METASOCIALITY - OWN YOUR IDENTITY ON THE BLOCKCHAIN

BIOMETRICALLY-MANAGED SELF-SOVEREIGN DIGITAL IDENTITY

PROTECTING YOU AND YOUR DIGITAL ASSETS

This document has been prepared for information purposes only and does not constitute an invitation, advice or solicitation of an offer to acquire MetaSociality products or tokens.

MetaSociality is a framework for creating and managing your identity
on blockchain networks, software services and DApps.

"Genius is making complex ideas simple"

- *Albert Einstein*

Contents

Credits

This whitepaper is prepared in collaboration with the community and partners of MetaSociality. All credit to the community and partners in driving the MetaSociality protocol forward. In true homage to a decentralized community, this is owned by all.

The Challenge of Digital Identity

The internet was built without an identity layer[5]. There is much literature which traces the evolution of identity over the history of the internet, resulting in the federated logins that we currently have with web2 today. For reasons which fall beyond the scope of this whitepaper, not much headway has been made to address a basic problem when interacting online:

- Is the person that I am interacting with, a real person?
- And if so, is that person who they say they are?

Recently, we have seen the emergence of various open standards on the blockchain. Two such open standards have finally laid the foundations for a unifying identity metasystem [5]:

- Ethereum Naming Service ("**ENS**"); and
- Sign In With Ethereum ("**SIWE**").

When combining these invaluable building blocks with biometrics and NFTs, a persistent and portable identity is created which resolves to a unique and real person, without compromising their privacy or data dignity

A second point of consideration is the current sentiment around data privacy and safety online. In 2021, MetaSociality conducted a survey across 4,000 key opinion leaders to better understand the current sentiment regarding sharing data online. The key finding from the MetaSociality Data Privacy Survey highlighted that only 9% of people feel safe, or very safe, in

sharing their personal data online. These findings are supported by other surveys conducted recently relating to cyber security risks. Please refer to the Annexure for more information.

It would appear opportune therefore, to create a digital safe space where there is a reliable way to establish who you are connecting with[5] and a mechanism to pierce the digital veil, as and when necessary, while preserving privacy and data dignity.

MetaSociality Protocol: Overview

MetaSociality introduces a unique use case for Non-fungible Tokens ("NFTs"), integrating the NFT with user identity to develop a biometrically-managed model of Self-Sovereign Identity ("**SSI**") on the Blockchain[2].

Powered by an BSC-20 token, MetaSociality gives control and ownership of digital identity back to the user. MetaSociality empowers people to own, verify, and maintain full control over the sharing and use of their identity and personal information through an NFT.

Design Principles

MetaSociality is designed to be:

User-centric:

- **Intuitive**: Interface is easy to navigate.
- **Convenient**: An easy way to link to a wallet
- **Frictionless**: Verify and attest identity within a few minutes.
- **Reusable**: Use a verification status surfacing the underlying data time and time again.
- **Extensible**: User decides what data is shared with a counterparty and for how long.

Decentralized:

- **Permissionless**: No centralized intermediary to moderate flow.
- **Verifiable**: Verify the identity of parties to a transaction on demand.
- **Compatible**: Forward compatible with emerging standards in ENS, SIWE, and BSC 721.
- **Proof of liveness**: Authenticate the liveness of a counterparty, eliminating bots and spoofers.
- **Interoperable**: Extend a secure identity to other chains while maintaining anonymity and control over personal data.

Secure:

- **Private**: Verify identity without exposing personal data.
- **Unique**: Resolve to a unique identity.
- **Data minimisation**: Data lives off chain, but utility provided on-chain.
- **Protected**: Utilizing the most developed data security protocols to protect data during the minting process.
- **Compliant**: Stringently applying international regulations and standards for data privacy and data control.

There exists a natural tension between user-centricity and decentralization. MetaSociality is focused on giving control of identity back to the user in a decentralized manner, without compromising their privacy or security.

Why MetaSociality?

