LITEPAPER

IDENTITY

V 1.1

01 INTRODUCTION

“Identity” had been forever changed by the Internet; formerly it had meant “who you really are” but now it meant “any one of a number of persistent faces that you can present to the digital universe.”

– Neal Stephenson, Fall; or Dodge in Hell[1]

Imagine a world where who you are transcends physical boundaries — a space where your existence is both fluid and immutable, crossing virtually all borders, boundaries, and experiences.

This is the essence of the open metaverse we envision: a three-dimensional audiovisual universe in which a wide variety of different experiences are distributed across virtual space in a coherent and agreed-upon configuration, capable of being accessed by very large numbers of users at the same time.

[1] https://www.nealstephenson.com/fall,-or-dodge-in-hell.html

At LAMINA1, our mission is to empower the creation of an open and immersive online world where individuals enjoy privacy and prosperity as they move through it. As we bring this vision to a reality, few topics hold as much importance and urgency as identity — the ability to prove who you are at any given moment and use that proof to navigate freely across virtual space and time. Identity, in its various forms, underpins essential aspects of future ownership, provenance, freedom, and online interaction in any blockchain. Understanding its significance and its challenges will be vital as we shape the landscape of this digital frontier.

This litepaper serves several crucial purposes in our development as a blockchain for the open metaverse: To shed light on the history and current state of identity solutions within the Web3 and blockchain space, to explore the issues and challenges that lie ahead for its creators, and provide insights into the different approaches we are investigating for the LAMINA1 platform.

This paper will not set out to answer every question surrounding how identity will work on LAMINA1, nor will it propose definitive solutions. The metaverse identity space, in particular, is a rapidly changing and expanding domain, and as such, our concepts and approaches will likely continue to evolve alongside the growth of LAMINA1 and the open metaverse at large.

To ensure the accuracy and credibility of our analysis, this litepaper draws upon a wealth of data, research, and expertise drawn from our Early Access Partners[2], external research, and direct surveys/inputs from our vibrant Discord community of builders and creators on LAMINA1.

By incorporating these diverse perspectives throughout this paper, we aim to provide an overview of the current landscape and begin to offer a compelling argument for the identity solutions we are considering. As we scale this exciting new frontier, it is our firm belief that an open and collaborative approach to identity will pave the way for a metaverse that empowers and embraces every individual who participates in it.

We invite builders everywhere to join us.

[2] https://www.lamina1.com/ecosystem

02
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[3], thus providing a rudimentary form of authorization. In contrast, the ancient Egypt civilization used signet rings and seals[4] along with tattoos and jewelry as means of identification[5].

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[6], established in 1841, which provided reliable credit information on businesses for American merchants, and Companies House[7], 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[8] 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[9], 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 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.

[3] https://link.springer.com/chapter/10.1385/1-59259-946-X:117
[4] https://www.britannica.com/art/signet-ring
[5] https://journals.sagepub.com/doi/full/10.1177/03075133221130094
[6] https://www.dnb.com/
[7] https://www.gov.uk/government/organisations/companies-house/about
[8] https://www.nytimes.com/2019/07/12/science/fernando-corbato-dead.html
[9] https://cr.yp.to/bib/1988/diffie.pdf

Recently, authentication on the internet has changed substantially, and the “single sign-on” approach[10] — where users simply log in or create accounts with a pre-established account with a big tech provider — is more convenient and allows for better security and fewer 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.

As a result, self-sovereign identity[11] 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. As the LAMINA1 chain takes shape, it will be crucial to address the multifaceted issues surrounding identity, including security, privacy, interoperability, and user control.

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

[10] https://www.researchgate.net/publication/325119173_A_Survey_on_Single_Sign-On

[11] https://www.sciencedirect.com/science/article/abs/pii/S1574013718301217

03
IDENTITY MEETS WEB3

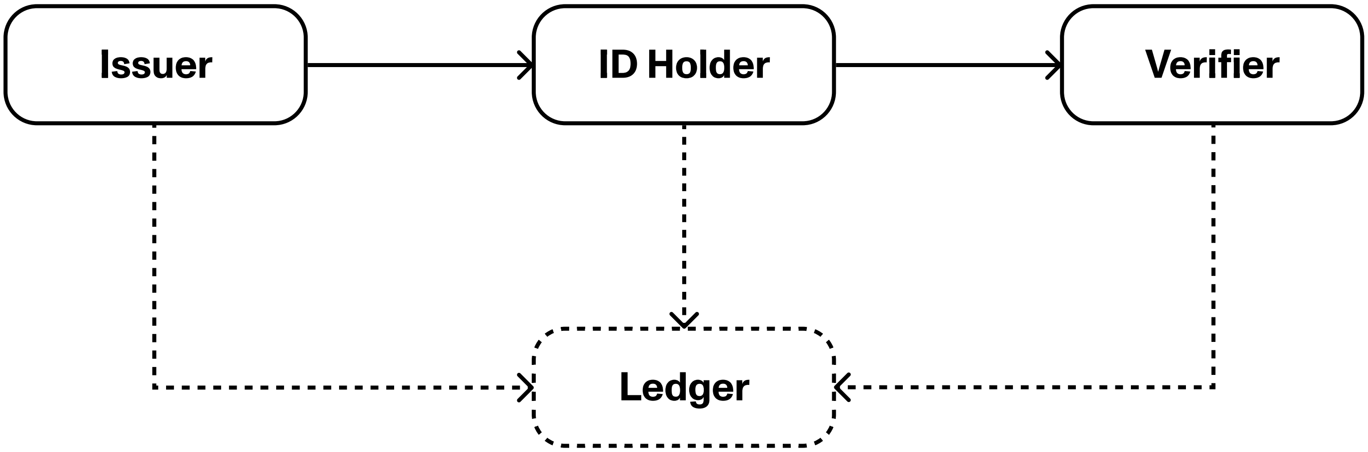
In the emerging Web3 era — where blockchain computing infrastructure powers open-source and interconnected decentralized applications in a new read/write/own online paradigm — identities (and credentials) typically involve three roles: an issuer, an ID holder, and a verifier.

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).



3.a Identity and Web3 Wallets

One of the core foundational elements associated with the decentralization ethos is the notion of a **wallet**[12]. Ideally, this wallet is controlled solely by its owner. The funds and credentials associated with these wallets are then stored on the blockchain, which is decentralized and replicated over different nodes in the world.

A result of this architecture is that any new notion of identity and credentials traditionally involves the wallets of the users, combined with the use of Non-Fungible Tokens, Soulbound Tokens, and/or Verifiable Credentials along with Decentralized Identifiers.

