Insights from building a blockchain-based metaverse

MARIO YAKSETIG, Lamina1, USA

This paper presents an in-depth exploration of the development and deployment of a Layer 1 (L1) blockchain designed to underpin metaverse experiences. As the digital and physical realms become increasingly intertwined, the metaverse emerges as a frontier for innovation, demanding robust, scalable, and secure infrastructure. The core of our investigation centers around the challenges and insights gained from constructing a blockchain framework capable of supporting the vast, dynamic environments of the metaverse. Through the development process, we identified key areas of focus: interoperability, performance and scalability, cost, identity, privacy, security, and accessibility.

Our findings indicate that most challenges can be effectively addressed through the implementation of cryptography and subnets (i.e., Avalanche architecture), which allow for segmented, optimized environments within the broader metaverse ecosystem. This approach not only enhances performance but also provides a flexible framework for managing the diverse needs of metaverse applications.

CCS Concepts: • **Security and privacy** → *Social network security and privacy*; **Social aspects of security and privacy**.

Additional Key Words and Phrases: Metaverse, Blockchain, Security

ACM Reference Format:
Mario Yaksetig. 2024. Insights from building a blockchain-based metaverse. -, -, Article - (2024), 13 pages.

1 INTRODUCTION

In the ever-evolving landscape of digital innovation, the concept of the metaverse has emerged as a frontier that promises to redefine our interaction with digital spaces, merging realities and digital realms into a cohesive, interactive experience. Central to this vision is the role of blockchain [5, 8], not merely as a ledger or a means of facilitating cryptocurrency transactions, but as a foundational layer that ensures security, interoperability, and ownership within these vast digital universes. Recognizing the potential of this synergy, we developed a Layer 1 (L1) blockchain specifically designed to underpin metaverse environments.

This paper presents a comprehensive account of our experiences and insights gleaned from developing a blockchain infrastructure capable of supporting the complex demands of metaverse applications. From addressing scalability challenges to ensuring a seamless user experience, our endeavor has navigated the multifaceted requirements of a technology that seeks to serve as the backbone for next-generation digital experiences. Through this work, we aim to contribute to the broader conversation on the practicalities of integrating blockchain technology with the metaverse, offering lessons learned and proposing pathways forward for others venturing into this promising yet demanding field.

2 OVERVIEW OF THE PAPER

We cover the main topics we believe to be the most important verticals to address when building a blockchain-powered metaverse platform. Concretely, we focus on the following:

- Scalability and Performance
- Interoperability

Author's address: Mario Yaksetig, Lamina1, USA, mario@lamina1.com.

ACM XXXX-XXXX/2024/–ART-

- Cost
- Identity
- Privacy
- Security
- Accessibility

We note that these verticals do not necessarily capture every detail associated with a blockchain-powered metaverse. We, however, believe the list covers most of the of challenges in the space.

3 SCALABILITY AND PERFORMANCE

As the metaverse continues to evolve, the underlying blockchain technology must not only be secure and decentralized but also scalable and high-performing. The digital expanse of the metaverse demands infrastructure that can handle vast numbers of transactions and interactions simultaneously, without compromising speed or user experience. This section delves into the performance and scalability challenges encountered in building a blockchain for the metaverse and explores potential solutions, focusing on Layer 2 (L2) solutions, sidechains, and subnets.

Layer 2 Solutions (L2s). Protocols that operate on top of a base blockchain (Layer 1), aiming to enhance its scalability and efficiency. L2s achieve this by handling transactions off the main chain, thereby reducing the burden on the base layer and allowing for faster and cheaper transactions. Examples of L2 solutions include rollups and state channels, each with its mechanism for off-chain transaction processing and finality on the main chain. While L2s offer significant improvements in performance, they sometimes introduce complexity in integration and may rely on the security mechanisms of their underlying L1 blockchain.

Sidechains. Distinct blockchains that run parallel to the main blockchain, with their own consensus mechanisms and block parameters. They are connected to the main chain via two-way bridges, allowing for asset and data transfer between the two chains. Sidechains can operate with different rules from the main blockchain, offering a customizable environment that can be optimized for specific applications, including those requiring high throughput. However, sidechains often necessitate their security measures, which can vary in robustness and may introduce additional security considerations.