The term, "MetaSocialitycity", describes the ability to adjust transparency to a certain stimulus. In sunglasses, exposure to sunlight reduces transparency. Through a smart contract, the project embraces a "MetaSociality" nature in that the user decides the level of transparency when engaging with other people and businesses. In due course, selective data sharing empowers the self -sovereign individual to manage and control their own data.

How MetaSociality Works

Using the MetaSociality decentralized application ("dApp"), an identity NFT is created in 5 steps:

- Reserve a MetaSociality identity as an ENS sub-domain [1] e.g. janedoe.metasociality.eth.

- Connect a wallet to the MetaSociality dApp.

- Verify the user's identity through a trusted identity provider that resolves to a government-backed identity and proof of liveness.

- Generate an avatar / PFP of identity using algorithmic art, which is generated with biometric data seeded from an image of the user's face.

- The identity NFT is then minted on the Blockchain.

With a MetaSociality identity NFT and assuming widespread adoption, a user is able to traverse the metaverse with autonomy over their digital identity[1].

Note:

At the discretion of the user, additional information can be shared onto the identity NFT, which will form part of the user's ENS text records. The user may therefore elect to develop the NFT to be compatible with libraries such as ethers.js or web3.js.

Technical Specifications

MetaSociality is powered by Ethereum standard tokens:

- BSC-721 identity NFT as a unique NFT representing a certain identity; and

- BSC-20 $MESO as a means of governance.

MetaSociality merges both existing and emerging standards into a unique identity solution:

- **ENS**: ENS is a distributed, open and extensible naming system that is evolving towards an open standard for multi-chain name and address resolutions, secured by Ethereum. It brings human readable names and metadata to web3[5], similar to the Domain Name System ("DNS") for internet addresses. ENS is an extensible system which enables integration with open protocols or web2 platforms like Twitter. MetaSociality builds upon ENS to provide programmatically verifiable identities for a multi-chain Blockchain future, which will in turn enable other developers to build upon the identity protocol and facilitate the portability of identity[4].

- **NFT**:By design, NFTs are unique, unmodifiable digital objects that can be owned and contain various data, including images, metadata or identification data. MetaSociality builds on BSC721, the leading standard for NFTs, and allows for integration in a dApp or trading on marketplaces such as LooksRare, OpenSea or Rarible. Using the chain agnostic addressing scheme for NFTs (CAIP-19), MetaSociality identities can be referenced in a standardized format.

- **SIWE**: SIWE enables users to take control of their digital identity by using an Ethereum account and an ENS profile. This is in direct contrast to a centralized or traditional intermediary which controls the profile and data of the user. SIWE is a collective effort to standardize verification in a decentralized manner that enables the user to take full control and ownership of their data and identity.

By combining these primitives into a single solution, users are provided with an additional level of security and convenience[2].

**Figure 1: MetaSociality merges ENS, SIWE and NFT**

Building Blocks of the Beta product

MetaSociality comprises:

- **dApp**: An intuitive front-end interface for users to connect their wallet and mint their MetaSociality NFTs.

- **Wallet integration**: Connection to major Ethereum-based wallet providers, thereby providing users with full flexibility and autonomy when connecting a wallet to the dApp[6].

- **Integration with ENS**: MetaSociality builds upon the success of ENS, the most widely integrated Blockchain naming standard, utilizing the system as the foundation for MetaSociality's SSI solution[6].

- **NFT generative art**: Each MetaSociality NFT holder will be provided with a unique digital representation of their identity using algorithmic art, which is created during the NFT minting process. To maximize decentralization and user control, the NFT artwork is stored on IPFS[6].

- **Software developer kit ("SDK")**: SDK for integrating MetaSociality identity validation, renewal and selective data sharing into other decentralized applications.

