Blockchain-Based DLTs for Metaverse Applications Security

Manuscript received May 11, 2023; revised June 22, 2023

Danial Jamil*
Information Technology Dept.
Ghazi University
Dera Ghazi Khan, Pakistan
2022gu1473@student.gudgk.edu.pk

Muhammad Jamil
Information Technology Dept.
Ghazi University
Dera Ghazi Khan, Pakistan
2022gu1469@student.gudgk.edu.pk

Muhammad Hassam
Information Technology Dept.
Ghazi University
Dera Ghazi Khan, Pakistan
meetings@gudgk.edu.pk

***Abstract*— Distributed Ledger Technologies (DLTs) and blockchain systems are used in various higher-level departments, government sectors and commercial industries. This article reviews how DLTs and blockchain systems work with IOT devices and how it provides security and scalability. The metaverse sets a new standard for social media sites and 3D virtual spaces. Moreover, the key aim of the virtual world is to safeguard the metadata of IOT customers. Additionally, crypto is an effective solution due to its openness, data integrity, and accountability characteristics. So, we review the two new burning technologies of crypto and the virtual world from a methodological perspective, i.e. data collection, saving data, allocation, integration, and data confidentiality are all aspects of data management. By each strategy, in this article, we discuss the methodological techniques of the meta chain and then investigate the potential benefits of blockchain technology. Further, we analyze how blockchain will influence other critical enabling technologies in the metaverse's service world, such as the IOT.**

Keywords—Block Chain, DLT, IoT, Metaverse, Multi-DLT Applications

I. INTRODUCTION

Over the last few years, blockchain is going the most famous system and distributed ledger technologies (DLTs) from academia, the government, and business. This article examines how DLTs are incorporated into the Internet of Things, another game-changing technology (IoT) [1]. Smart housing, intelligent transportation, Logistics, Media, and Smart Health benefits are just a few of the IoT-based applications that have the probability of revolutionizing our way of life and increasing the effectiveness of current infrastructures. This article will point out areas for future research, such as multi-DLT applications, [2] DLT security and adaptability, and Distributed ledger technology in quantum-resistant cryptography. Metaverse refers to IoT, Blockchain, AI, and other IT industries, including medicine. Metaverse uses the most IoT policies in their simulated workspace, making them digital twins. The blockchain-based metaverse tracks this data with a unique label. Artificial intelligence uses such Metaverse data. Metaverse utilizes AI and blockchain algorithms to create a digital cloud service in which users can interact in socioeconomic development in addition to the actual world securely and comfortably. These latest technologies will be used faster.

II. RESULTS AND DISCUSSION

A. Distributed Ledger Technology

With the advent of computers, old records used to keep track of money and property were replaced by digital documents composed of digitally stamped digital data. Today, a nexus of cryptologic conundrums, motivating structures, and privacy measures, which appear to have had no priority in the early history of people, enables the cooperative building of digitally distributed ledgers. It increases openness and confidence and allows cutting-edge applications that don't rely on centralized architecture to flourish. A rudimentary review of distributed ledger technology (DLT) is provided in this section, setting the stage for further in-depth explorations of the technology's possibilities in IOT contexts. Many layers are working in DLTs which are shown in Fig. 1.

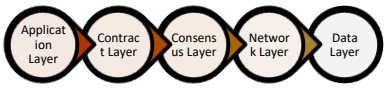

Fig. 1. Layer Diagram

The main aim is to scrutinize prospective DLT applications for IoT in addition to research on how various Distributed Ledger Technologies (DLTs) that have recently emerged have been used to address IoT concerns [3-4]. A distributed ledger can exist throughout that linked computer system where data is sent directly between nodes without going through a primary server, and a single unit does not keep it. Every network user can use the ledger to save records, share transactions, and synchronize transactions. Schemes that operate in a reorganized ledger are transparent, distributed, and safe. Such documents are often shared publicly in an open manner among users, who have the authority to confirm and approve or reject system activity, which leads to transparency (called transactions) [5-6]. Immutability is an essential feature of decentralized ledger technology. When one transaction is acknowledged and added to the record by many clients, it's hard to restore its last state in this property. It is completed through different combinations of crypto techniques like cryptographical mysteries and proprieties that preserve our transactions/records safe. This issue discussed the working of DLT with metaverse application used in IOT and discussion of several problems and the solution. For example, IoT platforms assemble user information like position and other records. A distributed protected platform understood by a DLT provides security, privacy and a trusted IOT world. There are