Subnets. Scalable and efficient solution [2, 9] that involves creating dedicated networks of nodes to support specific applications or ecosystems within the larger blockchain network. These sub-networks can have customized rules and parameters, tailored to the unique needs of the metaverse environments they support. Subnets offer a balance between scalability, security, and customization, allowing for dedicated resources to be allocated to specific areas of the metaverse without overburdening the main network. This targeted approach to scalability ensures that high-demand areas of the metaverse can operate smoothly and efficiently, benefiting from enhanced performance and reduced latency.

Our recommendation

After thorough consideration of the scalability solutions available, we recommend the implementation of subnets for blockchain-based metaverse projects. Subnets offer a pragmatic balance between performance, security, and flexibility, enabling tailored environments that meet the specific demands of various metaverse applications. This recommendation is based on our analysis and experience in building a blockchain infrastructure that not only supports the current needs of the metaverse but is also adaptable to its future growth and evolution. Through subnets, we envision a scalable,

high-performing blockchain foundation that can accommodate the expansive and diverse nature of the metaverse.

4 INTEROPERABILITY

In the rapidly evolving landscape of the blockchain-based metaverse, interoperability stands as a foundational pillar necessary for creating a cohesive, dynamic, and expansive digital universe. The capacity for diverse blockchain networks, subnets, and digital assets, such as Non-Fungible Tokens (NFTs), to seamlessly interact and transact with one another is crucial for fostering a truly interconnected metaverse. This section explores the significance of interoperability in the context of NFTs, subnets, and cross-blockchain communications, outlining the mechanisms and standards that can facilitate these interactions.

NFT Interoperability. For users, the ability to bring or use an NFT acquired in one virtual environment into another enhances the asset's intrinsic value and the user's engagement across platforms. Achieving this level of interoperability requires adherence to standardized token protocols and metadata structures that ensure compatibility across different ecosystems. We note, however, that many game developers believe that this is an impossibility as different development companies adhere to different standards. Therefore, the development of universal marketplaces and asset exchanges that can support the seamless transfer and utilization of NFTs remains an open problem until different organizations agree on specific standards.

Subnet Communication. Subnets, which in our case designed are to cater to specific needs or communities within the larger metaverse, must be able to communicate and exchange data and assets without friction. This interoperability is facilitated through cross-subnet bridges or protocols that enable asset transfers and message passing, ensuring that subnets do not become isolated silos but rather integrated components of a larger, interconnected ecosystem.

Cross-Blockchain Communication. The diversity of blockchain architectures and consensus mechanisms presents a complex challenge for interoperability. Solutions such as blockchain bridges, interoperability protocols, and cross-chain platforms are emerging as critical tools for enabling asset transfers, smart contract invocations, and information sharing between disparate blockchains. These technologies not only enhance the fluidity of asset movement across the metaverse but also enable a broader range of collaborations and innovations by connecting previously isolated blockchain communities.

To realize the full potential of interoperability, ongoing collaboration and standardization efforts are essential. Industry-wide standards for digital assets, smart contracts, and communication protocols will play a crucial role in creating a seamless and user-friendly metaverse. Moreover, the development of decentralized interoperability solutions that prioritize security, privacy, and user sovereignty is critical for maintaining the integrity and trust of the metaverse ecosystem.

In conclusion, interoperability is a cornerstone of the blockchain-based metaverse, enabling a unified, rich, and diverse digital universe. Through standardized protocols, cross-subnet communications, and cross-blockchain bridges, the metaverse can evolve into an expansive network of interconnected experiences and economies, unlocking new possibilities for creators, users, and developers alike.

Our Approach

We adopted the architecture from Avalanche which allows for cross-subnet messaging natively. Regarding the interoperability of NFTs, we actively encourage the community to support different

types of NFTs from different creators to foster a great collaborative environment. To communicate between different blockchains, we rely on traditional (centralized) cryptocurrency bridges.