Figure 2: Building blocks of MetaSociality
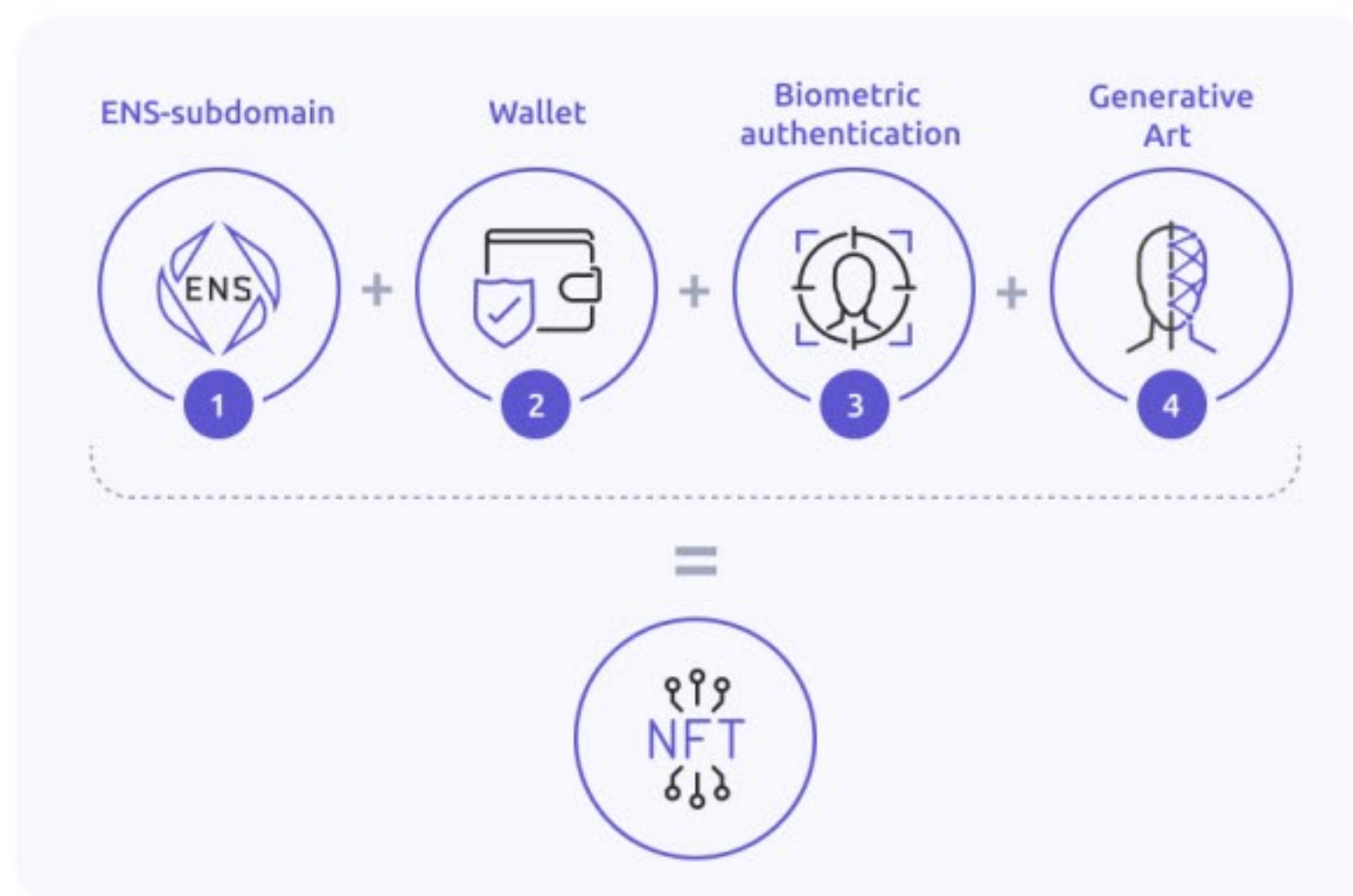
Protocol Revenue

MetaSociality will generate an income in the following ways:

- **Mint Fee**: To mint an identity NFT and create the visual art identity, users pay a once-off purchase fee.

