin empowered Industrial Internet of Things. *Future Gener. Comput. Syst.* **2023**, *141*, 16–27. [CrossRef]
48. Singh, S.K.; Yang, L.T.; Park, J.H. FusionFedBlock: Fusion of blockchain and federated learning to preserve privacy in industry 5.0. *Inf. Fusion* **2023**, *90*, 233–240. [CrossRef]
49. Ivanov, D.; Dolgui, A. OR-methods for coping with the ripple effect in supply chains during COVID-19 pandemic: Managerial insights and research implications. *Int. J. Prod. Econ.* **2021**, *232*, 107921. [CrossRef]
50. Dolgui, A.; Ivanov, D. Ripple effect and supply chain disruption management: New trends and research directions. *Int. J. Prod. Res.* **2021**, *59*, 102–109. [CrossRef]
51. Hader, M.; Tchoffa, D.; Mhamedi, A.; Ghodous, P.; Dolgui, A.; Abouabdellah, A. Applying integrated Blockchain and Big Data technologies to improve supply chain traceability and information sharing in the textile sector. *J. Ind. Inf. Integr.* **2022**, *28*, 100345. [CrossRef]
52. Klöckner, M.; Schmidt, C.G.; Wagner, S.M. Building resilient post-pandemic supply chains through digital transformation. In *Supply Chain Resilience*; Springer Series in Supply Chain Management; Khan, O., Huth, M., Zsidisin, G.A., Henke, M., Eds.; Springer: Cham, Switzerland, 2023; Volume 21. [CrossRef]
53. Huang, S.; Wang, G.; Yan, Y.; Fang, X. Blockchain-based data management for digital twin of product. *J. Manuf. Syst.* **2020**, *54*, 361–371. [CrossRef]
54. Chen, Y.; Chen, H.; Zhang, Y.; Han, M.; Siddula, M.; Cai, Z. A survey on blockchain systems: Attacks, defenses, and privacy preservation. *High-Confid. Comput.* **2022**, *2*, 100048. [CrossRef]
55. Christen, P.; Schnell, R.; Ranbaduge, T.; Vidanage, A. A critique and attack on blockchain-based privacy-preserving record linkage. *Inf. Syst.* **2021**, *108*, 101930. [CrossRef]
56. Homoliak, I.; Venugopalan, S.; Reijsbergen, D.; Hum, Q.; Schumi, R.; Szalachowski, P. The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 341–390. [CrossRef]
57. Nair, M.M.; Tyagi, A.K.; Sreenath, N. The future with industry 4.0 at the core of society 5.0: Open issues, future opportunities and challenges. In Proceedings of the 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 27–29 January 2021; pp. 1–7. [CrossRef]
58. Yang, Y.; Zhao, Y.; Huang, H.; Xiong, Z.; Kang, Z.; Zheng, Z. Fusing Blockchain and AI With Metaverse: A Survey. *IEEE Open J. Comput. Soc.* **2022**, *3*, 122–136. [CrossRef]
59. Cacciagrano, D.; Corradini, F.; Mostarda, L. Blockchain and IoT integration for society 5.0. In *Society 5.0*; Communications in Computer and Information, Science; Gerber, A., Hinkelmann, K., Eds.; Springer: Cham, Switzerland, 2021; Volume 1477. [CrossRef]
60. Cha, H.-S.; Im, C.-H. Performance enhancement of facial electromyogram-based facial-expression recognition for social virtual reality applications using linear discriminant analysis adaptation. *Virtual Real.* **2022**, *26*, 385–398. [CrossRef]
61. Wang, F.-Y.; Qin, R.; Wang, X.; Hu, B. Metasocieties in metaverse: Metaeconomics and metamanagement for metaenterprises and metacities. *IEEE Trans. Comput. Soc. Syst.* **2022**, *9*, 2–7. [CrossRef]
62. Xi, N.; Chen, J.; Gama, F.; Riar, M.; Hamari, J. The challenges of entering the metaverse: An experiment on the effect of extended reality on workload. *Inf. Syst. Front.* **2022**, 1–22. [CrossRef]
63. Jovanovic, A.; Milosavljevic, A. Vortex metaverse platform for gamified collaborative learning. *Electronics* **2022**, *11*, 317. [CrossRef]
64. Duan, H.; Li, J.; Fan, S.; Lin, Z.; Wu, X.; Cai, W. Metaverse for social good: A university campus prototype. In Proceedings of the 29th ACM International Conference on Multimedia, Virtual Conference, 20–24 October 2021; pp. 153–161.