Such wallet addresses, however, are traditionally represented as a long string of random alphanumeric characters. This representation often results in a poor user experience and difficulties in remembering and/or sharing such addresses. We highlight name services as a possible solution to this problem.

Name services[13] allow users to register unique domain names and associate them with their individual wallet addresses. As a result, a complicated wallet address could be linked to a domain name that is easy to remember and share, thus improving the overall user experience. Name services could also create an important foundation for the identity space as they allow users to claim domain names that match their traditional Internet and social media usernames, thus rolling over certain elements of their existing identity into Web3.

3.b Non Fungible Tokens (NFTs)

An **NFT**[14] is a type of digital asset that represents ownership or proof of authenticity of a unique item or piece of content, using blockchain technology. Unlike cryptocurrencies such as Bitcoin or Ethereum, which are more fungible and can potentially be exchanged on a one-for-one basis, NFTs are distinctive and cannot be exchanged on a like-for-like basis, thus conferring uniqueness to the assets they represent. This uniqueness is then cryptographically verified on the blockchain, providing immutable proof of ownership and provenance. Presently, there exist name services that treat domain names as NFTs. As a result, domain registrations inherit the same benefits as NFTs and can be transferred using the existing infrastructure.

[12] https://ieeexplore.ieee.org/document/9315193

[13] https://circleid.com/posts/20230120-blockchain-domains-and-what-they-could-mean-for-online-scams-and-brand-protection

[14] https://ethereum.org/en/developers/docs/standards/tokens/erc-721/

3.c Soulbound Tokens (SBTs)

An **SBT**[15] is a non-transferable and non-fungible token embedded in a blockchain that represents personal or entity-specific information, such as medical records or work history. While NFTs typically symbolize ownership of digital assets, SBTs embody a person or entity's reputation within the Web3 digital space. Importantly, SBTs hold no intrinsic monetary value and cannot be exchanged or traded once allocated to a specific wallet, reflecting the 'soulbound' concept from gaming where items are permanently linked to a player's character.

3.d Verifiable Credentials

Verifiable credentials[16] are a type of digital credentials that provide a way to prove the authenticity and integrity of information about an individual or entity. They are typically issued by trusted organizations or institutions, such as governments, educational institutions, or professional associations, and are designed to be tamper-proof and verifiable by anyone who needs to verify the contained information. These credentials contain specific pieces of information, such as personal identity details, educational qualifications, professional certifications, or any other relevant attributes. The issuer digitally signs the credentials, attesting to their authenticity and integrity. The credentials are stored in a digital format and can use decentralized or distributed ledger technologies, such as blockchain.

Verifiable credentials enable individuals to have more control over their personal data and provide a mechanism for selective disclosure. With verifiable credentials, individuals can share specific information from their credentials with different parties, limiting the amount of information disclosed and reducing the need to share copies of their original documents.

We also highlight the notion of decentralized identifiers (**DIDs**[17]), which are unique identifiers that users create, own, and control. These DIDs can be used to identify various entities like people, organizations, devices, or even abstract concepts. DIDs are decentralized and are designed to be unambiguous. Therefore, no single entity, other than the owner, has control over such identifiers.

DIDs are deeply connected to verifiable credentials, as together, they can establish a foundation for secure and trustworthy digital identities. On one hand, decentralized identifiers provide the required infrastructure for identifying and controlling the identity of a subject. On the other hand, verifiable credentials enable the issuance and verification of the credentials associated with such identity. Therefore, verifiable credentials can be securely linked to decentralized identifiers and produce a decentralized identity approach that revolves around the users and their privacy.

[15] https://ssrn.com/abstract=4105763
[16] https://www.w3.org/TR/vc-data-model/
[17] https://www.w3.org/TR/did-core/

04 IDENTIFIABILITY VS. AUTHENTICATION

“Everybody who goes into the metaverse is represented by this audiovisual body called an avatar, which becomes their identity in the metaverse. It’s linked to who they are, and it expresses who they are in some way. And it’s how they interact socially. It’s what makes the metaverse into a social environment.”

– Neal Stephenson, Metaverse Identity AMA[18]

Identifiability and authentication represent two fundamental aspects of identity management in the next online era, each serving distinct purposes in the realm of digital interactions. While interconnected, they are also different. Therefore, it is essential to understand these differences to effectively address the challenges of decentralized identity.

[18] https://www.youtube.com/watch?v=RGzZjBpadHo

4.a Identifiability

Identifiability refers to the ability to uniquely associate (or identify) an individual with a specific identity or set of attributes. Concretely, identifiability involves the process of recognizing and distinguishing individuals based on their unique characteristics, such as their name, unique identifier, or other distinguishing factors.

In the digital realm, identifiability traditionally relies on the use of unique identifiers, such as usernames, or email addresses. These identifiers serve as key references to link individuals with their associated data and activities within digital systems. The identifiability aspect of identity management focuses on accurately and reliably identifying individuals in a digital environment, enabling the tracking of transactions, records, and interactions associated with a particular identity.

In the context of decentralized identity, identifiability becomes a critical component that enables individuals to assert their identities potentially across multiple platforms and services. Moreover, identifiability represents a big obstacle to privacy as it allows for the profiling of individuals and their actions. The two concepts, however, are not mutually exclusive and the use of novel privacy technologies (e.g. **ZK-SNARKs**[19]) represents a promising path that will potentially allow users to achieve the strictly required level of identifiability while also protecting their privacy.

4.b Authentication

In modern digital applications, authentication can traditionally be classified into three categories:

- **Something a user knows.** For example, a password.
- **Something a user has.** For example, a bank card.
- **Something a user is.** For example, biometrics such as fingerprints or face recognition.

To authenticate themselves on the Internet, users provide websites with a username/password pair. By doing so, a user is able to prove knowledge of a secret that allows them to access specific resources on such websites. Alternatively, to access locked resources on their phones, users traditionally have two complementary approaches: fingerprint or face recognition and a PIN (or passcode). Typically, the passcode acts as a fallback for the biometric approach.

Web3, on the other hand, introduces a new model of online authentication. Instead of relying on a centralized server to store and verify user credentials, Web3 uses blockchain to allow users to create an identity that is tied to their digital wallet. This wallet, which is essentially a pair of cryptographic keys, is used by users to authenticate themselves. To do so, users sign a specific action request to prove that they are the owners of a specific wallet attempting to perform such an action.