 EISSN: 2961-872X ● PISSN: 2961-8924 ● DOI: 10.56741/esl.v2i02.351

many security problems with IoT. Identity operations and tracking user information are the most challenging problems. Due to resource limitations and the enormous scale of the IoT bias, solutions to these problems, To overcome these issues, and new methods and equipment must be developed that follow IoT disciplines. The following essential parts of distributed checks are practical tools for the IoT's incoming era. Some of them are

B. *Block Chain*

Conversely, in 2008, the digital currency Bitcoin was created. [1], One of the most emerging technologies, blockchain has become a focus of attention for various scholars and experts. Blockchain is a digital record that captures all activities that have taken place on a community link in a way that is convenient, independent, and clear. The key benefit of Blockchain technology over other techniques is that it lets different persons do safe transactions without a service provider getting in their way. Cutting out the foreign power can reduce computation costs while confidentiality and reliability of the funds' transfer are gained. See Fig. 2 for the blockchain process.

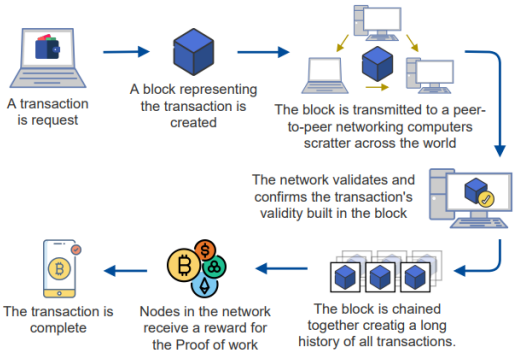

Fig. 2. Blockchain Process

C. *Metaverse*

What do we mean by metaverse? Prefix "meta," which means "more comprehensive" or "transforming," comes from the Greek language. "Verse" is a short form for "multiverse," representing a space/time spectrum. The concept of "Metaverse" refers to a unique digital living space where conventional social systems are converted or created after combining these words. New approaches are deployed to generate the new virtual world metaverse, representing everything in our life or world in a parallel universe. [15] These technologies include artificial environment, Virtual Reality VR, digital twin, cryptographic techniques, etc.

Metaverse applications are mentioned in the following given Fig. 3.

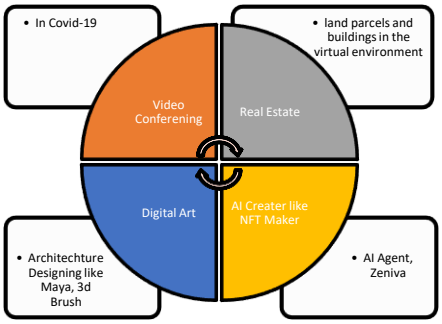

Fig. 3. Metaverse Applications

D. *Metachain*

A summary of the Meta Chain is given in Fig. 4. Using this schema, and the MSP is a support company providing the MUs with its software and services, such as virtual reality games, meetings, and live shows. Each MU has a scheme account and associated assets, such as coupons, cash, and objects. The MUs can use the service by paying the MSP and sending E-Wallets to other Metaverse users. The metaverse clients can also benefit individuals by incorporating processing capacity into the blockchain. The Metaverse service provider-managed blockchain works as a program to control all communications between the MSP and the MUs. These communications are captured in the blockchain as operations, along with the resources of the MUs.

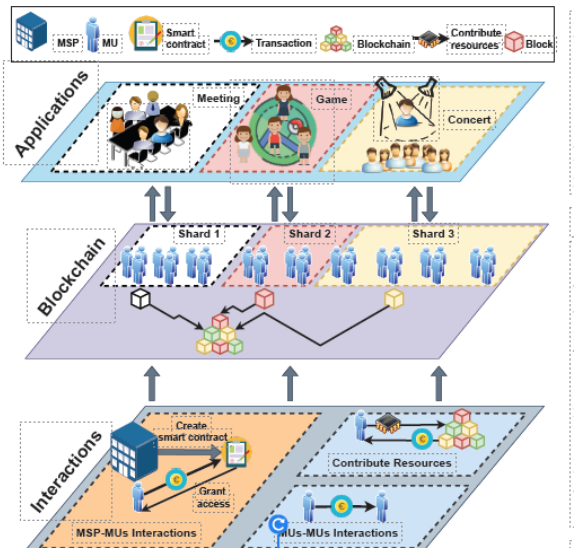

Fig. 4. Metachain Methodologies

There are four main components of the metaverse (Table I). Similar to a global plot inside a simulated environment, a supervisor's projection of augmented reality (AR) technology, or an element or client lifelog within a mirror or digital reality, their techniques overlap dramatically.

