

BlockVerse: A Decentralized Mobile App for Identity and Access Management in the Metaverse

Maryam Shaikh (Corresponding Author)

Lecturer, Department of Computer Science, IQRA University, Karachi, Pakistan.

maryam.shaikh@iqra.edu.pk

Muhammad Ahsan Hayat

Senior Lecturer, Department of Computer Science, IQRA University, Karachi, Pakistan.

muhammad.ahsan@iqra.edu.pk

<https://orcid.org/0009-0001-5063-7603>

Syed Rizwan

Senior Lecturer, Department of Computer Science, IQRA University, Karachi, Pakistan.

syed.rizwan@iqra.edu.pk

Faiza Irfan

Senior Lecturer, Department of Computer Science, IQRA University, Karachi,

Pakistan. faiza.irfan@iqra.edu.pk

Nazia Alfred Fernandes

Lecturer, Faculty of Health & Sciences, Iqra University North Campus, Karachi, Pakistan.

nazia.alfred@iqra.edu.pk

ABSTRACT

BlockVerse is a mobile first application designed to provide a single platform solution for secure identity and access management across Metaverse environments. By leveraging blockchain technology, it is built on a decentralized framework that enables users to manage digital identities while ensuring privacy and data integrity. Due to its user-friendly interface, BlockVerse allows users to seamlessly create and manage self-sovereign identities (SSI), thereby enabling secure interactions across multiple platforms. We have integrated wallet-based user authentication, user account registration and recovery, and access policy management to control personal data. BlockVerse adopts a hybrid model that includes both on-chain access control logic and off-chain

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

data storage for non-sensitive data. A prototype of this application has also been developed, implemented, and evaluated in a controlled test environment. The results indicate that BlockVerse can be a future solution for identity and access management in Metaverse environments.

Keywords: Web 3.0, DApp, Blockchain, Metaverse, Avatars, Identity and access management.

1. INTRODUCTION

The Internet has evolved significantly from its initial purpose of connecting people, and the concept of the Metaverse brings digital interaction closer to immersive, human centered connectivity. The Metaverse can be described as a virtual environment that extends the physical world, enabling users to interact through avatars for communication, collaboration, and engagement [1]. The term "Metaverse", derived from "Meta" meaning "Beyond" and "Verse" meaning "Universe", was first introduced in Neal Stephenson's 1992 novel Snow Crash [2]. In recent years, the Metaverse has influenced multiple domains, including education, healthcare, entertainment, and commerce [3]. This expansion is further supported by emerging technologies such as Digital Twins, which enable realistic simulations of physical objects and processes [4]. However, the increasing reliance on virtual identities also introduces significant identity and security challenges. Digital identities generate extensive data footprints, exposing users to threats such as identity theft, impersonation, unauthorized access, and misuse of personal information [5]. Ensuring secure authentication and access control is therefore essential for the safe adoption of Metaverse technologies.

Several critical questions arise in this context: Who owns user related data the user, the platform, or third parties? How should identity credentials be stored and managed in decentralized environments? Who is authorized to access this data, and how can accessibility be balanced with user privacy [6] Existing centralized identity management (IdM) frameworks struggle to address these concerns due to their reliance on trusted central authorities, which creates vulnerabilities such as single points of failure and limited user control.

To preserve user autonomy and trust, decentralization has been identified as a key requirement for the Metaverse [7]. Blockchain technology, with its inherent properties of transparency, immutability, and decentralization, provides a promising foundation for secure and privacy preserving identity management [8]. By leveraging blockchain, user centric identity systems can enhance data integrity while reducing dependence on centralized service providers.

Unlike many existing approaches we studied, BlockVerse emphasizes a DApp [Decentralized Application], as mobile usability was a recurring limitation in several existing systems. Integrated with Meta Mask Wallet, the application enables users to manage identities and perform transactions through a UI Built on React Native. By leveraging blockchain immutability [10], BlockVerse addresses challenges such as single point failure, limited user control, and data

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

breaches in Metaverse.

In this work, we focus on two main contributions based on the practical challenges we observed while designing a mobile first identity solution for Metaverse environments. First, it proposes a decentralized, blockchain enabled framework for secure identity and access management in Metaverse environments. Second, it introduces BlockVerse, a decentralized application that integrates user identity registration, revocation, access policy management, and basic analytics within a single platform. The remainder of this paper is organized as follows. Section II reviews related work, Section III describes the proposed framework and BlockVerse implementation, Section IV discusses scalability and integration considerations, and Section V concludes the paper.