5 COST

A critical aspect of developing and operating within the blockchain-based metaverse concerns the cost implications—both in terms of development and ongoing usage. These costs significantly influence the accessibility and sustainability of metaverse projects. This section explores the dual facets of cost, emphasizing how the strategic implementation of subnets can offer an effective mechanism for cost management and optimization within the blockchain infrastructure supporting the metaverse.

5.1 Development Cost

Development Cost encompasses the initial expenses associated with creating a blockchain infrastructure tailored to the metaverse. This includes the cost of research, design, coding, testing, and deploying the necessary protocols, smart contracts, and any other blockchain components. Given the complexity and the pioneering nature of blockchain-based metaverse projects, these initial costs can be substantial. Developers must invest in robust and scalable solutions from the outset to ensure that the infrastructure can handle the demands of a dynamic and expanding virtual world.

Subnets play a pivotal role in managing development costs by enabling a modular approach to blockchain infrastructure. By allowing developers to create specific environments for different parts of the metaverse, subnets can reduce the complexity and thus the cost of developing a one-size-fits-all solution. Each subnet can be optimized for its particular use case, which means resources are allocated more efficiently, and development efforts can be more focused and cost-effective.

5.2 Usage Cost

Usage Cost refers to the ongoing expenses associated with operating within the metaverse, primarily borne by users and developers in the form of transaction fees, smart contract deployments, and interactions within the virtual environment. In traditional blockchain models, these costs can fluctuate widely based on network congestion, leading to periods of prohibitively high fees that can deter participation and stifle innovation.

Subnets offer a strategic advantage in managing usage costs by segregating the fee markets within each ecosystem. This segregation means that the activity in one part of the metaverse does not unduly affect transaction costs across the entire network. Each subnet can implement its fee structure, tailored to the specific economic and operational dynamics of its ecosystem. This localized approach to fee markets allows for more predictable and potentially lower costs for users and developers, facilitating broader access and participation in the metaverse.

Furthermore, by providing a mechanism for resource allocation and optimization, subnets can help balance the load on the blockchain infrastructure, preventing bottlenecks and ensuring more stable and manageable costs. This is particularly important in a metaverse context, where diverse activities—from simple transactions to complex interactive experiences—must be supported efficiently and affordably.

Our conclusions

Subnets not only enhance the performance and scalability of blockchain infrastructure for the metaverse but also present a viable solution for managing the critical aspects of development and usage costs. By allowing for the customization of fee structures and optimizing resource allocation, subnets can make the metaverse more accessible and sustainable for a wider range of users and developers, ultimately contributing to the growth and diversity of virtual worlds.

6 IDENTITY

6.1 History of Identity

Throughout the history of human civilization, the concept of identity has played a crucial role in ensuring trust, establishing credibility, and facilitating various social interactions. Identity, in its essence, represents something used to ensure that an individual is who they claim to be, allowing for the reliable identifiability (or recognition) and authentication of individuals within a specific context.

Since the dawn of the human language, the need to distinguish individuals has been a foundational need, and resulted in the use of names, labels, and identifiers. In effect, since as early as 3000 BC, evidence indicates the use of fingerprints to 'seal' business transactions on clay tablets in ancient Babylon, thus providing a rudimentary form of authorization. In contrast, the ancient Egypt civilization used signet rings and seals along with tattoos and jewelry as means of identification.

As society evolves and becomes more complex and interconnected, the systems and practices surrounding identity have become more sophisticated. Fast forward to the mid-1800s, when foundational databases emerged. These databases were owned and operated by governments, corporations, and banks, and served to manage and access data concerning customers, employees, and various transactions among them. Notable examples include Dun & Bradstreet, established in 1841, which provided reliable credit information on businesses for American merchants, and Companies House, founded in 1844 as the UK's state registrar of companies.

For decades, the tracking and management of citizenship, credit, marriage, birth, and other aspects of identity relied heavily on massive physical bureaucracies, where these centralized systems and institutions played a pivotal role in maintaining records and ensuring the integrity of identity-related information.

However, the 'Digital Era' brought significant changes in the landscape of identity management. In 1960, computer pioneer Fernando Corbato introduced the concept of a "username/password," establishing one of the earliest and most lasting methods of securing a digital identity. Ten years later, in the 1970s, Whitfield Diffie and Martin Hellman discovered public key cryptography, a breakthrough that enabled a symmetric key establishment over a public network. A result of this breakthrough is that public key cryptography is still widely used as a foundation for privacy on the Internet.