[19] https://people.cs.georgetown.edu/jthaler/ProofsArgsAndZK.pdf

4.b Authentication (Cont.)

The private key, kept secret by the user, is used to sign transactions and authenticate their identity, while the public key, visible to everyone on the network, is used to verify these signatures, thus eliminating the need for a centralized authority to verify the identities of users. The management of such key pairs, however, is traditionally not user-friendly, as it requires the secure storage of a 12 (or 24) word seed phrase which is used to generate the secret key material. This seed phrase, if lost, results in a complete loss of the key material (and potentially funds, credentials, or any digital asset associated with such a wallet).

Presently, it is often the case that when a user installs a new Web3 dApp, they must store a new set of 12 (or 24) words, which results in an even more challenging user experience and key management setting. As a result, different platforms are introducing new approaches to wallet key generation to allow users to have a better experience and usability experience without compromising security.

While these solutions have made significant strides, they are not without their challenges. One of the main issues is the concept of key management. Losing access to a private key potentially results in the permanent loss of a user's digital identity and its associated assets. This places a significant responsibility on users. Therefore, one of the biggest outstanding issues in Web3 is the development of much-needed user-friendly key management solutions. On one hand, we want users to be able to onboard on a system as smoothly as possible. On the other hand, the generated wallets should be as secure as possible. Finding the right balance, however, remains an open question.

4.c Wallet Approaches

Below are seven approaches LAMINA1 has investigated in the current Web3/blockchain space that are both very relevant to the topics of identifiability and authentication.

Mnemonic Key Management

A critical aspect of wallet-based authentication in Web3 is the creation and management of a 12-word mnemonic phrase, which is a human-readable representation of the user's private key and is traditionally generated when a new Web3 app is downloaded. While the use of a 12-word mnemonic phrase simplifies the process of managing private keys, it introduces its own set of challenges. Concretely, this approach forces users to take on the responsibility of securely storing and managing their mnemonic phrases, which can be a daunting task, especially for those new to the Web3 space. Therefore, while mnemonic-based key management is currently standard practice in wallet-based authentication, it is clear that this approach has significant drawbacks and exposes the need for more user-friendly key management solutions.

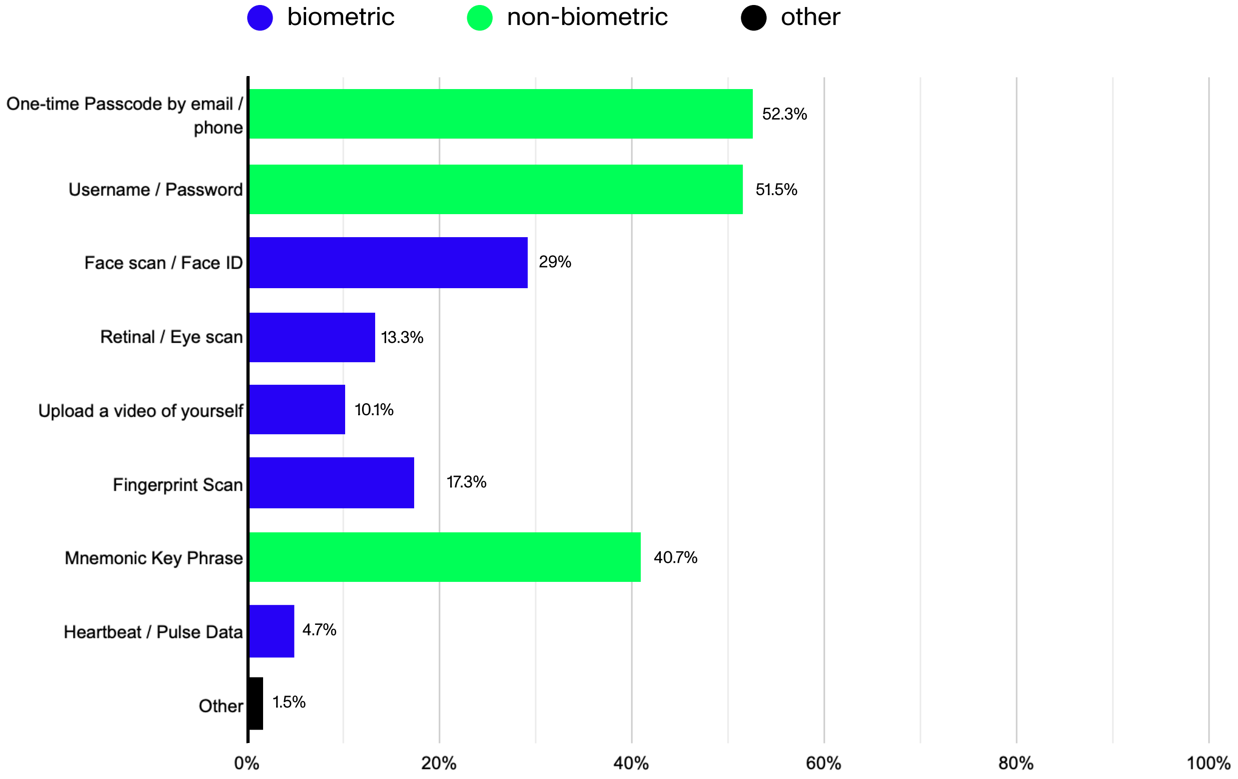
4.c Wallet Approaches (Cont.)

Biometric Authentication

We highlight that a potential approach to improve on this problem is to rely on biometric data (e.g. Face ID). This is considered quite user-friendly, especially taking into account that this is how most users authenticate themselves to access the resources on their phones.

However, results from recent surveys of the LAMINA Discord community[20] show that the use of usernames and passwords is still widely accepted among early open metaverse participants and that the use of biometrics for authentication is taken with significant skepticism.

Which of these authentication methods would you be willing to use to verify your identity?



Interestingly, this goes against many current UI/UX trends in the cryptocurrency wallet space that are attempting to leverage the use of biometrics. We highlight, however, that biometrics is something that is not necessarily secret and, as a result, should not be used as a sole element for the generation or protection of secret keys.

[20] https://discord.com/channels/981694584474181654/1024441873152102483/1113293364733943878

Multi-Party Computation

The fundamental idea behind multi-party computation (**MPC**[21]) is to distribute the computation across multiple parties in such a way that they collectively compute the desired result while keeping their private inputs confidential. Each party holds their own private input and interacts with the other parties in a secure manner to compute an output without any party gaining knowledge about the inputs of others. Concretely, it allows a group of participants to collaborate and compute a desired result without disclosing their individual inputs.