TABLE I. RELATED TECHNOLOGY

No	Technology	Examples
1	Communication Computing Infrastructure	
	• Network and Communication	IoT, 5G, 6G
	• Nano Perception	Nano Perception, Quantum Perception
2	Fundamental Technology	
	• Artificial Network Intelligence	Machine Learning ML, Deep Learning DL, Natural Learning Processing NLP
	• Security and Privacy	
3	Virtual Reality Object Connection	
	• Identity Modeling	Identity Authentication
	• Decentralized Technology	Blockchain
	• Social Computing	Social Network, Swarm Intelligence
4	Virtual Reality Space Convergence	
	• Extended Reality	VR/AR/MR
	• Brain-Computer Interface	
	• Video Game	Game Engine

IoT technology, including metaverse foundational stream's roles, is as an IoT device. Our data shows that virtual reality (VR) will become commonplace in 43 per cent of

manufacturing companies within the next few years, with augmented reality (AR) focusing more on engineering applications than user software packages. Most businesses are already implementing 5G and 6G technology as they prepare for the arrival of the virtual world, the new generation of the Internet.

E. Fundamental Technology

Virtualization technology is an upcoming new technology in which people can intermingle with visual three-dimensional objects and graphical virtual interfaces of one another in a way that replicates the actual universe differently. It was made using strategies from ai technology. Fig. 5 shows the five stages of AI in the metaverse.



Fig. 5. Five Stages of AI in the Metaverse

III. Related Works and Contribution

The distributed ledger has been the focus of many researchers and developers in the past few ages. At a similar period, various review articles have been issued examining the underlying issues of blockchain and DLT. Explain how the Bitcoin protocol can be used for purposes other than virtual currency, and cite reference [8] as an example. Both [9] and [10] examine Bitcoin and related systems from the view of safety and secrecy concerns. The fundamental weaknesses of conventional centralized exchanges are addressed by blockchain technology. Some cutting-edge study is currently conducted in DLT-based IoT integration [12-19, 96]. There are presently 18 several platforms of blockchain technology that are discussed in reference [12]. There are just four use cases that were built with IoT in consideration. The author's sketch Some Cutting-Edge Blockchain Solutions to Meet Your IoT Security Requirements - Review may be read at [13]. The project's primary goal is to discover and categorize security problems in light of the IoT's management structure.

According to many academic articles that have made a connection between the Internet of Things and DLT. They pay little attention to other crucial aspects of the Internet of Things in favour of safety and confidentiality concerns. Dealing with identities and automated exchanges between machines resolves this void. The use cases for the (IoT) that he develops with distributed ledger technologies (DLTs), such as logistic networks and digital shipping, are examples. Table II provides a side-by-side comparison of the various aspects that were (and were not) discussed in previous research and the multiple aspects that readers will find in this article. A highlight of one such comparison is provided. We will use this as the post list in our following list.

- This article offers a more comprehensive explanation of how DLT can assist with specific IoT needs than previous research publications.
- Everything is from the "smart" house to "smart" mobility to "smart" treatment to "smart" resources.
- Demonstrate and discuss a wide range of the currently available DLT-based solutions for IoT, including their benefits and drawbacks. We also look at the following alternatives to expand on the standard blockchain ledger. B. A directed acyclic graph structure as opposed to the traditional blockchain.
- Present some current DLT systems that may help with data security and tracking in IoT applications; these platforms' merits and drawbacks are analyzed and contrasted.
- Conclude by pointing out several research gaps for further study in developing DLT and IoT integration.