2. LITERATURE REVIEW

Numerous studies have explored the role of blockchain in enhancing Metaverse functionality, particularly with respect to decentralization, security, and interoperability. Tan et al. [11] highlight blockchain's potential to decentralize the Metaverse ecosystem by enabling secure data storage and controlled information sharing. Griol et al. [12] emphasize the importance of transparency, authenticity, and efficiency in virtual environments, and call for dedicated system models and authentication mechanisms. Falchuk et al. [13] focus on blockchain enabled networking in social virtual worlds; however, aspects such as persistent data storage, identity governance, and integrated access control are not examined in detail. More recently, Yang et al. [26] identify core principles of Metaverse identity, namely Equivalence and Alignment and Fusion and Expansiveness, while highlighting challenges related to interoperability, privacy, and synthetic identities. Overall, these studies establish a conceptual foundation for blockchain based identity management in the Metaverse, but most remain at a high level architectural or theoretical stage. Several blockchain based systems have also been proposed to address practical identity management challenges. The uPort platform [14] supports Self-Sovereign Identity (SSI) on Ethereum through identity and messaging protocols. ShoCard [15] provides a permissioned blockchain solution for identity verification between users and enterprises. SCPKI [16] introduces a smart contract-based public key infrastructure to mitigate rogue certificate issues, although it offers limited support for fine grained access control. DNS-IdM [17] employs Ethereum and IPFS to enable distributed attribute management, while HealthID [18] applies a consortium blockchain model to healthcare identity management.

While these solutions address core aspects such as identity registration, authentication, and attribute handling, several gaps remain. In particular, existing systems provide limited support for identity revocation and identity related analytics, often lack a mobile app, and do not offer a unified interface for managing access policies across multiple Metaverse platforms. Moreover, many solutions are developed for domain specific use cases and are not evaluated in cross platform or mobile centric Metaverse environments.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Motivated by the limitations identified in existing studies, we designed BlockVerse with a focus on mobile usability and practical access control rather than purely conceptual identity models. By enabling wallet-based authentication and cross platform access control, BlockVerse aims to improve usability and user control while addressing practical deployment considerations that are not fully explored in existing blockchain based identity management solutions.

3. APPLICATION MODEL

In the Metaverse, a user is digitally represented by an avatar [2]. A digital identifier is used to associate user related information with the corresponding avatar. Access to Metaverse services typically requires users to register with multiple platform servers, which often involves sharing identifiers, passwords, and personal data. In many existing systems, such identifiers are not stored or managed in a fully secure manner, increasing the risk of information leakage, unauthorized modification, and identity theft. Furthermore, adversaries may create malicious avatars to deceive users in virtual environments, where mechanisms for verifying the identity of interacting entities are often limited [10]. These challenges can lead to fraud involving virtual assets, impersonation, and privacy violations [4].

As the Metaverse continues to evolve, an important question arises regarding the security and trustworthiness of placing personal data and digital identities within virtual environments. Addressing this concern requires mechanisms that reduce reliance on centralized platforms while improving transparency and control. Blockchain technology plays a significant role in this context. As a distributed ledger composed of cryptographically linked blocks, blockchain provides properties such as decentralization, immutability, and transparency [19]. These characteristics make it suitable for managing identity related data in a way that reduces dependence on individual platform servers and enhances data integrity. During implementation, we found that separating access control logic from attribute storage simplified both development and testing on mobile devices.

Traditional identity and access management systems are typically centralized and therefore vulnerable to single points of failure. In contrast, blockchain based approaches enable a more distributed trust model by shifting control from centralized authorities to users and decentralized networks. Some design decisions were influenced by constraints of mobile performance and transaction latency observed during early testing. Extending the application of blockchain beyond financial systems to areas such as cybersecurity and identity management has shown potential for strengthening privacy, accountability, and user control over digital identities.