Subsequently, during the 1990s and 2000s, centralized services emerged as the primary providers of online identity. Consequently, users were required to create different logins (or identities) for each different platform. This shift resulted in a setting where users relied on password protection to safeguard their identities and, subsequently resulted in strict password policies from these providers in an attempt to mitigate the identity theft and unauthorized accesses. Although this solution worked partially, it also resulted in users adopting many different relatively weak passwords that were easily forgettable.

Recently, authentication on the internet has changed substantially and the "single sign-on" approach where users simply login or create accounts with a pre-established account with a big tech provider is more convenient and allows for better security and less passwords to remember (and forget). However, this approach also results in a centralization of power and gives these big tech providers control over massive amounts of data that should belong exclusively to the users.

To address this data leakage and lack of control, self-sovereign identity is now gaining traction as it allows each user to become their own identity provider, and gives back the ownership and control of the data. Nonetheless, fully achieving a self-sovereign identity approach is a very complicated challenge.

Successfully navigating this complex landscape is imperative for realizing the vision of decentralized identity management and its potential.

6.2 Identity Meets Web3

In the emerging Web3 era—where blockchain computing infrastructure powers open-source and interconnected decentralized applications in a new read/write/own online paradigm—identities (and credentials) typically involve three roles: an issuer, an ID holder, and a verifier.

The issuer is responsible for creating and assigning digital identities or credentials to individuals and is typically a trusted authority or organization that verifies the authenticity of the information before embedding it into a credential. In the digital identity space, once created, the digital credentials are cryptographically signed by the issuer to ensure unforgeability and adequate security.

The ID holder is an entity or individual who owns and manages a digital identity or credential. They possess control over their personal information and can choose when and with whom to share their credentials. ID holders interact with their digital identities through a secure digital wallet, which stores and manages their credentials.

Lastly, the verifier is an entity responsible for validating the authenticity of the shared credentials. A verifier ensures that the information provided by the ID holder is valid and trustworthy. In the digital identity space, this is traditionally performed by checking the issuer's cryptographic signature on specific attributes of the ID holder.

We also feature in the figure below a ledger as an additional entity present in the identity model. This is to capture the recent developments in the identity space where credentials are traditionally publicly issued on a distributed ledger (e.g. blockchain).

6.3 Identity Model

Identities (and credentials) typically involve three roles: an issuer, an ID holder, and a verifier.

The issuer is the entity responsible for creating and assigning digital identities or credentials to individuals. The issuer is typically a trusted authority or organization that verifies the authenticity of the information before embedding it into a credential. In the digital identity space, once created, the digital credentials are cryptographically signed by the issuer to ensure unforgeability and adequate security.

The ID holder, is an entity or individual who owns and manages a digital identity or credential. They possess control over their personal information and can choose when and with whom to share their credentials. ID holders interact with their digital identities through a secure digital wallet, which stores and manages their credentials.

The verifier is an entity responsible for validating the authenticity of the shared credentials. A verifier ensures that the information provided by the ID holder is valid and trustworthy. In the digital identity space, this is traditionally performed by checking the issuer's cryptographic signature on specific attributes from the ID holder.

We highlight a ledger as an additional entity present in the identity model. This is to capture the recent development in the decentralized identity space where credentials are traditionally publicly issued on a distributed ledger (e.g, blockchain).

We refer the reader to figure 1 below containing a diagram of the entities.

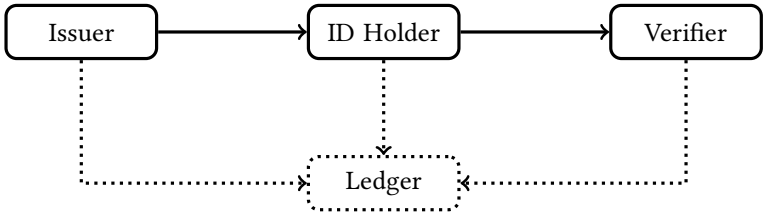

Fig. 1. Identity model encompassing the different entities. The issuer is responsible for attesting to the veracity of the claims. The ID holder who is responsible for the control over the credentials. The verifier who requires the ID holder to provide proof of specific attributes. We denote in dotted lines the optional use of a Ledger, that can potentially store credentials or some form of cryptographic commitment to credentials.