TABLE II. DLT BENEFITS IOT, AND IN IOT PANELS

How DLT benefit IoT				DLTs in IOT Panels			
Consistency and confidentiality	Uniqueness	Machine Transaction	Source	Smart Home	IOV	Supply chain	Smart Healthcare
✓	×	×	×	×	×	×	×
✓	✓	×	×	×	×	×	×
×	×	×	×	×	×	×	×
✓	×	✓	×	✓	✓	✓	✓
✓	×	✓	×	✓	×	×	×
✓	×	×	×	×	×	×	×
✓	×	×	×	×	×	×	×

Without a chance of doubt, [1] IoT platforms are quietly transforming all elements of our familiar atmosphere. Intelligent, networked home appliances that can be controlled and monitored from afar guarantee peace of mind for their owners. The Internet of Things (IoT) and blockchains can have impressive effects [2]. Blockchains allow us to create distributed, trustworthy, and auditable ledgers of transactions between peers. Many community applications that work together to address issues in a decentralized manner have emerged on the Internet in recent years, as pointed out in [3]. Several non-profit, community-based systems have achieved notoriety; [4] Bitcoin offers a workable platform to the Byzantine Generals issue thanks to its proof-of-work based agreement technique and safe timestamping facility. However, Bitcoin leaves itself defenceless to an extensive range of risks because of its distributed consensus architecture.[5] They examine the concepts of privacy and secrecy and the research conducted to propose ways to enhance them. The first group comprises information disclosure via blockchain, network analysis, and deanonymization methods.[6] Data integrity ensures that information during storage or transmission has not been modified. Conventionally, this is achieved using cryptographic signatures in conjunction with verification procedures. [7] Decentralized and Computational data analysis apps that can scale to billions of policies while protecting user privacy may find a valuable tool in the blockchain and other Peer-to-Peer techniques. According to Ref. [8], IoT gadgets lack security and cannot defend themselves. IoT devices have limited resources, there need to be established standards, and there needs to be secure hardware or software out there. Diverse IoT resources work against efforts to provide a global strategy for safeguarding the many layers that make up the network. The IoT prioritizes edge-centric computing to provide better connectivity, lower latency, and higher bandwidth [9]. However, the bandwidth and connection of older cloud-centric platforms have deteriorated, negatively impacting service quality. [10] The Internet of Things automatically processes and transfers vast amounts of data, some containing sensitive information that must be protected. As a result, they pique the interest of those who would seek to harm them. [11] The metaverse platform collects and processes data from numerous IoT devices to guarantee its smooth operation in several metaverse applications, including medicine, education, and smart cities. One famous problem with systems that are controlled

 EISSN: 2961-872X ● PISSN: 2961-8924 ● DOI: 10.56741/esl.v2i02.351

remotely and switch platforms is the absence of an immersive experience. Mainly when operating SCADA or PLC-based virtual robotic systems [4], observing marketable ownable property or planning, comprehending visual representation in health, commerce or online education, remote monitoring of unmanned aerial, nautical, or ground containers, and engaging in online media that exceeds multiple components.

A. *Blockchain Methods in Different Terminologies*

Intelligent devices like IOT within the metaverse can interconnect data via cross-chain platforms that eventually establish records of linked activities in virtual worlds as represented by blockchain. See Table III for the metaverse technical views. Due to cryptography, servers and clients can transmit and connect directly to intelligent device data without central control or monitoring [38]. IoT-enabled blockchain in the metaverse makes storing knowledge in real-time possible. Because blockchain transactions are immutable, all investors can trust the info and act rapidly and successfully [39]. It will assist in resolving difficulties in the metaverse. Blockchain technology enables investors to track their IoT databases in shared blockchain records.

TABLE III. METAVERSE TECHNICAL VIEWS

Metverse Technical View							
Blockchain as facilitating skill for the metaverse							
Blockchain components							
Conceptual Considerations for implementing blockchain-based Methods							
Effect of blockchain helpers							

Remark: Red: Technical Analysis; *Yellow: High Level; Green: Introducing*

Blockchain technology allows social networking platforms to collect accurate data from the virtual world known as the metaverse. Digital Records or digital ledger, also known as Distributed led by blockchain, can track user information in the metaverse and authenticate business accounts [40, 41]. The mainstream of ledger nodes must approve before any variations of the metaverse's data can be finished; data gathering is consequently immune to assaults [42]. Every information obtained in the virtual world is verified using a blockchain-specific procedure driven by consensus methodology [43], [44]. Data, a timestamp, and a cryptographic code of the prior transaction are all recorded alongside each operation in a blockchain. [45]. Hence, modifying a statement within a block also affects the other blocks. Every block's data is invulnerable to altering [46]. The prospect of manufacturing an identical block is virtually nil, assuring that there will be no repetition during information collection. All blocks are permitted on the blockchain; the information gathered via blockchain-enabled achievement processes in the metaverse will be trustworthy [47].