Presently, one of the primary applications of MPC in cryptocurrency wallets is for secure key generation and storage. By using a multi-party computation, a private key can be generated in a distributed manner, with each party contributing to the generation process but without a single party having access to the entire key. This separation reduces the risk of key loss or theft, as an attacker would need to compromise multiple parties to gain access to the entire key. This approach also provides a robust solution for key recovery, as the key can be reconstructed from the shares held by the different parties, even if some of them are lost.

Hardware Secure Modules

The pursuit of non-custodial solutions is gaining considerable momentum, as users strive for greater control over their digital assets. Non-custodial systems enable individuals to maintain complete control over the custody of their private keys, eliminating the need for third-party intermediaries. However, a perplexing paradox emerges when some platforms claiming to be non-custodial rely on Hardware Secure Modules (HSMs) for secret key generation and custody. In this context, HSMs are specialized hardware devices that offer enhanced security for generating, storing, and managing cryptographic keys. Integrating HSMs into blockchain aims to bolster the overall security of private key management, reducing the risk of theft or compromise.

However, the use of HSMs in supposedly non-custodial systems raises thought-provoking questions about the true nature of user control and autonomy. Can a system genuinely be considered non-custodial if it relies on external hardware for key generation? While HSMs enhance security, they introduce an element of trust in the manufacturer or provider of these devices. This trust contradicts the core principles of decentralization and self-sovereignty that non-custodial systems aim to achieve.

Credentials From OAuth

OAuth[22] is an open standard for access delegation that can be used by a credential issuer to generate and issue private credentials based on a user's authenticated session. For example, when a user logs into a service using OAuth, they grant that service permission to access certain information from their account, as defined by the scope of an OAuth token. This information can include basic profile details, email addresses, and other data. A credential issuer can then leverage this authenticated session to issue a private credential. For instance, once a user has authenticated with a service using OAuth, the credential issuer can generate a credential that attests to certain claims about the user, such as their identity, email address, or other account details. This credential can then be used by the user to prove these claims to other services, without having to share their actual OAuth token or other sensitive information (Continued on following page...)

[21] https://en.wikipedia.org/wiki/Secure_multi-party_computation
[22] https://oauth.net/

This approach provides several benefits. Firstly, it enhances privacy, as users can prove certain claims about themselves without revealing their full account details. Secondly, it provides a secure means of authentication, as the credential issuer can verify the user's claims without needing to access their actual credentials. Lastly, it provides a flexible and interoperable framework for identity verification, as these credentials can then be used across different services and platforms.

Account Abstraction

Account abstraction[23] seeks to address the issue of different blockchain account types by providing a unified interface for all accounts. Instead of having separate rules and functionalities for externally owned accounts and smart contract accounts, account abstraction proposes that all accounts should be treated as contract accounts. This means that every transaction, regardless of its origin, would be processed according to the rules defined in its contract code.

This approach provides greater flexibility for developers, as they can define custom rules for transaction processing in the contract code. This could potentially enable new features and functionalities that are not possible under the current model, especially in the (decentralized) identity space. For example, novel mechanisms to integrate recoverability in wallet addresses.

NFTs vs. SBTs

Finally, non-fungible tokens and soulbound tokens present unique opportunities for digital identities and credentials in the Web3 space. These tokens, with their inherent properties of uniqueness (NFTs) and non-transferability (SBTs), can serve as robust tools for identity verification.

NFTs can be used to represent unique digital identities or credentials. For instance, an NFT could be issued to a user as a digital passport, with the token containing verifiable information about the user's identity. This NFT could then be used to authenticate the user's identity on various platforms, with the assurance that the token, and therefore the identity it represents, is unique and cannot be duplicated.

Soulbound tokens, on the other hand, offer a different kind of utility. Given that these tokens are permanently bound to a user's wallet and cannot be transferred, they can serve as permanent credentials. For example, a soulbound token could be issued to a user as proof of an individual accomplishment (e.g., university degree) and as long as the user retains control of their wallet, they retain this proof, which cannot be transferred or sold to any other user.

The combination of NFTs and SBTs could provide a robust framework for digital identities and credentials. A user could hold an NFT as a unique digital identity, with various soulbound tokens representing different credentials or access rights associated with this identity. This would provide a high level of security and privacy, as users could prove their identity and credentials without revealing any sensitive information.

[23] https://ethereum.org/en/roadmap/account-abstraction/

4.d Privacy

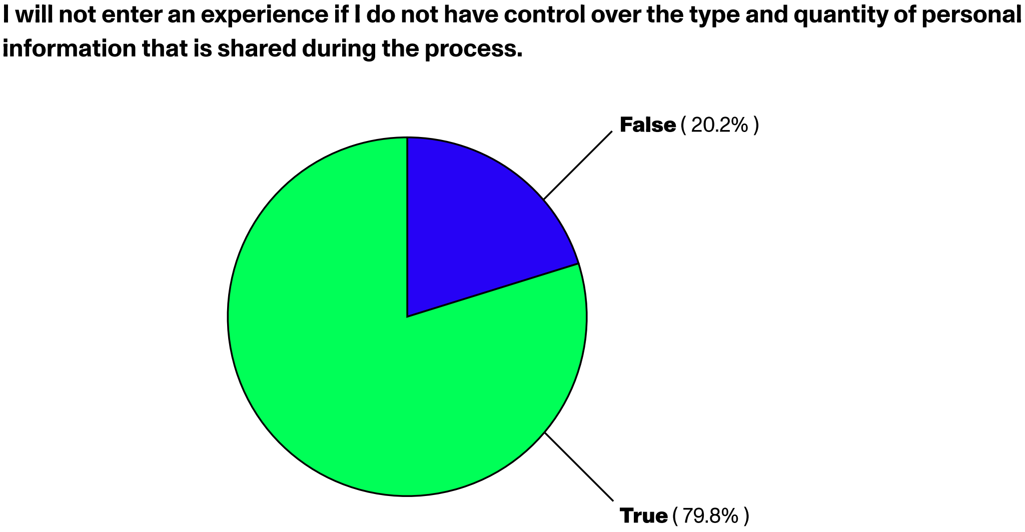
“The trend is going to be towards people trying to maintain their own identity and their own brand across multiple platforms. The more people do that, the more important it is to them, the more important it is that it looks secure, that it can’t be spoofed.That it can’t be stolen away from them. People running experiences in the metaverse are going to want to find ways to support that.”