6.4 Identity Verticals

We divide identity into the following verticals: identification, authentication, authorization, credential management, security, and privacy. We refer to figure 2 for a visual illustration of this separation.

Identification. Initial process of representing an individual, entity, or device in case it is a digital context, typically involving the assignment of a unique identifier, such as a username or a digital ID number.

Authentication. Process of verifying the identity of a user, device, or system. This step usually involves validating credentials against a known set of data.

Authorization. Once the identity is authenticated, the process of authorization determines what actions the authenticated entity is permitted to perform within the system. This vertical often involves the use of access controls and permissions.

Credential Management. This involves the creation, issuance, and management of digital credentials used for authentication. It can also include processes for recovering lost credentials or updating and revoking them when necessary.

Privacy. In digital identity systems, privacy management is crucial. It involves ensuring the confidentiality of personal information, providing individuals with control over their data, and complying with relevant data protection regulations.

Security. This encompasses measures taken to protect digital identities and related processes from threats and attacks. It can include encryption, secure storage, intrusion detection systems, and other security protocols.

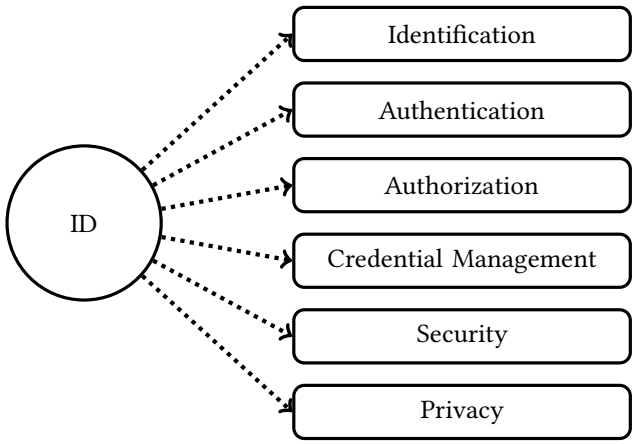

Fig. 2. Caption

6.5 Naming Service

In the development of our blockchain infrastructure for the metaverse, we recognized the critical importance of user identity and the potential vulnerabilities associated with it. To address this, we introduced the Lamina1 Naming Service (L1NS), a pivotal feature designed to enhance both user experience and security within the digital realm.

The L1NS serves a dual purpose: it not only facilitates a more user-friendly approach to navigating the blockchain by allowing users to claim an initial username for free, thus replacing the cumbersome hexadecimal wallet addresses with easily memorable identifiers, but it also embodies our commitment to user safety. A key design principle of the L1NS was to prohibit the registration of wallet addresses as usernames. This decision was made with a keen awareness of the phishing threats that have emerged in similar naming services, as evidenced by recent attacks on the Ethereum Name Service [1]. By disallowing wallet addresses as usernames, we significantly reduce the risk of phishing attacks, where malicious actors could otherwise impersonate wallet addresses to deceive users.

This strategic choice underscores our holistic approach to security, where prevention is prioritized through thoughtful system design. The L1NS is not merely a convenience tool; it is a robust security measure that anticipates and mitigates specific attack vectors. In implementing this feature, we aimed to strike a balance between user-friendliness and the imperative to safeguard against sophisticated digital threats.

Furthermore, the decision to offer the initial username registration for free is rooted in our dedication to accessibility and inclusivity. We believe that entry barriers should be minimized to foster a broad and diverse user base. By removing financial hurdles at the point of entry, we make it easier for individuals from varied backgrounds to join and contribute to the metaverse, enriching the community with a wider range of perspectives and experiences.

In summary, the introduction of the Lamina1 Naming Service reflects our commitment to creating a metaverse that is not only accessible and user-friendly but also secure and resilient against evolving digital threats. Through innovative features like the L1NS, we aim to build a foundation that supports a safe, inclusive, and thriving digital ecosystem.