65. Tao, H.; Bhuiyan, M.Z.A.; Abdalla, A.N.; Hassan, M.M.; Zain, J.M.; Hayajneh, T. Secured data collection with hardware-based ciphers for IoT-based healthcare. *IEEE Internet Things J.* **2018**, *6*, 410–420. [CrossRef]
66. Shiau, W.-L.; Huang, L.-C. Scale development for analyzing the fit of real and virtual world integration: An example of pokemon go. *Inf. Technol. People* **2022**. [CrossRef]
67. Xu, C.; Qu, Y.; Luan, T.H.; Eklund, P.W.; Xiang, Y.; Gao, L. A lightweight and attack-proof bidirectional blockchain paradigm for internet of things. *IEEE Internet Things J.* **2022**, *9*, 4371–4384. [CrossRef]

68. Bouraga, S. A taxonomy of blockchain consensus protocols: A survey and classification framework. *Expert Syst. Appl.* **2021**, *168*, 114384. [CrossRef]
69. Guo, J.; Ding, X.; Wu, W. Reliable traffic monitoring mechanisms based on blockchain in vehicular networks. *IEEE Trans. Reliab.* **2021**, *71*, 1219–1229. [CrossRef]
70. Bian, Y.; Leng, J.; Zhao, J.L. Demystifying metaverse as a new paradigm of enterprise digitization. *Int. Conf. Big Data* **2021**, *12988*, 109–119. [CrossRef]
71. Alrubei, S.M.; Ball, E.A.; Rigelsford, J.M.; Willis, C.A. Latency and performance analyses of real-world wireless IoT-blockchain application. *IEEE Sens. J.* **2020**, *20*, 7372–7383. [CrossRef]
72. Chen, L.; Fu, Q.; Mu, Y.; Zeng, L.; Rezaeibagha, F.; Hwang, M.-S. Blockchain-based random auditor committee for integrity verification. *Future Gener. Comput. Syst.* **2022**, *131*, 183–193. [CrossRef]
73. Wang, X.; Liu, X.; Cheng, C.-T.; Deng, L.; Chen, X.; Xiao, F. A joint user scheduling and trajectory planning data collection strategy for the UAV-assisted WSN. *IEEE Commun. Lett.* **2021**, *25*, 2333–2337. [CrossRef]
74. Kiong, L.V. *Metaverse Made Easy: A Beginner's Guide to the Metaverse: Everything you Need to Know About Metaverse, NFT and GameFi*; Independently Published: Chicago, IL, USA, 2022.
75. Liang, W.; Fan, Y.; Li, K.-C.; Zhang, D.; Gaudiot, J.-L. Secure data storage and recovery in industrial blockchain network environments. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6543–6552. [CrossRef]
76. Jeon, H.-j.; Youn, H.-c.; Ko, S.-m.; Kim, T.-h. Blockchain and AI meet in the metaverse. *Adv. Converg. Blockchain Artif. Intell.* **2022**, *73*, 1–94. [CrossRef]
77. Xie, J.; Yu, F.R.; Huang, T.; Xie, R.; Liu, J.; Liu, Y. A survey on the scalability of blockchain systems. *IEEE Netw.* **2019**, *33*, 166–173. [CrossRef]
78. Kraus, S.; Kanbach, D.K.; Krysta, P.M.; Steinhoff, M.M.; Tomini, N. Facebook and the creation of the metaverse: Radical business model innovation or incremental transformation? *Int. J. Entrep. Behav. Res.* **2022**, *28*, 52–57. [CrossRef]
79. Yu, K.; Tan, L.; Aloqaily, M.; Yang, H.; Jararweh, Y. Blockchain enhanced data sharing with traceable and direct revocation in IIoT. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7669–7678. [CrossRef]
80. Egliston, B.; Carter, M. Critical questions for facebook's virtual reality: Data, power and the metaverse. *Internet Policy Rev.* **2021**, *10*, 1–23. [CrossRef]
81. Ali, O.; Jaradat, A.; Kulakli, A.; Abuhalimeh, A. A comparative study: Blockchain technology utilization benefits, challenges and functionalities. *IEEE Access* **2021**, *9*, 12730–12749. [CrossRef]
82. Mourtzis, D.; Panopoulos, N.; Angelopoulos, J.; Wang, B.; Wang, L. Human centric platforms for personalized value creation in metaverse. *J. Manuf. Syst.* **2022**, *65*, 653–659. [CrossRef]
83. Jabbar, R.; Fetais, N.; Krichen, M.; Barkaoui, K. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In Proceedings of the IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2–5 February 2020; pp. 310–317. [CrossRef]
84. Wibowo, S.; Sandikapura, T. Improving data security, interoperability, and veracity using blockchain for one data governance, case study of local tax big data. *Int. Conf. ICT Smart Soc. (ICISS)* **2019**, *7*, 1–6. [CrossRef]
85. Hughes, I. The metaverse: Is it the future? *ITNOW* **2022**, *64*, 22–23. [CrossRef]
86. Kumar, P.; Kumar, R.; Srivastava, G.; Gupta, G.P.; Tripathi, R.; Gadekallu, T.R.; Xiong, N.N. PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2326–2341. [CrossRef]
87. Bushnell, M. Global Capital Markets and Cryptocurrency: Exploring the International Political Economy of Blockchain Ecosystems and Metaverse Development. Cryptopedia Staff., 2022, Illuvium (ILV): A Decentralized Ethereum RPG. 2022. Available online: https://www.gemini.com/cryptopedia/illuvium-crypto-rpg-blockchain-game-ilv-token (accessed on 26 December 2022).