- **Extension Fee**: MetaSociality identities are valid for a fixed period and will need to be refreshed to ensure that the biometric verification and KYC process retain validity. The identity NFT will be extended annually by paying the extension fee (similar to ENS).

- **Transaction Fee**: Partnering protocols or third parties that integrate with, or leverage, MetaSociality identities may pay a transaction fee per secure identity re-verification process.

Partner Ecosystem

MetaSociality has established and continues to build deep relationships with strategic partners. Our partnerships span across the identity, wallet, NFT and DeFi focus areas.

Figure 3: Overview of partnerships
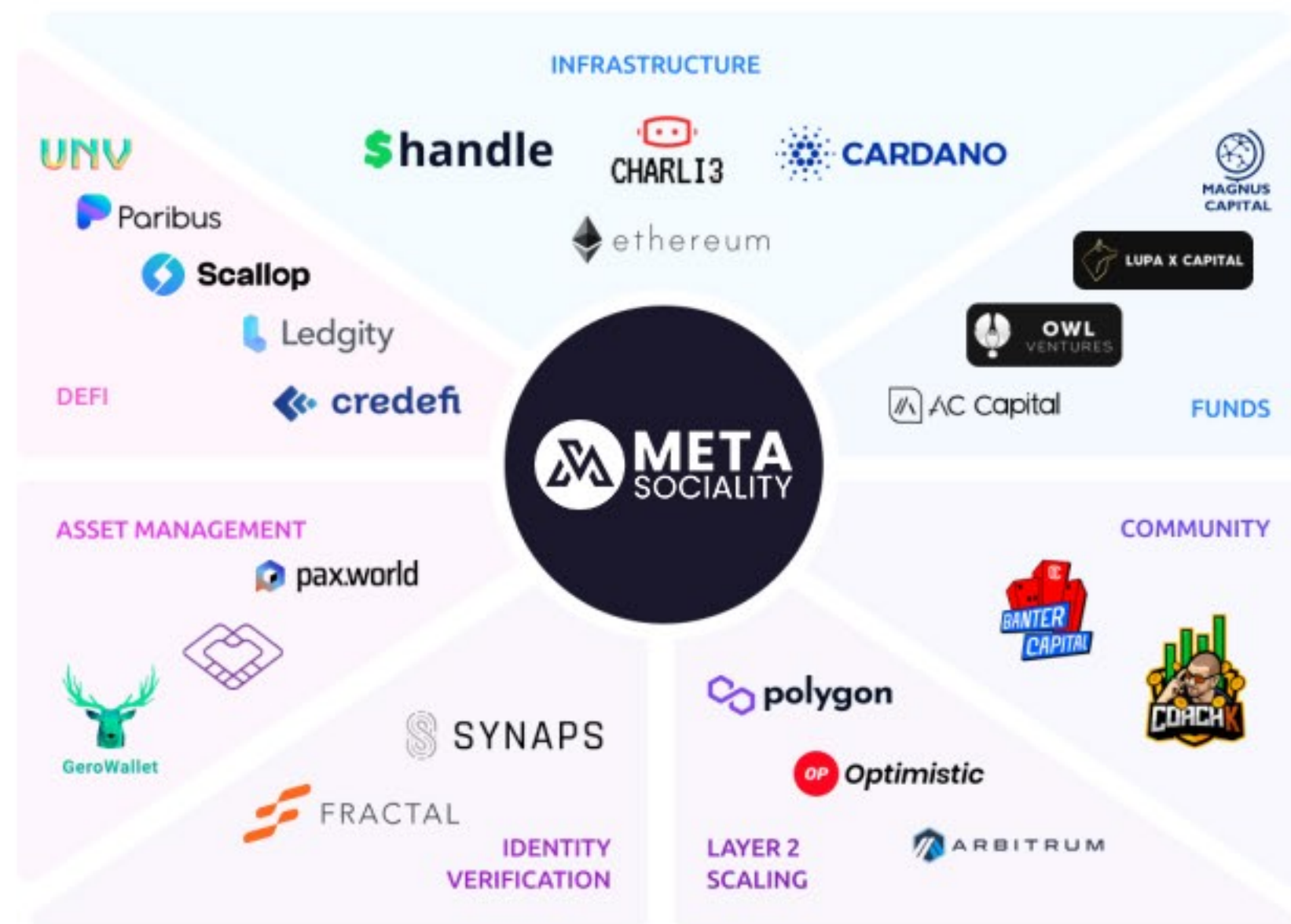
Use Cases