– Neal Stephenson, Metaverse Identity AMA[24]

The ethos behind self-sovereign identities is that users are fully in control of the data associated with their identity. When issuing an identity, issuers traditionally insert specific information into the credentials of the user. As a result, the issuer now has full access to the data present in such a credential. The security of this data is now deeply connected to the security of the storage of the issuer. A decentralized identity scheme can, however, provide assurances that a specific user can restrict access to updates in the data associated with their credentials.

[24] https://www.youtube.com/watch?v=RGzZjBpadHo

4.d Privacy (Cont.)



Today, as suggested by the survey data above[25], users are increasingly more aware of the existing privacy leakages on the Internet and are actively requesting for control over the type and quantity of information that is revealed when performing specific actions online. Any identity solution LAMINA1 chooses will have to empower users by giving them means to protect their privacy far beyond what exists in the current online landscape.

Private Verifiable Credentials

One potential solution to this issue/need LAMINA1 is exploring currently is private verifiable credentials. Private verifiable credentials represent a significant advancement in the realm of digital identity and authentication as they are a type of digital credential that can be verified independently, without the need for a centralized authority, while also preserving the privacy of the user's sensitive information.

A private verifiable credential is a cryptographically secure statement made by an issuer about a subject. The issuer, which could be a trusted authority or a decentralized identity on a blockchain, asserts certain claims about the subject. These claims are then packaged into a credential and signed with the issuer's private key.

What sets private VCs apart is their focus on privacy. When a subject presents a private VC, they do not need to reveal all the information in the credential. Instead, they can choose to disclose only the minimum amount of information necessary for the verification process. This is traditionally achieved through the use of zero-knowledge proofs (e.g., ZK-SNARKs), a cryptographic technique that allows a subject to prove that certain information is true without revealing the information itself. For example, a user should be able to prove they are over a certain age without needing to reveal the full information present on a driver's license or passport. By leveraging zero-knowledge proofs, users benefit from a high level of privacy as they can prove their identity or specific credentials without exposing any unnecessary information that is potentially sensitive.

[25] https://discord.com/channels/981694584474181654/1024441873152102483/1113293364733943878

05
IMPLICATIONS FOR THE OPEN METAVERSE

"In the metaverse, you should be able to fluidly move from one place to another. You can walk out the door of one experience and go down the street, and the street itself is an environment with avatars in it. You might then turn down another street or go into a building or an amusement park or a game experience.

And your expectation is that when you do those things, your avatar naturally travels with you. You don't have to stop at the threshold of each experience and log out from one system and log on to another one."

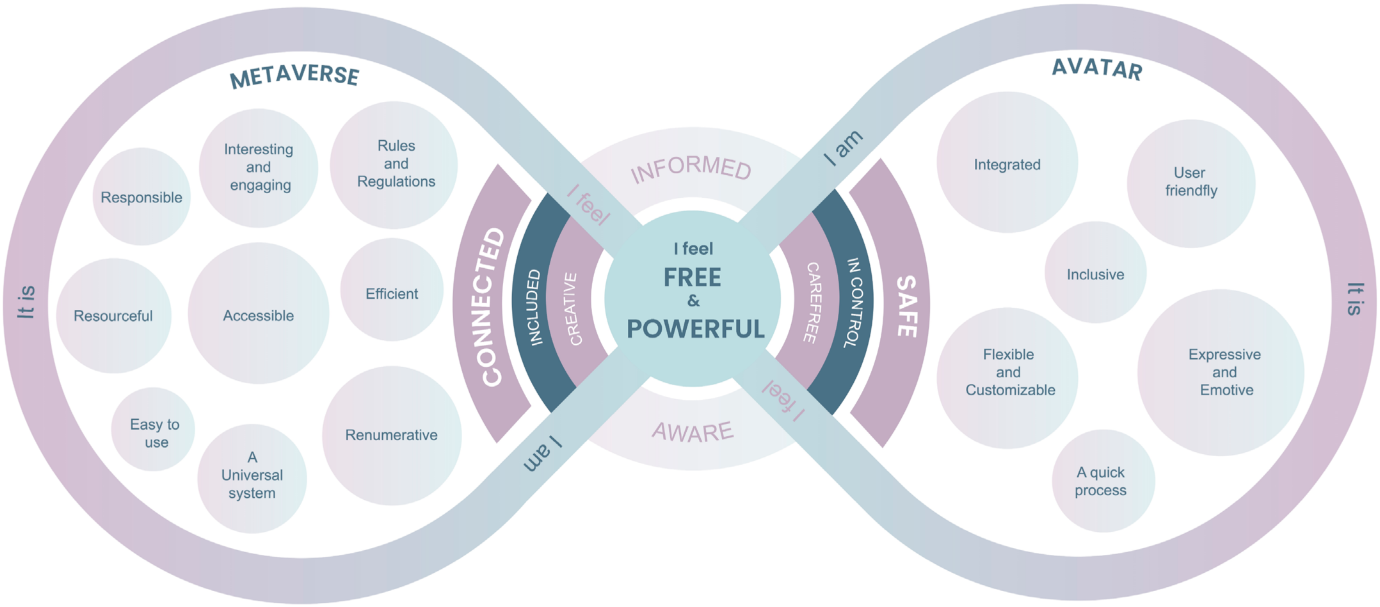
– Neal Stephenson, Metaverse Identity AMA[26]

[26] https://www.youtube.com/watch?v=RGzZjBpadHo

5.a Avatars

Related to identity, the growing role of avatars in our digital lives also signals a profound shift in the manner in which the world perceives and protects identities online. As we enter the next online era, avatars are no longer just a simple digital representation in a game or visual placeholder for a social media profile — they are quickly becoming the de-facto standard for personal identity, identifiability, and self-expression in an increasingly decentralized online world.

Recent research[27] conducted by graduate students at Savannah College of Art and Design investigated how internet users feel about metaverse identity and the avatars they use to express them, revealing the critical emotional need for a balance of freedom, safety, creativity, and empowerment in the next era of online life.



Metaverse Experience Research Group (SCAD), 2023

Avatars allow users to ensure a sense of individuality and privacy while simultaneously reflecting the user's interests and values — e.g. an identity worth protecting and taking with you across the online world.

As avatars continue to evolve, we expect a shift in the way digital goods are perceived and utilized in the context of metaverse identity as well. For example, digital wearables, which enhance the range of individual expression and interactions in metaverse and proto-metaverse experiences. Wearables provide users with a unique platform for self-expression, making digital personas more relatable and engaging, similar to the real world.