Figure 1 illustrates the conceptual blockchain enabled framework adopted in this work to support secure identity management in Metaverse environments.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

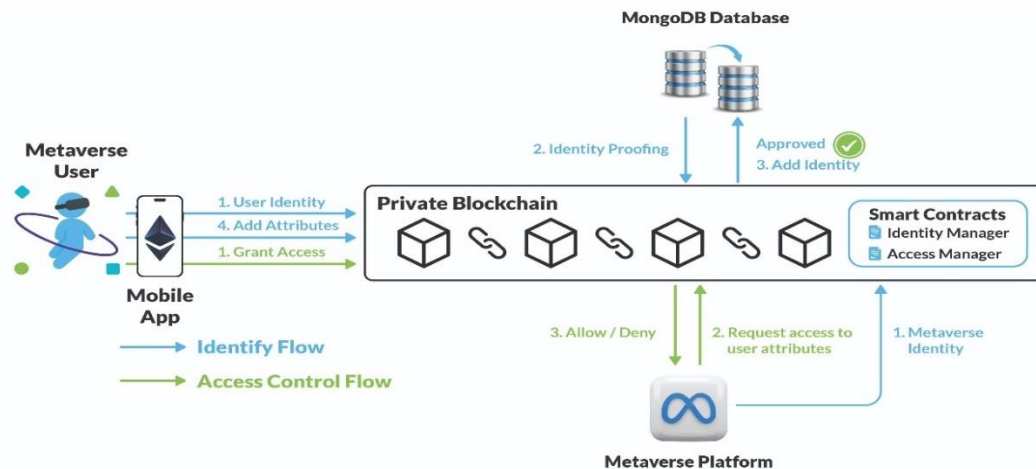
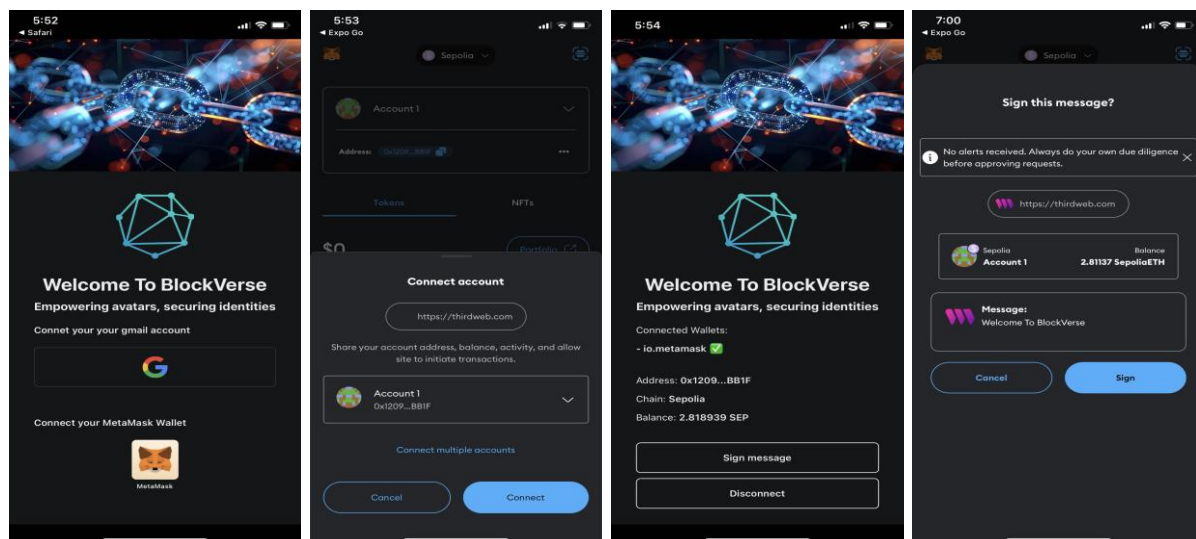


Fig. 1: Blockchain enabled framework to secure user identities in Metaverse

4. BLOCKCHAIN ENABLED FRAMEWORK TO SECURE USER IDENTITIES IN METAVERSE

In the proposed system model, a Web 3.0-based mobile application named BlockVerse is developed as a decentralized application (DApp) that leverages blockchain technology to reduce reliance on centralized identity providers. The framework distributes control across decentralized components while allowing users to manage identity related operations through a mobile interface. Blockchain is used to support integrity, transparency, and verifiability of identity and access control operations, enabling more secure avatar interactions within Metaverse environments.



(a) Connect with MetaMask (b) Connect Account (c) Connect to ETH account (d) Sign the

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

message

Fig. 2: UI for connecting MetaMask wallet.