MetaSociality's use cases cover the full spectrum of digital transacting and will impact various areas of web3:

NFT-holder / individual user

- **Authentication**: authenticate and attest the identity on a web2 and web3 platform, including but not limited to:

  - Authenticate identity when entering an online retail site.
  - Authenticate entrance into online / metaverse events.
  - Transact on DeFi platforms by verifying ownership of assets.
  - Authenticate identity and player status in GameFi.
  - Authenticate achievement levels in gaming.
  - Verify professional qualifications and accreditations.

- **Ownership**: authenticate and verify ownership of for example Twitter handles, digital art and NFTs.

- **Social media authentication**:control, maintain and verify social media status online, minimizing identity fraud and other security related risks.

Platforms / institutions

- **Allowlisting**: simplify, streamline and expedite the allowlisting and on-boarding process of verified and trusted web3 market participants.

- **DAO reputation**: verify and attest the authenticity and trustworthiness of existing and new members of a community.

- **Membership**: authenticate and attest membership to NFT-gated communities.

- **Regulatory AML / KYC / identity verification**: authenticate, attest and expedite identity verification and onboarding process of new clients as may be required under relevant regulatory requirements.

Benefits

The benefits of an identity NFT are detailed hereunder, but may vary on a case by case basis.

NFT-holder / individual user

Privacy-preserving data exchange [3][5]:

- Minimizes the friction of KYC / AML compliance.
- Reduces the time required to interact
- Enhances the user experience.

By enabling a user to consolidate their data into a holistic picture, the user is empowered with identity autonomy, data dignity[4] and a consistent user experience while enabling a separation of both public and private identity showcasing[5].

Platforms / institutions

By minimizing the data exchanged to attest identity and by biometrically-enabling the NFT[5]:

- Minimize security risk.
- Reduce the time required to both onboard new users and verify existing users.
- Enhance the user experience.

By de-duplicating resources for identity verification, the cost of doing business is reduced, freeing up resources to refocus on core business functions.

Tokenomics

$MESO will be distributed in MetaSociality's upcoming Initial Decentralized Exchange Offering ("IDO").

META SOCIALITY

TOKENOMICS OVERVIEW

TOKEN TICKER	MESO

List Price	Initial Market Cap
$0.001	$742,500

TOKEN ALLOCATION	INITIAL UNLOCK	VESTING SCHEDULE
Advisors	10%	10% after 60 days, then linearly over 12 months
Seed	10%	10% after 60 days, then linearly over 12 months
Private Sale	10%	10% after 45 days, then linearly over 12 months
Public IDO + Airdrop winners	50%	50% after 14 days; 25% one month later; 25% one month thereafter.
Community incentive	0%	Linearly over 24 months
Development	25%	Linearly over 6 months
Marketing and Partnerships	10%	10% after 21 days, then linearly over 12 months
Liquidity pool	100%	100% locked for 12 months
Team	0%	6 Month cliff and then linearly over 24 months

TOKENOMICS

- **27.5%** - Community incentive
- **22.5%** - Private sale & IDO
- **18.0%** - Team
- **12.5%** - Development
- **4.0%** - Liquidity pool
- **3.5%** - Advisory
- **12.0%** - Marketing & partnerships

Token supply: **45 Million**

Future Enhancements and Roadmap

Our top five development plans for 2022 will expand on the beta product release, extending the utility provided to MetaSociality NFT holders:

Figure 4: Top five priorities for 2022

- **Layer 2 scaling**: While embracing a multi-chain future, secure tamper-proof identities deserve the security of the most secure smart contract platform and Ethereum. Given the popularity of Ethereum and the total value it secures, Ethereum Layer 1 transaction fees are high. A Layer 2 solution combines the security of Ethereum at a fraction of the cost, thereby making MetaSociality more accessible. MetaSociality can be used on any other Layer 1 chain (Solana, Polkadot, Cardano), sidechains (Polygon) or other Ethereum Layer 2 platforms (Arbitrum and Optimism). For these integrations, MetaSociality follows the roadmap of ENS including standardization efforts on off-chain data retrieval and validation (EIP-3668).