B. *Blockchain for Metaverse Digital Twins*

Due to the blockchain's encoding competencies and historical statistics accessibility, digital twins are attack-resistant and may safely communicate data [33] across several simulated worlds. With a brainy or smart distributed ledger, data is often common between digital twins in digital platforms. A smart distributed ledger will sync real-world items with their metaverse counterparts on the blockchain. Using digital twins on crypto technology will also assist in resolving confidentiality and data safety issues [34]. Combining cryptography and AI technology will make it feasible to collect device data and construct superior digital twins in the metaverse. The blockchain, which is unchangeable and needs an agreement to alter, will include a transaction for digital representation activity in the metaverse [35].

C. *Blockchain as a Big Data Multiverse*

By collecting figures from dependable databases, blockchain technology will help reduce the quantity of inaccurate data received, the data possessors will control their statistics, and third parties won't be able to manipulate the data in any way. It guarantees that the worth of the data flows inside the multiverse is admirable [41]. Because blockchain technology is decentralized, data researchers in the metaverse can interact and team up on information cleansing. Data categorization, the generation of statistics for dashboards and reports, and the risk of data pollution may all be significantly decreased. Data availability for stakeholders of the metaverse may be improved by the immutability of the blockchain, which makes it intolerable to modify the data because it will be repeated throughout the network.

D. *Blockchain for the Metaverse*

IoT devices may securely store and transport physical data between virtual contexts using blockchain. Blockchain systems require plenty of computation. Blockchains are susceptible if a few miners dominate the network's hash rate. Private IoT data can only be confirmed once published on the Metaverse blockchain due to governance issues. Blockchain networks may breach the legislation on metaverse DTLs. Blockchain security makes tracking metaverse IoT transactions involving fraudulent services complex. The blockchain's independence has numerous advantages, but it's hard to identify who's responsible for specific actions [89]. Expanding the metaverse requires blockchain governance.

The metaverse makes it hard to verify data. Blockchain is often delayed despite its ability to sidestep these constraints [48]. Blockchain transactions take longer. The process takes days. Transaction fees are more significant, reducing network usage [49]. Data copied along a blockchain requires storage. Data requires additional storage [50]. The metaverse needs a more robust blockchain to report data-collecting issues.

Blockchain makes big data analytics promising. Metaverse users will have complete financial and personal control. The blockchain will eliminate third-party data collection and labelling. Consensus models, mining block value, and transaction verification remain concerns. [41]. Blockchain provides answers that necessitate new challenges to ongoing systems or replacements. By getting the outcome, fixing the entire system will be difficult and time-wasting.

TABLE IV. IMPACT OF BLOCKCHAIN IN TECHNICAL PERSPECTIVE

Technical Perspective	Data Acquisition Capacity	Data Storage	Data Sharing	Data Interoperability	Data Privacy Preservation
IoT	H	L	H	L	H
Digital Twins	H	L	H	M	H
XR Applications	H	M	H	L	H
AI	L	M	L	L	H
Big Data	H	H	L	L	H

L Low Impact M Medium Impact H High Impact

IV. CONCLUSION

In the future, big data stats will have efficient blockchain or cryptographic technology programs. The newly made virtual world handlers will have control of their personal information and financial activities. Cryptography eliminates the need for a third party to achieve trustable information. Several difficulties, including consensus models, the cost of mining blocks, and financial activities, authentication, still need to be solved. Crypto offers different techniques that need significant modifications to current systems or their entire replacement. So, altering technology as a whole will be difficult and time-wasting. Although the implementation of blockchain technology with the metaverse is still in its beginning, mentioned problems will be handled in the upcoming era, opening the way to a vast array of new and stirring prospects.

This paper profoundly explores and discusses the parts and consequences of cryptography techniques, problems and security for developing and expanding apps and services in the metaverse. The main thoughts of blockchain and the metaverse, as well as blockchain's role in the establishment and growth of the metaverse, were introduced at the commencement of this work. Some key technical challenges and scenarios of cryptography in the virtual world were also thoroughly investigated; furthermore, the technical problems analysis and application discussion provided in this paper also identify prospective future research avenues.