BlockVerse is designed as a blockchain based identity and access management application that facilitates secure connections between users and multiple Metaverse platforms. The framework generates decentralized digital identifiers that are resistant to unauthorized modification. The overall architecture consists of four main layers: the physical system, the virtual system, the Web 3.0 application layer, and the blockchain infrastructure. This layered design allows users to interact with Metaverse services while retaining control over identity related operations through the mobile application.

The application provides a user-friendly interface for generating identifiers, registering with Metaverse platforms, and managing access permissions. User interactions with the blockchain are abstracted through the mobile application to improve usability while maintaining cryptographic verification through wallet-based authentication. Once development was completed, dummy transactions were submitted to the blockchain network to validate functional correctness and system behavior under controlled conditions.

BlockVerse Architecture

The BlockVerse framework is designed to support secure access to Metaverse platforms without requiring users to disclose unnecessary identity attributes. The overall workflow, illustrated in Figure 1, focuses on providing controlled access while preserving user autonomy. The main steps of the framework are summarized as follows:

Metaverse platforms register with the system in order to request identity verification services.

Users register through the mobile application and associate their identities using wallet-based authentication. The framework performs identity verification and registration based on cryptographic credentials rather than centralized authorities. After successful registration, users may define attributes and configure access policies that determine which platforms are permitted to access specific information.

Architecture Components: The main components of the framework shown in Figure 1 are described below:

Metaverse User: The owner of a Self-Sovereign Identity (SSI) who controls which identity attributes are shared with Metaverse platforms through user defined access policies.

Metaverse Platform: A service provider that requests access to user attributes in order to grant entry to Metaverse services after successful verification.

MongoDB Database: Used to store non sensitive platform related information and application metadata required for system operation.

Online ISSN

3007-3197

Print ISSN

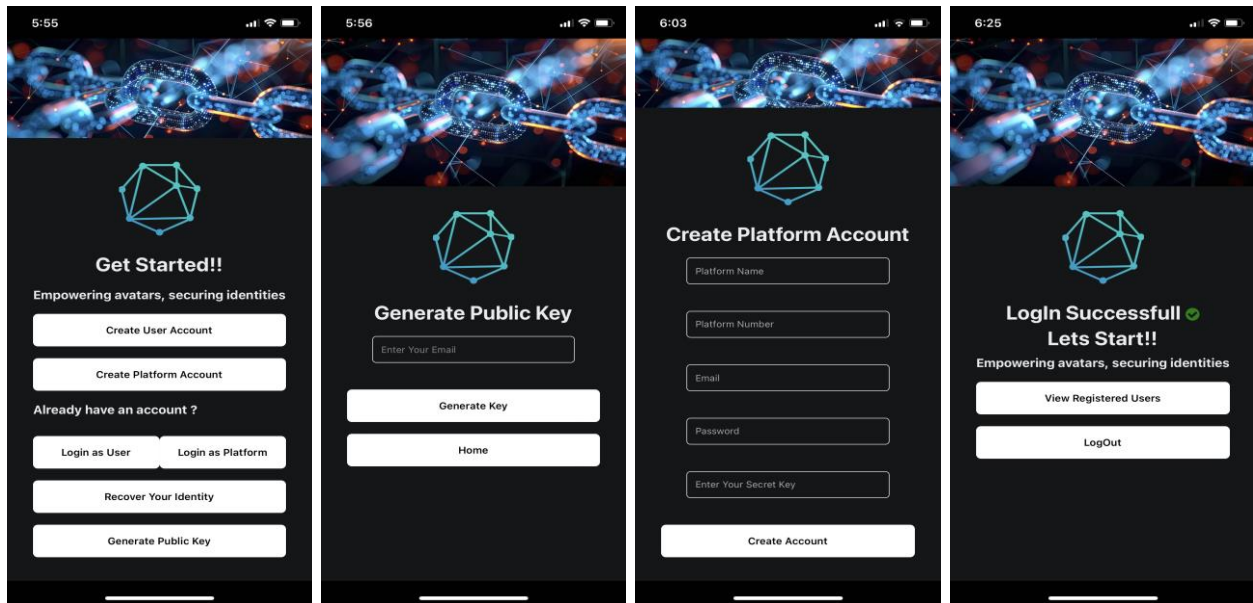
3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Mobile Application: Serves as the primary interface through which users interact with the blockchain and manage identity related operations.