- **Selective data sharing**: In keeping with the functionality and extensibility of ENS in the beta release, MetaSociality will leverage the functionality of the SIWE project. This will facilitate easy and convenient user-centric access to multiple Web-based services and enable users to selectively share bespoke, customized components of their identity without compromising their privacy[3-5]. Selective data sharing empowers the user to self-select the public and private attributes of their identity, with the public attributes being easily searchable via their wallet , thereby creating a readable and searchable history of transactions[1]. In this way, the public attributes of digital identity can be showcased in bespoke contexts to select audiences [1].

With this functionality, MetaSociality hopes to unlock untapped opportunity for MetaSociality NFT holders, including:

- **DeFi**: facilitating a simple and cost-effective allowlisting of verified and trusted DeFi market participants.

- **Crypto Exchange login**: reusing identity verification for frictionless sign-up for new services and by enabling decentralized crypto exchanges that offer leveraged trading to non-US residents to geographically limit their services.

- **Cross-chain reputation for DAOs**: providing DAO participants with a mechanism to leverage their reputation across multiple platforms.

- **Secure data exchange**: securely exchanging business cards or personal info without relying on centralized parties.

- **Decentralized payment solutions**: facilitating frictionless web3 centric e-commerce and payment services.

- **Age validation**: verifying the age of participants in regulated activities such as when applying for a driver's license or voting in elections.

- **Secure digital assets transactions**: securing transfers of digital assets between individuals without intermediaries or commissions.

- **Decentralizing identity providers**: MetaSociality intends to onboard additional identity providers, offering greater optionality and flexibility for users when initially verifying their identity in the NFT minting process. MetaSociality will propose specification and onboarding processes for identity solutions which will be selected and prioritized in the MetaSociality DAO.

- **Ecosystem partnerships**: MetaSociality intends to integrate with multiple partners, which partnerships will be announced as and when possible.

- **MetaSociality DAO**: The MetaSociality DAO will be established as soon as possible in 2022 to guide collective decision-making, permissionless ownership, transparent and public information-sharing and open-source IP. In the true spirit of decentralization, MetaSociality will empower users and tokenholders with full autonomy, voting rights and influence on the roadmap.

The Evolution of PhotoSapiens

Given the inherent challenges associated with digital identity, the evolution from HomoSapien to PhotoSapien is an endeavor to empower the community to collectively reclaim control and ownership of digital identity. As a PhotoSapien, a unique digital identity on a NFT can be used across the Blockchain, without having to expose personally identifiable information. There are two collections of PhotoSapiens, namely the Genesis and Soulbound Editions.

Genesis Edition

The Genesis Edition is the first collection of PhotoSapien NFTs that will define and direct the journey of MetaSociality. This first mint creates a founding community, decentralized autonomous organization ("**DAO**") and aggregates the choice of generative art. When the biometric PhotoSapien NFT ("**Soulbound Edition**") deploys, the design will be guided by the DAO. This collection of 10,000 global citizens opens up and unlocks the future of a secured digital identity in a web3 world.for web3.

Soulbound Edition

The Soulbound[2] Collection of the PhotoSapiens, is a biometrically-enabled NFT, which can be used to authenticate, verify, and attest identity on the Blockchain. By virtue of the fact that it is generated by the user's unique biometrics, and it is therefore non-transferable. As part of the Soulbound Collection, the user will be able to create their own ENS sub-domain and will be directed to an approved identity verification partner for identity verification purposes.