Blockchain has provided the considerable ability to change the interactive number of apps and facilities developed within the simulated environment, according to an exhaustive investigation of blockchain for the metaverse, from both research methods and different situations from different points of view. Consensus algorithms, network monitoring, and blockchain integration are a few of the technical and practical aspects of all current blockchain implementations that have attracted much more academic interest. As a result, connecting the current system and the new platform is required to facilitate the advancement of developing technologies in the metaverse. Consensus methods ensure that authorized connections in a distributed system are approved on the state of specific statistics. Cross-chain is the optimal method for achieving interoperability across several chains, allowing users to properly conduct dealing (with value and information) over different cryptographic networks. Farmworkers can transfer information from one chain to another, such as Ethereum data to the Polygon blockchain, or simultaneously. This interoperability technique also encourages the expansion of the construction of entirely decentralized systems with cross-chain bridges. There are many benefits to using blockchain-based applications and services (such as financial services, crypto algorithms, concurrency control, and shared data ledger) is a blockchain service platform that can socialize with a broad range of professional environments.

REFERENCES

[1] D.L.Xu, W.He, and S. Li. 2014. Internet of things in industries: A survey. IEEE Trans. Industr. Inf. 10, 4 (2014), 2233–2243.

[2] K. Christidis and M. Devetsikiotis. 2016. Blockchains and smart contracts for the Internet of Things. IEEE Access 4 (2016), 2292–2303.

[3] F. Tschorsch and B. Scheuermann. 2016. Bitcoin and Beyond: A technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutor. 18, 3 (2016), 2084–2123.

[4] M. Conti, S. Kumar, C. Lal, et al. 2018. A survey on security and privacy issues of Bitcoin. IEEE Commun. Surv. Tutor. 20, 4 (2018), 3416–3452.

[5] M. C. K. Khalilov and A. Levi. 2018. A survey on anonymity and privacy in Bitcoin-like digital cash systems. IEEE Commun. Surv. Tutor. 20, 3 (2018), 2543–2585.

[6] T. Salman, M. Zolanvari, A. Erbad, et al. 2018. Security services using blockchains: A state of the art survey. IEEE Commun. Surv. Tutor. 21, 1 (2018), 858–880.

[7] M. Conoscenti, A. Vetro, and J. C. De Martin. 2016. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA'16). IEEE, 1–6.

[8] M. A. Khan and K. Salah. 2018. IoT security: Review, blockchain solutions, and open challenges. Fut. Gener. Comput.Syst. 82 (2018), 395–411.

[9] K. Yeow, A. Gani, R. W. Ahmad, et al. 2018. Decentralized consensus for edge-centric Internet of Things: A review, taxonomy, and research issues. IEEE Access 6 (2018), 1513–1524.

[10] E. F. Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, et al. 2018. A survey of how to use blockchain to secure the Internet of Things and the stalker attack. Security and Communication Networks Article 9675050 (2018), 27 pages.

[11] T. M. Fernández-Caramés and P. Fraga-Lamas. 2018. A review on the use of blockchain for the Internet of Things. IEEE Access 6 (2018), 32979–33001.

[12] A. Reyna, C. Martín, J. Chen, et al. 2018. On blockchain and its integration with IoT. Challenges and opportunities. Fut. Gener. Comput. Syst. 88 (2018), 173–190.

[13] T. M. Fernández-Caramés and P. Fraga-Lamas. 2019. A review of the application of blockchain to the next generation of cybersecurity industry 4.0 smart factories. IEEE Access 7 (2019), 45201–45218.

[14] Thippa Reddy Gadekallu, Blockchain for the Metaverse: A Review

[15] P. Kumar, R. Kumar, G. Srivastava, G. P. Gupta, R. Tripathi, T. R. Gadekallu, and N. N. Xiong, "PPSF: a privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities," IEEE Transactions on Network Science and Engineering, vol. 8, no. 3, pp. 2326–2341, 2021.

[16] J. Sedlmeir, F. V¨olter, and J. Str¨uker, "The next stage of green electricity labelling: using zero-knowledge proofs for blockchain-based certificates of origin and use," ACM SIGENERGY Energy Informatics Review, vol. 1, no. 1, pp. 20–31, 2021.

[17] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain-based IoT systems: Integration issues, prospects, challenges, and future research directions," Future Generation Computer Systems, vol. 97, pp. 512–529, 2019.

[18] T. G. Kanter, "The metaverse and extended reality with distributed IoT," IEEE Internet of Things Magazine (IoT), 2021.