Blockchain Network: The framework conceptually supports a Proof of Stake (PoS) based blockchain model to achieve energy efficient consensus and distributed trust [20]. In the prototype implementation, smart contracts are deployed on the Ethereum Sepolia TestNet to evaluate functionality and performance under realistic blockchain conditions.

Smart Contract: Smart contracts are deployed to manage identity registration and access control logic. The contract design consists of two main components:



(a) Get started screen (b) Generate public key (c) Create Platform Account (d) Account created success

Fig. 3: Generate Public Key and Metaverse Platform Registration

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Identity Manager Contract: Responsible for registering and managing user and platform identities, as well as supporting account recovery operations.

Access Manager Contract: Manages access permissions and policy enforcement. User attributes are referenced through the contract to control platform access, while sensitive data management is handled off-chain to preserve privacy.

Software Stack and Development Tools

BlockVerse was developed using a blockchain enabled architecture supported by a combination of frontend, backend, and blockchain development tools. The selected technologies were chosen to support rapid prototyping, cross platform compatibility, and seamless integration with blockchain networks.

Frontend and Mobile Development: The mobile application was developed using React Native [21] to enable cross platform deployment across Android, iOS, and web environments. Expo Go was used for on device testing, Metro Server for JavaScript bundling, and Visual Studio Code as the primary development environment.

Backend and APIs: Node.js was used to manage application logic and backend services, with Express.js providing RESTful API support for handling client requests. MongoDB serves as a trusted anchor database for storing non sensitive platform related information and application metadata. Node mailer is used to support email-based notifications during registration and recovery workflows, without transmitting or storing private cryptographic keys.

Blockchain and Smart Contracts: Smart contracts were implemented in Solidity [22] and deployed on the Ethereum Sepolia TestNet to evaluate functionality in a realistic blockchain environment. The Hardhat framework [23] was used for contract compilation, deployment, and testing, while the Thirdweb SDK [24] facilitated integration between the mobile application and blockchain components. Web3.js [25] enables wallet connectivity and interaction with the Ethereum network, and Remix was used for rapid smart contract prototyping.

Testing and Development Tools: Postman was used for API testing and request validation, while Node Package Manager (NPM) was employed for dependency management during development.

5. DECENTRALIZED APPLICATION (DAPP) IMPLEMENTATION

The proposed framework is implemented as a decentralized application (DApp) that serves as the primary interface between users, Metaverse platforms, and the underlying blockchain infrastructure. The application was developed using React Native, for user interface components. It communicates with a Node.js backend that manages routing, API requests, and interaction with off-chain services. Through the DApp, users and Metaverse platforms can register, authenticate, and manage access permissions. The application is designed to abstract blockchain complexity from end

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

users while preserving cryptographic verification through wallet-based authentication. User interactions that require blockchain operations are executed through explicit wallet confirmations, ensuring that users retain control over identity related actions.

Connection to MetaMask Wallet

Users initiate blockchain related functions by connecting their MetaMask wallet to the application. Upon accessing the homepage (Fig. 2a), users are prompted to connect their wallet. Once connected, account details and wallet balance are displayed. To verify wallet ownership, the application requests the user to sign a message, which is used for authentication without exposing private keys (Fig. 2).

Generate Public Key

New users may select the "Generate Public Key" option shown in Fig. 3a. This process involves generating a public identifier associated with the user's wallet address. An email notification is sent to the user to confirm successful generation and registration. The generated key is used as a reference for identity related operations, while cryptographic control remains within the user's wallet.

Metaverse Platform Registration

Metaverse platforms register through the interface shown in Fig. 3c. During registration, platform related information is stored in MongoDB, and verification is performed using a platform specific secret key. Upon successful registration, a confirmation screen is displayed, as shown in Fig. 3d. This process enables platforms to request identity verification and access permissions from users.

User Account Registration and Login

Users create accounts through the "Get Started" screen. Account creation requires confirmation of a MetaMask transaction, which registers the user on the blockchain. During login, users select a target Metaverse platform and authenticate using their registered credentials and wallet-based verification.

Account Deletion and Recovery

The application supports account deletion and recovery to provide users with control over their identities. Users may delete their accounts through the login interface (Fig. ??a), which triggers a blockchain transaction to update the identity state. Account recovery is supported by generating a new public identifier through the user's wallet, allowing access to be restored without reliance on centralized recovery authorities.