The table hereunder illustrates how the Genesis Collection differs from the Soulbound Collection:

	Genesis	Soulbound
Ability to transfer your NFT	✔	
MetaSociality DAO participation	✔	
First in line for future perks and airdrops	✔	
Generative art from a picture of the user	✔	✔
Create an ENS sub-domain		✔
Connect a wallet	✔	✔
Verify an identity		✔
Generate an avatar	✔	✔
Mint a NFT	✔	✔

Parting Words

MetaSociality provides an identity on-ramp from the physical to the digital world in a decentralized manner, equipping users with autonomy while preserving their right to data privacy and security. We welcome the opportunity to work with like-minded creators in moving digital identity forward.

Should you have any comments or suggestions on this workpaper, please share them with us.

Website | Twitter | Telegram | Medium | LinkedIn | Discord | Facebook

Annexure 1: Insights from cyber security risk surveys

The key findings from the MetaSociality Data Trust Survey are:

- **Concern**: 89% of people are either concerned or very concerned that sensitive, personal information may be hacked or compromised in the future.

- **Safety**: Only 9% of people feel safe or very safe in sharing their personal data online.

- **Confidence**: In the event of a data breach or the like, only 22% of people are confident or very confident that they would know who to contact, how to recover their data and / or how to minimize the effects of the data breach on their personal, digital safety.

- **Biometric authentication**: 79% of participants would use a biometrically-enabled tool to secure their identity online.

Figure 5: Key findings of the MetaSociality Trust Survey

89% Concerned or very concerned that sensitive personal information may be hacked going forward

22% Confident or very confident of being able to minimise data lost in a breach

9% Feel safe or totally safe sharing personal data online

79% Likely or vey likely to use a biometrically-enabled tool to secure data online

The findings from the MetaSociality Data Privacy Survey are in keeping with the findings from other online privacy and cybersecurity surveys:

- Security breaches in 2020 alone increased by 17%, impacting 280 million people in the US. (Data Breach Analysis of the ITRC, 2021 Q3)

- 75% of targeted cyberattacks start with an email. (Round Robin, 2020)

- During Covid, the FBI received c.2,000 internet crime complaints per day. (FBI, 2020)

- 58% of adults are worried about being a victim of cybercrime. (Norton, 2021)

- 62% of adults admit difficulty in assessing credibility of data online. (Norton, 2021)

- 63% of consumers are very worried their identity will be stolen. (Norton, 2021)

- 78% of consumers are concerned about data privacy. (Norton, 2021)

- 83% of consumers want to protect their privacy. (Norton, 2021)

- 91% of people know the risks of reusing passwords across their online accounts, but 66% do it anyway. (LastPass, 2020)

Figure 6: Statistics from recent cybersecurity surveys
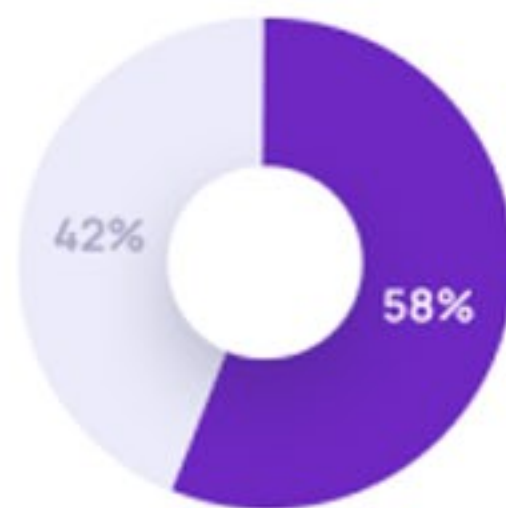
3 in 4 cyberattacks start with email

Source: Round Robin (2020)