Additionally, blockchain plays a critical role in ensuring the authenticity and ownership of these digital goods. With its immutable and transparent nature, blockchain effectively validates the provenance and uniqueness of digital wearables. (Continued on following page...)

[27] https://uploads-ssl.webflow.com/63fe332d7b9ae4159d741e55/64b021c2b9d14ab16e1e14dd_Client%20Book_The%20Ideal%20Experience%20of%20Identities%20in%20the%20Metaverse%20(1)-compressed.pdf

5.a Avatars (Cont.)

Users can then adorn their avatars with a variety of digital wearables, crafting unique identities that reflect their preferences and personalities. Platforms, however, must cooperate to ensure that assets are compatible across different ecosystems or then purposefully fragment the market of digital wearables.

> “I think there is some sort of romanticism to having a digital counterpart that thinks like you, behaves like you.”
>
> – Metaverse Identity Research Group (SCAD), 2023[28]

Central to the conversation of decentralized identity is the concept of authentication. In particular, the identity of digital goods also relies on robust authentication mechanisms. In this context, authentication extends to the validation of the legitimacy of all digital goods. With the aid of rigorous authentication protocols, brands can issue valid credentials to NFTs associated with real-world assets, thereby ensuring their authenticity from the source and creating a transparent record of ownership. This approach to authentication offers brands a reliable means of establishing a verifiable chain of provenance, enabling users to rapidly check the origins of digital goods and promptly detect counterfeit items.

5.b Digital Assets in the Metaverse

For many people, the most important part of digital metaverse identity are the assets associated with the identity they carry with them across the online experiences they interact with.

On this front, LAMINA1 aims to be pivotal in addressing the issue of unauthorized usage of digital art and assets, such as NFTs. In a metaverse setting, these NFTs can represent the wearables for a specific user in the system. Presently, unauthorized digital usage is a substantial challenge for artists navigating the digital landscape as it results in substantial losses to these creators. By integrating robust authentication mechanisms, we want to empower artists to regain control of their digital creations and enable them to benefit from the legitimate use

[28] https://uploads-ssl.webflow.com/63fe332d7b9ae4159d741e55/64b021c2b9d14ab16e1e14dd_Client%20Book_The%20Ideal%20Experience%20of%20Identities%20in%20the%20Metaverse%20(1)-compressed.pdf

of their work. For example, via the use of integrated royalties. This kind of robust authentication could potentially become the backbone of the increasingly popular 'Phygital' (physical + digital) goods. As we witness an increasing interplay of physical and digital elements within goods, robust authentication mechanisms will be instrumental in verifying the authenticity and ownership of both physical and digital products. By leveraging this intersection of identity and authentication, LAMINA1 will be able to create a solid foundation for a metaverse for the people.

Additionally, to prevent scenarios where users purchase an NFT and then later find out that it disappeared due to the centralized hosting nature of the NFT, we will enforce a decentralized storage approach where users can remain assured that their digital goods remain properly stored and not at the mercy of a single server on the Internet. For example, you might buy an expensive NFT, which is hosted at a centralized URL, only to find someone has hacked in, and replaced the image located at that URL with a picture of a rug. This scam is called rug-pulling.

5.c Experiences in the Metaverse

> "...In the entire world, there are only a couple of thousand people who can step over the line into The Black Sun. [Hiro] turns and looks back at the ten thousand shrieking groupies. Now that he's all by himself in the entryway, no longer immersed in a flood of avatars, he can see all of the people in the front row of the crowd with perfect clarity...

"...They are all done up in their wildest and fanciest avatars, hoping that Da5id — The Black Sun's owner and hacker-in-chief — will invite them inside."
– Neal Stephenson, Snow Crash[29]

The metaverse is rapidly becoming a new frontier for digital identity. To access anything in the metaverse, some form of identification is required, unless the space is designed to be completely anonymous. In that case, the challenge is even more complex, as it is ideal to be able to authenticate users without identifying them.

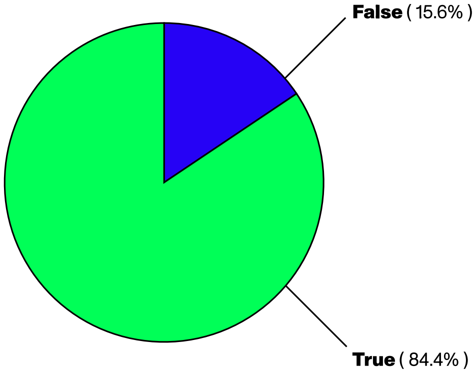
As exemplified in Neal Stephenson's Snow Crash, The Black Sun serves as a compelling exclusive club in the metaverse exemplifying the crucial role of identity verification in virtual spaces. Once inside the metaverse, users can engage in a wide range of activities, including certain experiences that require special access.

Today, these experiences can be gated behind digital tickets, which can be represented as NFTs and, in this context, serve as proof of ownership for access to these exclusive experiences. Interestingly, recent data[30] from the LAMINA1 Discord community reveal that over 80% of surveyed users believe that a person should also be able to adopt different identities in the metaverse — a position seemingly at odds with the need for exclusivity, safety, and gated access in certain online experiences. This calls to mind the online phenomena of 'aliases' or secondary accounts on social media, where people act differently since they can no longer be identified by their original username (or handle).

[29] https://www.nealstephenson.com/snow-crash.html
[30] https://discord.com/channels/981694584474181654/1024441873152102483/1113293364733943878

5.c Experiences in the Metaverse (Cont.)

A person should be able to adopt different personas / identities based on what they're doing in the metaverse.



On the one hand, a user might purchase an NFT ticket to an exclusive virtual concert. This ticket is then tied to their digital identity and can be verified by the event organizers, ensuring that only those who have purchased a ticket can access the event. This model not only provides a secure means of access control but feeds and empowers new digital experiences in the metaverse. The artists can then reward their biggest fans and 'pay it forward' by verifying their claims and attendances to their shows.

On the other hand, users with aliases, secondary accounts, or 'Finstas' may be doing so to protect their privacy, freedom, or sense of self-expression online. This is a critical need to consider while shaping the future of metaverse identity in the next online era.

06
AREAS OF FUTURE RESEARCH

"I would like to do things that are quite impossible in real life, like emulate magic, fly, and have special abilities. I feel liberated from the constraints of the physical world. I feel free in the metaverse – a space that is the closest embodiment of magic in the real world."