Access Policy and Profile Details

Users may optionally add profile attributes such as email address, date of birth, or gender through the application interface. Access permissions are managed through a policy control interface, enabling users to explicitly allow or deny Metaverse platforms access to specific attributes. This policy driven approach supports selective disclosure and user controlled access management.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

6. SCALABILITY AND INTEGRATION CONSIDERATIONS

BlockVerse is designed with scalability and interoperability in mind to support evolving Metaverse environments. The framework adopts a Proof of Stake (PoS)–based blockchain model to reduce energy consumption and improve transaction throughput compared to traditional Proof of Work mechanisms. This design choice supports more sustainable operation for identity and access management workloads that may involve frequent authentication and policy updates.

Scalability at the application level can be further supported through off-chain data management. MongoDB enables horizontal scaling through sharding and replication, allowing the system to handle increasing numbers of users and platforms without overloading blockchain resources. In addition, the use of gas efficient Solidity contracts and modular smart contract design helps reduce computational overhead and transaction costs during identity registration and access control operations. Interoperability is supported through the use of established blockchain identity standards and Web3 application programming interfaces. In particular, compatibility with ERC- 725–based identity models and standard Web3 interfaces facilitates integration with existing and emerging Metaverse platforms. This includes platforms such as Decentral and, The Sandbox, and Unity based virtual environments. While the current implementation focuses on functional integration and performance evaluation, these design choices provide a foundation for extending BlockVerse to larger scale and cross platform Metaverse deployments in future work.

7. PERFORMANCE EVALUATION

To evaluate the functionality and responsiveness of the proposed BlockVerse framework, a series of experiments were conducted in a controlled test environment. The evaluation focused on measuring key performance indicators related to identity registration, smart contract execution, and data storage operations. We conducted the experiments using 100 test users, which allowed us to evaluate system behavior under controlled but realistic conditions.

Account Registration Time: This metric measures the average time required to register a new user account, including MetaMask wallet confirmation and blockchain transaction processing. The observed average registration time was about **12.3 seconds**.

Transaction Latency: Smart contract execution latency was measured on the Ethereum Sepolia TestNet to assess blockchain responsiveness. The average transaction latency was observed to be **4.8 seconds per transaction**.

Data Storage Speed: The time required to insert platform and user related records into MongoDB was measured to evaluate off-chain data handling performance. The average insertion latency was **20 ms per document**.

Wallet Connection Success Rate: The reliability of wallet-based authentication was

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

evaluated by measuring successful MetaMask connections on the first attempt. A success rate of **98.2%** was observed. From our evaluation, we observed that the BlockVerse prototype provides responsive identity and access management operations suitable for small scale scenarios. While the evaluation does not claim large scale deployment readiness, it demonstrates the practical feasibility of integrating a DApp for a Blockchain based Identity and Access Management.

8. CONCLUSION AND FUTURE WORK

In this study, we presented BlockVerse, a decentralized application for identity and access management in Metaverse environments. By leveraging blockchain technology, BlockVerse enables users to manage digital identities and access permissions while preserving data integrity and reducing dependency on centralized identity providers. The proposed framework demonstrates how wallet-based authentication and smart contract-based access control can be integrated into a practical mobile application for Metaverse environments.

The BlockVerse architecture emphasizes usability and user control by providing a single interface for identity registration, access policy management, and account recovery. Through a hybrid on-chain and off-chain design, the system balances transparency with performance, enabling efficient identity operations while limiting unnecessary exposure of user data. Experimental evaluation indicates that the proposed approach is feasible for prototype level and small scale Metaverse scenarios.

While the current implementation focuses performance evaluation, several challenges remain for real world deployment. These include addressing regulatory and legal considerations such as user consent and data protection requirements (e.g., GDPR), strengthening security through additional authentication mechanisms, and improving interoperability across diverse Metaverse platforms. Future work will explore the integration of biometric authentication, enhanced recovery mechanisms, and broader evaluation under larger and more diverse use cases. These directions aim to further improve the robustness, usability, and applicability of decentralized identity management solutions in emerging Metaverse ecosystem.