[19] L. Zhang, F. Li, P. Wang, R. Su, and Z. Chi, "A blockchain-assisted massive IoT data collection intelligent framework," IEEE Internet of Things Journal, 2021.

[20] F. Rollo, B. Sudharsan, L. Po, and J. G. Breslin, "Air quality sensor network data acquisition, cleaning, visualization, and analytics: a real-world IoT use case," in Adjunct Proceedings of the 2021 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2021 ACM International Symposium on Wearable Computers, 2021, pp. 67–68.

[21] Y. Hajjaji, W. Boulila, I. R. Farah, I. Romdhani, and A. Hussain, "Big data and IoT-based applications in smart environments: A systematic review," Computer Science Review, vol. 39, p. 100318, 2021.

[22] U. Majeed, L. U. Khan, I. Yaqoob, S. A. Kazmi, K. Salah, and C. S. Hong, "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," Journal of Network and Computer

[23] A. Dorri, F. Luo, S. Karumba, S. Kanhere, R. Jurdak, and Z. Y. Dong, "Temporary immutability: A removable blockchain solution for prosumer-side energy trading," Journal of Network and Computer Applications, vol. 180, p. 103018, 2021.

[24] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: Challenges and solutions," Blockchain: Research and Applications, vol. 2, no. 2, p. 100006, 2021.

[25] Q. Chen and S.-J. Lee, "Research status and trend of digital twin: Visual knowledge mapping analysis," International Journal of advanced smart convergence, vol. 10, no. 4, pp. 84–97, 2021.

[26] K. Yoon, S.-K. Kim, S. P. Jeong, and J.-H. Choi, "Interfacing cyber and physical worlds: Introduction to IEEE 2888 standards," in IEEE International Conference on Intelligent Reality (ICIR), 2021, pp. 49–50.

 EISSN: 2961-872X ● PISSN: 2961-8924 ● DOI: 10.56741/esl.v2i02.351

[27] C. Zhuang, J. Gong, and J. Liu, “Digital twin-based assembly data management and process traceability for complex products,” Journal of manufacturing systems, vol. 58, pp. 118–131, 2021.

[28] L. U. Khan, W. Saad, D. Niyato, Z. Han, and C. S. Hong, “Digital-twin-enabled 6G: Vision, architectural trends, and future directions,” IEEE Communications Magazine, vol. 60, no. 1, pp. 74–80, 2022.

[29] D. Lee, S. H. Lee, N. Masoud, M. Krishnan, and V. C. Li, "Integrated digital twin and blockchain framework to support accountable information sharing in construction projects," Automation in construction, vol. 127, p. 103688, 2021.

[30] W. Shen, T. Hu, C. Zhang, and S. Ma, “Secure sharing of big digital twin data for smart manufacturing based on blockchain,” Journal of Manufacturing Systems, vol. 61, pp. 338–350, 2021.

[31] B. K. Wiederhold, “Ready (or not) player one: Initial musings on the metaverse,” pp. 1–2, 2022.

[32] A. A. Hussain and F. Al-Turjman, “Artificial intelligence and blockchain: A review,” Transactions on Emerging Telecommunications Technologies, vol. 32, no. 9, p. e4268, 2021.

[33] S. Han and T. Kim, "News big data analysis of 'metaverse using topic modelling analysis," The Journal of Digital Contents Society, vol. 22, no. 7, pp. 1091–1099, 2021.

[34] D. M. Gligor, K. G. Pillai, and I. Golgeci, “Theorizing the dark side of business-to-business relationships in the era of AI, big data, and blockchain,” Journal of Business Research, vol. 133, pp. 79–88, 2021.

[35] J. O. Yang and J. S. Lee, “Utilization exercise rehabilitation using metaverse (vr· ar· mr· xr),” Korean Journal of Sport Biomechanics, vol. 31, no. 4, pp. 249–258, 2021.

[36] P. Bhattacharya, D. Saraswat, A. Dave, M. Acharya, S. Tanwar, G. Sharma, and I. E. Davidson, “Coalition of 6G and blockchain in AR/VR space: Challenges and future directions,” IEEE Access, vol. 9, pp. 168 455–168 484, 2021.

[37] S. Kumar, A. K. Bharti, and R. Amin, “Decentralized secure storage of medical records using blockchain and IPFS: A comparative analysis with future directions,” Security and Privacy, vol. 4, no. 5, p. e162, 2021.