88. Doku, R.; Rawat, D.B.; Liu, C. On the Blockchain-Based Decentralized Data Sharing for Event Based Encryption to Combat Adversarial Attacks. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 1033–1043. [CrossRef]
89. Liu, L.; Feng, J.; Pei, Q.; Chen, C.; Ming, Y.; Shang, B.; Dong, M. Blockchain-enabled Secure Data Sharing Scheme in Mobile-edge Computing: An Asynchronous Advantage Actor-critic Learning Approach. *IEEE Internet Things J.* **2020**, *8*, 2342–2353. [CrossRef]
90. Chen, X.; Zhang, K.; Liang, X.; Qiu, W.; Zhang, Z.; Tu, D. Hyperbsa: A High-performance Consortium Blockchain Storage Architecture for Massive Data. *IEEE Access* **2020**, *8*, 178402–178413. [CrossRef]
91. Dwivedi, S.K.; Amin, R.; Vollala, S. Blockchain-based Secured Ipfsenable Event Storage Technique with Authentication Protocol in VANET. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 1913–1922. [CrossRef]
92. Ben Sasson, E.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M. Zerocash: Decentralized anonymous payments from bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Washington, DC, USA, 18–21 May 2014; pp. 459–474. [CrossRef]
93. Miehle, D.; Meyer, M.M.; Luckow, A.; Bruegge, B.; Essig, M. Toward a decentralized marketplace for self-maintaining machines. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Seoul, Korea, 14–17 May 2019; pp. 431–438. [CrossRef]
94. Seitz, A.; Henze, D.; Miehle, D.; Bruegge, B.; Nickles, J.; Sauer, M. Fog computing as enabler for blockchain-based IIOT app marketplaces—A case study. In Proceedings of the 2018 5th International Conference on Internet of Things: Systems, Management and Security, Valencia, Spain, 15–18 October 2018; pp. 182–188. [CrossRef]

95. Dohler, M.; Franzese, G. Top Four Blockchain and Metaverse Challenges and Opportunities for Telco, 2022, Ericsson Blog. Available online: https://www.ericsson.com/en/blog/2022/10/metaverse-challenges-and-opportunities (accessed on 27 December 2022).
96. Jelinek, T.; Wallach, W.; Kerimi, D. *Coordinating Committee for The Governance of Artificial Intelligence*; G20 Insights; Global Solutions Initiative Foundation: Berlin, Germany, 2020.
97. Ning, H.; Wang, H.; Lin, Y.; Wang, W.; Dhelim, S.; Farha, F.; Ding, J.; Daneshmand, M. A survey on metaverse: The state-of-the-art, technologies, applications, and challenges. *arXiv* **2021**, arXiv:2111.09673.
98. Lee, L.H.; Braud, T.; Zhou, P.; Wang, L.; Xu, D.; Lin, Z.; Kumar, A.; Bermejo, C.; Hui, P. All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *arXiv* **2021**, arXiv:2110.05352.
99. Mystakidis, S. Metaverse. *Encyclopedia* **2022**, *2*, 486–497. [CrossRef]
100. Park, S.-M.; Kim, Y.-G. A metaverse: Taxonomy, components, applications, and open challenges. *IEEE Access* **2022**, *10*, 4209–4251. [CrossRef]