6.6 Private Authentication

Using Σ–Protocols [6, 10], users can prove using zero-knowledge proofs [3, 4, 6, 7] the following statement: "I know one of the secret keys associated with this set of public keys". This allows for secure authentication while preserving privacy of the user.

Our takeaways

Identity in the web3 space is a very complicated challenge. We note that the space is incredibly fragmented and many different companies are trying to achieve the same objectives often using very similar approaches. We highlight the importance of a secure and usable naming service as it resonates with users since traditionally users have to memorize a username (and a password). Additionally, the support of zero-knowledge proving is of extreme importance as many users want to be able to have different aliases according to the app being used.

7 PRIVACY

Privacy emerges as a cornerstone of user trust and security, especially within the expansive realms of the metaverse. As users navigate through diverse virtual experiences, their ability to control and selectively disclose personal information becomes paramount. This section delves into the significance of privacy in the metaverse, emphasizing the nuanced requirements of users and the mechanisms that can be implemented to safeguard their data.

The metaverse, by design, is a tapestry of interconnected experiences, each with its own context and set of interactions. Users may partake in a wide range of activities, from social gatherings and gaming to education and commerce. With this variety comes a complex landscape of privacy needs. For instance, a user might be willing to share their avatar and gaming achievements in a public forum but prefer to keep their transaction history in a virtual marketplace private. This variability underscores the necessity for flexible privacy controls that empower users to manage the visibility of their personal and transactional data.

Effective privacy in the metaverse hinges on the development and implementation of robust data protection protocols. These protocols should enable users to specify their privacy settings at a granular level, allowing for the selective disclosure of information based on the context of the metaverse experience. Privacy settings must be intuitive and accessible, ensuring that users of all technical proficiencies can navigate and configure them according to their preferences.

Moreover, the underlying blockchain infrastructure must support these privacy preferences. Technologies such as zero-knowledge proofs (ZKPs) offer promising solutions in this regard. ZKPs enable the verification of transactions or interactions without revealing the underlying data, thus preserving the privacy of user actions while maintaining the integrity and security of the blockchain.

In addition to technical solutions, privacy in the metaverse also requires a strong ethical framework. Developers and operators of metaverse platforms must adhere to principles of data minimization, collecting only the information necessary for the intended experience and retaining it for no longer than needed. Transparency about data collection, processing, and sharing practices is essential to building user trust. Users should be informed about how their data is used and have the option to opt out of data collection processes that they are uncomfortable with.

Our remarks

Interoperability plays a crucial role in privacy as well. As users move between different experiences and subnets within the metaverse, their privacy preferences should seamlessly carry over. This necessitates standards and protocols that enable the consistent application of privacy settings across diverse environments and platforms.

Privacy is not just a feature but a fundamental right that must be embedded into the fabric of the metaverse. By prioritizing user control over personal information and implementing sophisticated data protection measures, developers can create a safe, secure, and trustful environment. A metaverse built with privacy at its core not only protects users but also enriches their experience, fostering a space where everyone can explore, interact, and create with peace of mind.

Presently, we are exploring the best mechanisms to ensure the privacy of users across different experiences in an efficient and secure manner.

8 SECURITY

In the context of a blockchain-based metaverse, security is not merely a feature but a foundational requirement. The integrity and trustworthiness of the metaverse rely on the cryptographic robustness of the system, the security of the underlying blockchain, and the protection of its digital assets. This section explores the multifaceted approach to ensuring comprehensive security within our metaverse infrastructure, highlighting the importance of cryptographic techniques, blockchain security mechanisms, and asset protection strategies.

Cryptographic Security. Ensures the confidentiality, integrity, and authentication of transactions and data. Our blockchain employs advanced cryptographic algorithms, including asymmetric encryption for secure key exchanges, hashing functions for integrity verification, and digital signatures for authentication. These cryptographic primitives are essential for creating a secure communication channel between parties, safeguarding user identities, and preventing unauthorized access to sensitive information.