[38] D. G. Johnson and N. Diakopoulos, “What to do about deepfakes,” Communications of the ACM, vol. 64, no. 3, pp. 33–35, 2021.

[39] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, "A survey on blockchain technology: Evolution, architecture and security," IEEE Access, vol. 9, pp. 61 048–61 073, 2021. applications, vol. 181, p. 103007, 2021.

[40] S. Wang, M. A. Qureshi, L. Miralles-Pechua'an, T. Huynh-The, T. R. Gadekallu, and M. Liyanage, "Explainable AI for B5G/6G: Technical aspects, use cases, and research challenges," arXiv preprint arXiv:2112.04698, 2021.

[41] T. R. Gadekallu, Q.-V. Pham, D. C. Nguyen, P. K. R. Maddikunta, N. Deepa, B. Prabadevi, P. N. Pathirana, J. Zhao, and W.-J. Hwang, "Blockchain for edge of things: Applications, opportunities, and challenges," IEEE Internet of Things Journal, vol. 9, no. 2, pp. 964–988, 2022.

[42] Q. Ynag, Y. Zhao, H. Huang, and Z. Zheng, “Fusing blockchain and AI with metaverse: A survey,” arXiv preprint arXiv:2201.03201, 2022.

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

[44] H.-j. Jeon, H.-c. Youn, S.-m. Ko, and T.-h. Kim, “Blockchain and AI meet in the metaverse,” Advances in the Convergence of Blockchain and Artificial Intelligence, p. 73, 2022.

[45] S. Mystakidis, “Metaverse,” Encyclopedia, vol. 2, no. 1, pp. 486–497, 2022.

[46] F.-Y. Wang, R. Qin, X. Wang, and B. Hu, “Megasocieties in metaverse: Meta economics and meta management for meta enterprises and megacities,” IEEE Transactions on Computational Social Systems, vol. 9, no. 1, pp. 2–7, 2022.

[47] S.-M. Park and Y.-G. Kim, “A metaverse: taxonomy, components, applications, and open challenges,” IEEE Access, vol. 10, pp. 4209–4251, 2022.

[48] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Decentralized Business Review, p. 21260, 2008.

[49] Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., ... & Hui, P. (2021). All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. arXiv preprint arXiv:2110.05352.

[50] Ayiter, E. (2012, September). Further dimensions: Text, typography, and play in the metaverse. In 2012 International Conference on Cyberworlds (pp. 296-303). IEEE.

[51] [Internet]. Available: MetaVRse Engine - MetaVRse “A Guide to The Medical Metaverse”.

[52] Claudio, P., & Maddalena, P. (2014). Overview: Virtual reality in medicine. Journal of Virtual Worlds Research, 7(1).

[53] [Internet]. Available: www.healthmanagement.org, “Facebook’s Metaverse Could Revolutionize Healthcare”, 2021.

[54] Andrews, C., Southworth, M. K., Silva, J. N., & Silva, J. R. (2019). The extended reality in medical practice. Current treatment options in cardiovascular medicine, 21(4), 1-12.

[55] Dionisio, J. D. N., III, W. G. B., & Gilbert, R. (2013). 3D virtual worlds and the metaverse: Current status and future possibilities. ACM Computing Surveys (CSUR), 45(3), 1-38.

[56] Duan, H., Li, J., Fan, S., Lin, Z., Wu, X., & Cai, W. (2021, October). Metaverse for social good: A university campus prototype. In Proceedings of the 29th ACM International Conference on Multimedia (pp. 153-161).

[57] Falchuk, B., Loeb, S., & Neff, R. (2018). The Social Metaverse: Battle for Privacy. IEEE Technology and Society Magazine, 37(2), 52-61.

[58] Suzuki, S. N., Kanematsu, H., Barry, D. M., Ogawa, N., Yajima, K., Nakahira, K. T., ... & Yoshitake, M. (2020). Virtual Experiments in Metaverse and their Applications to Collaborative Projects: The Framework and its Significance. Procedia Computer Science, 176, 2125-2132.

[59] [Internet]. Available: www.sagentiainnovation.com What does the metaverse hold for healthcare | Sagentia Innovation.

[60] Han, Y., Niyato, D., Leung, C., Miao, C., & Kim, D. I. (2021). A Dynamic Resource Allocation Framework for Synchronizing Metaverse with IoT Service and Data. arXiv preprint arXiv:2111.00431.