– Metaverse Identity Research Group (SCAD), 2023[31]

For future research in this space, we highlight the importance of interoperability and artificial intelligence. Interoperability, if done correctly, will allow users to port their existing attributes across different platforms and apps into a more unified approach. Meanwhile, artificial intelligence will allow for the novel development of new functionalities in the metaverse while also deeply affecting the corresponding authentication of items and individuals.

[31] https://uploads-ssl.webflow.com/63fe332d7b9ae4159d741e55/64b021c2b9d14ab16e1e14dd_Client%20Book_The%20Ideal%20Experience%20of%20Identities%20in%20the%20Metaverse%20(1)-compressed.pdf

6.a Interoperability

One of the key challenges in decentralized identity lies in achieving seamless interoperability across the entire ecosystem. The ability to bring your digital identity (YOU) across various platforms and applications is a complex endeavor that necessitates collaboration and standardized protocols. Despite skeptics claiming it cannot be done or may face resistance, several interoperability-focused projects and use cases have emerged. For instance, the concept of single sign-on (**SSO**[32]) has gained traction as a means to leverage authentication across multiple platforms. Exploring the potential of extending SSO capabilities beyond a single platform and enabling its interoperability across a wider ecosystem could significantly enhance user experience and simplify identity management.

If you are developing standards, protocols, or infrastructure for interoperable identity in the open metaverse, and would like to collaborate, reach out to us at ecosystem@lamina1.com.

6.b Artificial Intelligence

The advent of AI is causing a significant transformation in the everyday process of identity authentication. On the one hand, hackers and scammers are exploiting advancements in artificial intelligence to deceive individuals, such as mimicking their voices to defraud their loved ones. Consequently, it is no longer reliable to assume that a phone call received from a familiar number is genuinely from the person associated with that number.

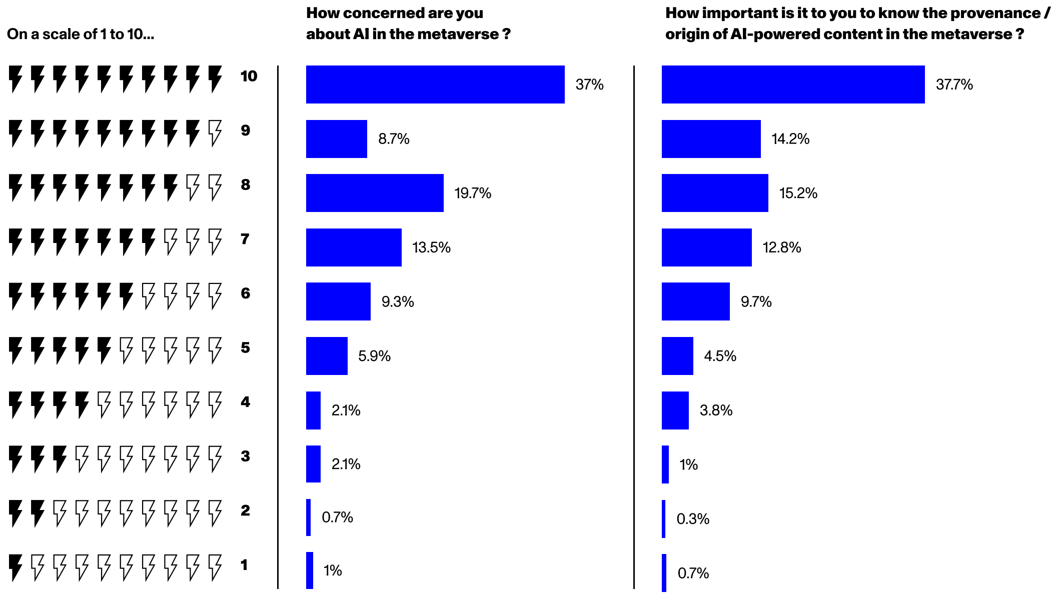
On the other hand, verifying the validity and authenticity of digital entities, such as identities, assets, or transactions, can benefit from AI-powered algorithms. For instance, AI can be utilized to determine if a person captured on camera matches the image in their identification documents, enabling enhanced know-your-customer (**KYC**[33]) processes.

Additionally, as AI-driven virtual agents, chatbots and characters become more prevalent in digital life, we believe it will become crucial to develop methods for distinguishing between interactions with real individuals and AI NPCs (Non-Player Characters).

In recent surveys[34] of the LAMINA1 Discord community, over 40% of early metaverse builders, creators, and enthusiasts signaled they were deeply concerned about AI in the metaverse. Over 90% of the community signaled they were at least somewhat concerned about its effects. Meanwhile, a similar percentage of users signaled it was very important for them to be able to know the origin/provenance of AI-powered content in the metaverse. Less than 5% of users signaled that knowing the difference was not very important.

[32] https://en.wikipedia.org/wiki/Single_sign-on
[33] https://ieeexplore.ieee.org/abstract/document/9036811
[34] https://discord.com/channels/981694584474181654/1024441873152102483/1113293364733943878

6.b Artificial Intelligence (Cont.)



Further research should explore the ethical implications of allowing AI to act on behalf of real individuals using their credentials, as well as addressing concerns surrounding identity theft and unauthorized AI use. Community research and engagement are essential in shaping the discourse around AI and decentralized identity, considering people's desire for transparency, understanding the provenance of information, and distinguishing between human and AI interactions.

For more information about LAMINA1's stance on Artificial Intelligence as it pertains to metaverse creators, read our Metaverse-as-a-Service Whitepaper[35] or listen to our latest AMA on the topic[36].

[35] https://uploads-ssl.webflow.com/63fe332d7b9ae4159d741e55/64499d8f08bd5bdd1fe6bce1_MaaS_Whitepaper_v1.0.pdf
[36] https://www.youtube.com/watch?v=vaz5gqSZIKM

07
CONCLUSION

“Reality is what we make it. Or what is made for us by the companies we keep. It is our clay from which we fashion ourselves.”

– Neal Stephenson, Twelve Tomorrows 2013[37]

In the fast-evolving landscape of Web3, decentralized identity, and the metaverse, one thing is clear: excellence is the key to shaping the future. We have set our standards high and are actively developing and contributing to solutions that meet our rigorous requirements. As we dive into the realm of decentralized identity and identity in the metaverse, we actively seek out new avenues for research and development.

We understand that interoperability is a crucial aspect of bringing digital identities seamlessly across different ecosystems. Our team remains dedicated to exploring ways to achieve this, leveraging technologies that allow users to have full control over their secret key material and the best user experience.