Blockchain Security Mechanisms: The security of the underlying blockchain is critical to maintaining the overall security posture of the metaverse. We implement a robust consensus mechanism that not only facilitates decentralized decision-making but also provides resistance against common attacks such as double-spending and 51% attacks. By carefully selecting and optimizing our consensus protocol, we ensure that the blockchain can operate securely and efficiently, even in the face of concerted malicious efforts. Furthermore, regular security audits and stress testing of the blockchain infrastructure help to identify and mitigate potential security weaknesses, reinforcing the resilience of the system.

Asset Protection: Digital assets, including Non-Fungible Tokens (NFTs), play a pivotal role in the metaverse economy, representing ownership of virtual items, property, and more. Protecting these assets from theft, fraud, and other security threats is paramount. To this end, we employ smart contract security measures, including thorough code reviews, static analysis, and formal verification, to prevent vulnerabilities such as reentrancy attacks, overflow/underflow errors, and unauthorized access. Additionally, we advocate for and implement secure wallet practices, such as multi-signature wallets and hardware wallet integration, providing users with robust tools to manage and protect their valuable digital assets.

In addressing the broader challenge of interoperability—both within our ecosystem's subnets and among different blockchains—we prioritize security in the design of cross-chain communication protocols. These protocols are crafted to ensure that asset transfers and information exchanges across different blockchain environments maintain the highest security standards, preventing cross-chain attacks and data leaks.

Our conclusions

The security of our blockchain-based metaverse is built on a foundation of strong cryptographic practices, a secure and resilient blockchain infrastructure, and rigorous protection of digital assets. By addressing these critical components, we aim to provide a safe and trustworthy environment

where users can freely explore, interact, and transact. As the metaverse continues to evolve, we remain committed to advancing our security measures, ensuring that our digital world remains a secure haven for all its inhabitants.

9 ACCESSIBILITY

In this section we cover the required accessibility of a metaverse platform. Concretely, anyone should be able to use the system and interact with most (if not all) experiences.

The promise of the metaverse lies not only in its vast, immersive landscapes but also in its potential to be an inclusive, democratized space where anyone, anywhere, can participate, create, and explore. Accessibility in the context of a blockchain-based metaverse encompasses two critical dimensions: the ease of participating in metaverse experiences and the accessibility of joining and contributing to the network itself. Achieving high levels of accessibility in both areas is fundamental to realizing the full potential of the metaverse as an open, decentralized platform for innovation, entertainment, and social interaction.

Participation Accessibility. Ability of users to easily access and engage with the metaverse. This includes intuitive user interfaces, minimal technical requirements for devices, and affordable access points. To ensure that participation is as broad as possible, metaverse platforms must prioritize cross-platform compatibility, allowing users to access the virtual world from a variety of devices, including smartphones, PCs, and VR headsets. Moreover, lowering the barriers to entry involves optimizing the metaverse for varying levels of internet connectivity and computing power, ensuring that users from different economic backgrounds and geographic locations can have a seamless experience.

Developers can enhance participation accessibility by adopting user-friendly design principles, offering scalable graphics settings, and providing clear guidance for newcomers. Furthermore, educational resources and community support can empower users to not only navigate the metaverse more effectively but also contribute to its development and governance.

Network Accessibility. Mechanisms by which individuals can join and support the blockchain network underpinning the metaverse. A truly decentralized metaverse requires that the process of becoming a node or validator on the network is open and feasible for a wide array of participants. This means that the hardware and financial requirements for running a node should not be prohibitive. Decentralization is critical for ensuring that the metaverse remains a public, transparent, and secure environment, resistant to censorship and centralized control.

Achieving network accessibility involves implementing consensus mechanisms that are inclusive and energy-efficient, such as Proof of Stake (PoS), which, unlike Proof of Work (PoW), does not require extensive computational power. Additionally, initiatives to educate and onboard potential validators are essential, as they help to distribute network governance more widely and deepen community engagement.

The integration of identity verification processes that respect user privacy and autonomy is also crucial. These systems should enable secure, anonymous participation while preventing fraud and abuse, thus maintaining the integrity of the metaverse without unnecessary barriers to entry.

In conclusion, accessibility is a multifaceted challenge that requires careful consideration of both user experience and network participation. By addressing these aspects, developers can create a metaverse that is truly open to all, fostering a rich, diverse community that drives innovation and shared experiences. Achieving this vision of accessibility will be key to unlocking the transformative potential of the metaverse, making it a space where everyone has the opportunity to explore, create, and connect.