REFERENCES

1. S.-M. Park and Y.-G. Kim, "A Metaverse: Taxonomy, components, applications, and open challenges," *IEEE Access*, vol. 10, pp. 4209–4251, 2022.
2. Azam, H., Tariq, H., Shehzad, D., Akbar, S., Shah, H., & Khan, Z. A. (2023). Fully Automated Skull Stripping from Brain Magnetic Resonance Images Using Mask RCNN-Based Deep Learning Neural Networks. *Brain Sciences*, 13(9), 1255. <https://doi.org/10.3390/brainsci13091255>
3. J. Joshua, "Information bodies: Computational anxiety in Neal Stephenson's *Snow Crash*," *Interdisciplinary Literary Studies*, vol. 19, no. 1, pp. 17–47, 2017.
4. Engr. Rukhsar Zaka, Syed Muhammad Mushtaher Uddin, Muhammad Ahsan Hayat, Aribah Murtaza, Syed Arsalan Haider, & Chaman lal Beejal. (2025). AI-

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

- Driven Cybersecurity for IoT–Cloud Ecosystems. *Physical Education, Health and Social Sciences*, 3(3), 63–76. <https://doi.org/10.63163/jpehss.v3i3.633>
5. SALEEM, H. U. S. S. A. I. N. (2012). Mobile Agents: An Intelligent Multi-Agent System for Mobile Phones. *IOSR Journal of Computer Engineering*. <https://doi.org/10.9790/0661-0622634>
 6. L.-H. Lee, T. Braud, and P. Y. Zhou, “All one needs to know about Metaverse: A survey on technological singularity, virtual ecosystem, and research agenda,” *arXiv:2110.05352*, 2021. [Online]. Available: <https://arxiv.org/abs/2110.05352>
 7. S. Banaeian Far and A. Imani Rad, “Applying digital twins in Metaverse: User interface, security and privacy challenges,” in *Proc. Int. Conf. on ICT for Smart Society (ICTSS)*, Yogyakarta, Indonesia, 2022.
 8. Blockchain-Secured Iot Framework for Smart Waste Management in Urban Environments. (2025). *The Critical Review of Social Sciences Studies*, 3(3), 1462-1467. <https://doi.org/10.59075/mcze1x98>
 9. R. Zhao, Y. Zhang, Y. Zhu, R. Lan, and Z. Hua, “Metaverse: Security and privacy concerns,” *arXiv:2203.03854*, Mar. 2022. [Online]. Available: <https://arxiv.org/abs/2203.03854>
 10. T. T. T. Ngo, T. A. Dang, V. V. Huynh, and T. C. Le, “A systematic literature mapping on using blockchain technology in identity management,” *IEEE Access*, vol. 11, pp. 26004–26032, 2023.
 11. M. Xu et al., “A full dive into realizing the edge-enabled Metaverse: Visions, enabling technologies, and challenges,” *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 656–700, 1st Quart. 2023.
 12. Borkar, S. (2005). Design challenges of technology scaling. *IEEE Micro*, 25(4), 23–29. <https://doi.org/10.1109/MM.2005.62>
 13. H.-N. Dai, Z. Zheng, and Y. Zhang, “Blockchain for Internet of Things: A survey,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.
 14. Y. K. Dwivedi et al., “Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda,” *Int. J. Inf. Manage.*, vol. 66, Art. no. 102542, 2022.
 15. S. M. Y. Aks et al., “A review of blockchain for security data privacy with Metaverse,” in *Proc. Int. Conf. on ICT for Smart Society (ICTSS)*, Yogyakarta, Indonesia, 2022.
 16. T. F. Tan et al., “Metaverse and virtual health care in ophthalmology: Opportunities and challenges,” *Asia-Pacific J. Ophthalmol.*, vol. 11, no. 3, pp. 237–246, 2022.
 17. D. Griol, A. Sanchis, J. M. Molina, and Z. Callejas, “Developing enhanced conversational agents for social virtual worlds,” *Neurocomputing*, vol. 354, pp. 27–40, Aug. 2019.
 18. B. Falchuk, S. Loeb, and R. Neff, “The social Metaverse: Battle for privacy,” *IEEE Technol. Soc. Mag.*, vol. 37, no. 2, pp. 52–61, Jun. 2018.
 19. Muhammad Ahsan Hayat, Syed Affan Ahmed, Sana Fatima, Engr. Faiza Irfan, Muhammad Osama Nizamani, & Ammar Khalil. (2025). TINY MACHINE LEARNING (TINYML) ADVANCEMENTS FOR INTELLIGENT BATTERY-POWERED IOT SENSORS. *Spectrum of Engineering*