We recognize that decentralized identity has deep implications in the royalties and digital rights management landscape. As a result, we aim to devise robust mechanisms that enable the secure transfer and usage of NFTs across our ecosystem, taking into account the importance of royalties in these transactions. This brings back the power to creators and content owners. In contrast, we highlight that the current ongoing AI development represents a fascinating opportunity to explore how to further enhance experiences in the metaverse.

LAMINA1 is approaching the exploration of decentralized identity with enthusiasm and a commitment to excellence. We welcome new solutions that push boundaries and align with our vision.

[37] https://mitpress.mit.edu/9780262535588/twelve-tomorrows-2013/

Credits

Mario Yaksetig
LAMINA1

Will Carter
LAMINA1

Casey Halter
LAMINA1

Alaina Bryan
LAMINA1

Acknowledgements

Neal Stephenson
LAMINA1

Dele Atanda
metaMe

Metaverse Experience
Research Group (SCAD)

Disha Shah
Sneha Shetty
Kanika Trivedi
Cristina Cordova

Community Research
powered by BlockSurvey

Contact

Ecosystem Development
ecosystem@lamina1.com

Events
events@lamina1.com

Opportunities
jobs@lamina1.com

Anything Else
hello@lamina1.com

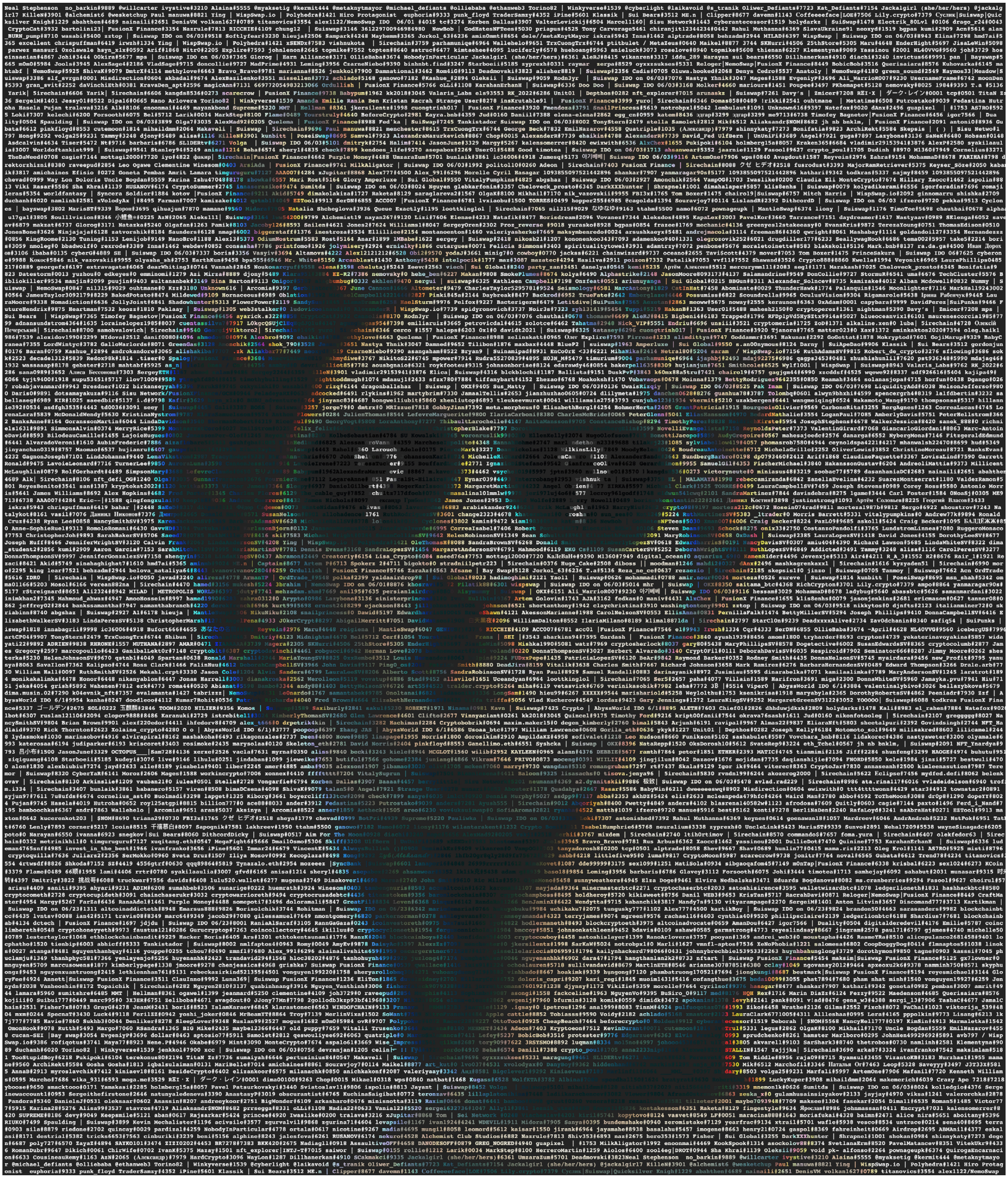
Get Involved

Join the Community:
discord.gg/LAMINA1

Visit the Website:
LAMINA1.com

Secret Code
ID3NT1TYLITEPAPER!!

+ Thank you to the LAMINA1 Discord Community for your thoughts and insight into metaverse identity for this litepaper. All community participants are credited below:



DISCLAIMER

This Litepaper and the LAMINA1 website are intended for general informational purposes only and do not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, or any offer to sell any product, item or asset (whether digital or otherwise). The information herein may not be exhaustive and does not imply any element of a contractual relationship. There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information. Where the Litepaper or the Website includes information that has been obtained from third party sources, the Translaminal team has not independently verified the accuracy or completion of such information. The Litepaper is a working document that is subject to changes as LAMINA1 is further developed and as it responds and evolves in light of new contributions and ideas, as well as potential changes in the regulatory environment that may govern Translaminal Inc or LAMINA1. You acknowledge that circumstances may change and that the Litepaper or the Website may become outdated as a result; and Translaminal is not under any obligation to update or correct this document in connection therewith. The information set out in the Litepaper and the Website is for community discussion only and is not legally binding. NOTHING HEREIN CONSTITUTES LEGAL, FINANCIAL, BUSINESS OR TAX ADVICE AND YOU SHOULD CONSULT YOUR OWN LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S) BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH.

Nothing in the Litepaper or the Website constitutes any offer to sell any L1 token (as defined herein) nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. Nothing contained in the Litepaper or the Website is or may be relied upon as a promise, representation or undertaking as to the future performance of LAMINA1.