Our notes

Accessibility is an extremely important topic as it touches on the fundamental principles of the blockchain and web3 space. Therefore, it is crucial to have a system where anyone can join the network and either build or interact with dApps.

10 CONCLUSION

In our journey to build a blockchain infrastructure tailored for the metaverse, we have traversed a landscape marked by technical challenges, innovative solutions, and invaluable insights. This paper has outlined our experiences and the lessons learned from developing a Layer 1 (L1) blockchain designed to underpin metaverse experiences. Through this endeavor, we have not only contributed to the burgeoning field of blockchain technology but also taken significant strides towards realizing the full potential of the metaverse as a decentralized, inclusive, and secure digital realm.

Our exploration of performance and scalability underscored the critical need for an infrastructure that can support the dynamic and expansive nature of the metaverse. The implementation of subnets emerged as a key solution, offering a balance between scalability, performance, and cost efficiency. By enabling targeted optimizations and segregating fee markets, subnets provide a flexible and scalable framework that can accommodate the evolving demands of metaverse applications.

Cost considerations, both in terms of development and usage, played a pivotal role in our strategic planning. We recognized early on that minimizing barriers to entry and participation was essential for fostering a diverse and vibrant metaverse community. Our adoption of subnets significantly contributed to this goal, offering a mechanism to manage and optimize costs effectively, thereby ensuring that the metaverse remains accessible to a broad audience.

Accessibility emerged as a fundamental theme in our work, reflecting our commitment to creating a metaverse that is open and available to all. The development of the Lamina1 Naming Service (L1NS) exemplified our approach to enhancing user experience and security. By providing users with an initial username for free and preventing the use of wallet addresses as usernames, we addressed both usability and security concerns, paving the way for a safer and more user-friendly digital environment.

In conclusion, our journey in building a blockchain-based metaverse has been both challenging and rewarding. The insights gained from this endeavor have profound implications for the future of digital spaces. We have demonstrated the feasibility of a decentralized, scalable, and secure infrastructure that can support the diverse needs of the metaverse. As we look forward, it is clear that the lessons learned from this project will serve as a valuable foundation for future innovations in the field. The metaverse stands at the threshold of a new era of digital interaction, and through our efforts, we are one step closer to unlocking its full potential.

ACKNOWLEDGMENTS

We thank Neal Stephenson for constructive feedback.

REFERENCES

[1] Hayden Adams. 2024. https://twitter.com/haydenzadams/status/1757632516444311937

[2] Avalanche. 2018. Avalanche: Create without limits. https://www.avax.network/

[3] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. 2018. Scalable, transparent, and post-quantum secure computational integrity. *IACR Cryptol. ePrint Arch.* (2018), 46. http://eprint.iacr.org/2018/046

[4] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. 2014. Succinct non-interactive zero knowledge for a von Neumann architecture. In *Proceedings of the 23rd USENIX Conference on Security Symposium* (San Diego, CA) *(SEC'14)*. USENIX Association, USA, 781–796.

[5] Vitalik Buterin. 2013. Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform. (2013). https://github.com/ethereum/wiki/wiki/White-Paper

[6] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. 1994. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In *Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '94)*. Springer-Verlag, Berlin, Heidelberg, 174–187.

[7] S Goldwasser, S Micali, and C Rackoff. 1985. The knowledge complexity of interactive proof-systems. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing* (Providence, Rhode Island, USA) *(STOC '85)*. Association for Computing Machinery, New York, NY, USA, 291–304.

[8] Satoshi Nakamoto. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. (May 2009). http://www.bitcoin.org/bitcoin.pdf

[9] Team Rocket. 2018. Snowflake to Avalanche : A Novel Metastable Consensus Protocol Family for Cryptocurrencies Team Rocket. https://api.semanticscholar.org/CorpusID:198184325

[10] C. P. Schnorr. 1991. Efficient signature generation by smart cards. *J. Cryptol.* 4, 3 (jan 1991), 161–174.

Received 20 February 2007; revised 12 March 2009; accepted 5 June 2009