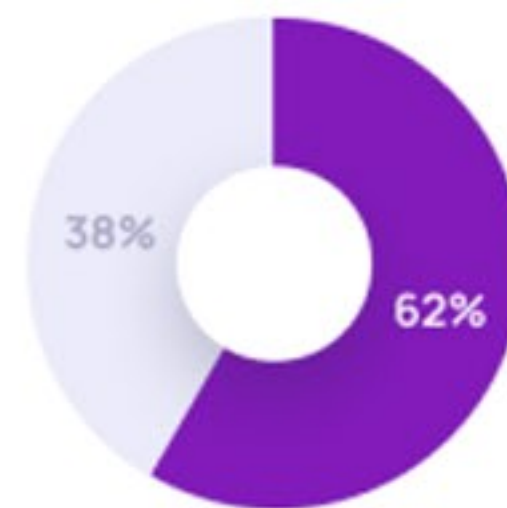**3** in 5 consumers are very worried their identity will be stolen

Source: Norton (2021)

58% of adults are worried about being a victim of cybercrime

42%
58%

Source: Norton (2021)

62% Of adults admit it is difficult to determine if the information they see online is from a credible source

38%
62%

Source: Norton (2021)

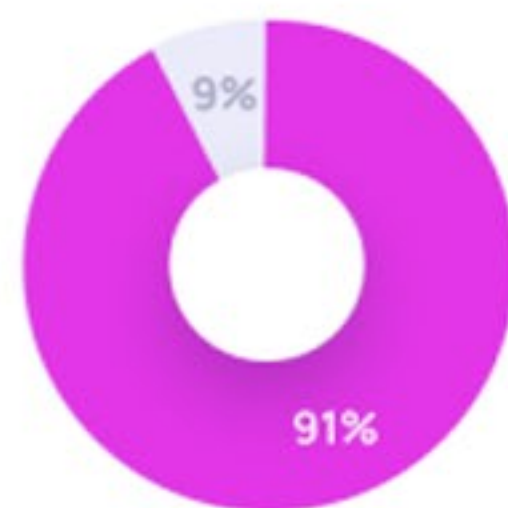**4** In 5 consumers are concerned about data privacy

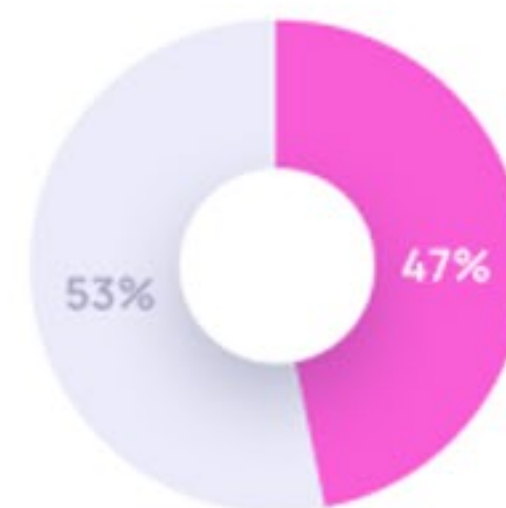Source: Norton (2021)

2 in 3 people reuse passwords

Source: LastPass (2020)

91% Of people know the risks of reusing passwords across their online accounts

9%
91%

Source: LastPass (2020)

47% Don't know how to protect their identity effectively

53%
47%

Source: Norton (2021)

In 2021, there were a number of high profile cybersecurity attacks that warrant mention:

- In June, Volkswagen/Audi disclosed a data breach impacting over 3.3 million customers and some prospective customers. The data breach was believed to take place at an associated vendor and exposed data collected between August 2019 and May 2021.

- In August, T-Mobile announced a data breach of the names, addresses, Social Security numbers, driver's licenses, IMEI and IMSI numbers and ID information of c.50 million customers.

- In September, AP-HP, Paris' public hospital system, announced a security breach of the personally identifiable information of individuals who took COVID-19 tests in 2020.

- In October, Coinbase announced that the accounts of 6,000 US-based customers had been compromised and the customer funds had been removed from the platform.

- In November, Robinhood experienced a data breach of email addresses, names, phone numbers affecting 5 million users.

In summary, there is clearly a need for more effective mechanisms to help safeguard user data and identity online.