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

- Sciences, 3(8), 818–832. Retrieved from <https://thesesjournal.com/index.php/1/article/view/875>
20. R. Heck, J. Torstensson, Z. Mitton, and M. Sena, “uPort: A platform for self-sovereign identity,” [Online]. Available: <https://www.uport.me>, accessed Mar. 13, 2021.
21. ShoCard, “ShoCard,” [Online]. Available: <https://shocard.com>, accessed Mar. 13, 2021.
22. M. Al-Bassam, “SCPki: A smart contract-based PKI and identity system,” in Proc. ACM Workshop on Blockchain, Cryptocurrencies and Contracts (BCC), Apr. 2017, pp. 35–40.
23. J. A. Kassem et al., “DNS-IdM: A blockchain identity management system to secure personal data sharing,” *Applied Sciences*, vol. 9, no. 15, Art. no. 2953, 2019.
24. T. Javed et al., “Health-ID: A blockchain-based decentralized identity management for remote healthcare,” *Healthcare*, vol. 9, no. 6, Art. no. 712, Jun. 2021.
25. R. C. Merkle, “Protocols for public key cryptosystems,” in Proc. IEEE Symp. Security and Privacy, 1980, pp. 122–133.
26. Muhammad Ahsan Hayat, Imran Ali Channa, Ubaidullah Khan, Nazia Alfred Fernandes, Urooj Tariq, & Khan Ikram Uddin. (2025). BRIDGING CLASSICAL STATISTICS AND MODERN AI TOWARD INTERPRETABLE DATA-SCIENCE MODELS. *Spectrum of Engineering Sciences*, 3(9), 525–537. Retrieved from <https://thesesjournal.com/index.php/1/article/view/1031>
27. S. King and S. Nadal, “Peercoin: Peer-to-peer cryptocurrency with proof-of-stake,” [Online]. Available: <https://peercoin.net/assets/paper/peercoin-paper.pdf>, accessed Jul. 17, 2025.
28. Muhammad Ahsan Hayat, Jahangir Baig, Shayan Ahmed, & Ahmed Faraz Ayubi. (2025). TOWARDS EARLY AND ACCURATE DISEASE DETECTION THROUGH MULTIMODAL PREDICTIVE MODELING: FUSION OF ELECTRONIC HEALTH RECORDS, MEDICAL IMAGING, AND OMICS DATA USING INTERPRETABLE MACHINE LEARNING. *Policy Research Journal*, 3(11), 01–29. Retrieved from <https://policyrj.com/1/article/view/1222>
29. C. T. B. Garrocho et al., “Blockchain-based process control and monitoring architecture for Industry 4.0,” arXiv:2007.05788, Jul. 2020. [Online]. Available: <https://arxiv.org/abs/2007.05788>
30. Available: <https://arxiv.org/abs/2007.05788>
31. Y.-G. Kim and M.-S. Jun, “A design of user authentication system using QR code identifying method,” in Proc. Int. Conf. Multimedia and Ubiquitous Engineering (MUE), Seoul, South Korea, May 2011, pp. 115–120.
32. D. Dasgupta, A. Roy, and A. Nag, *Advances in User Authentication*. Cham, Switzerland: Springer, 2017.
33. Thirdweb, “What is Thirdweb?,” 2024. [Online]. Available: <https://www.thirdweb.com>, accessed Jul. 17, 2025.
34. Musadique Hussain, Ahmed Faraz Ayubi, Satyadhar Joshi, Sumayya bibi, Nazia

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Alfred Fernandes, Muhammad Ahsan Hayat, & Huzaifa Hussain. (2025). META-LEARNING FOR FEW-SHOT AND ZERO-SHOT LEARNING: ENABLING RAPID ADAPTATION TO NEW TASKS WITH LIMITED DATA. Policy Research Journal, 3(11), 653–669. Retrieved from <https://policyrj.com/1/article/view/1311>

35. “Web3.js: Ethereum JavaScript API,” [Online]. Available: <https://web3js.readthedocs.io/en/v1.7.3>, accessed May 19, 2022.
36. J. Yang, Z. Qin, J. Kang, and Z. Han, “Metaverse identity: Core principles and critical challenges,” arXiv:2406.08029, 2024. [Online]. Available: <https://arxiv.org/abs/2406.08029>