

LUISS GUIDO CARLI – MSC DATA SCIENCE AND MANAGEMENT

DATA-DRIVEN INNOVATION – Spring Semester 2022

MEDUSA

TEAM 2

Instructor:

Prof. Ceci Federica

Prof. Niloofar Kazemargi

Prof. Tiziano Volpentesta

Students:

Amadori Marco

Gioia Matteo

Imperatore Claudia

Leonardi Giorgia

Sciammarella Carlamaria

Striano Vincenzo Junior

MEDUSA

A SOLUTION TO ENSURE METAVERSE PERSONAL IDENTITY



Be yourself; everyone else is already taken

Oscar Wilde

Mint your identity as an NFT and use it to show the world exactly who you are.

Stored on the blockchain, it is your digital passport to limitless opportunity.

The Problem

Since its development to the public since the mid-90s, Internet has been characterized as an official democratic network without effective regulation and identification layer: anyone can do anything she wants with a certain degree of anonymity, indeed no personal identification is required to join it.

To avoid anarchy, some online services ask us to prove our identity requiring sensitive, personal information, which are stored in their databases. Once their own data are in cloud, people lose the control over them, and their property moves to the service providers, creating a monopolistic market of data, sometimes with malicious intents. Moreover, some data-driven companies gain profits from selling those data to advertising services i.e., Facebook, with no economic benefits for users.

It's notorious the case of Cambridge Analytica, which acquired personal data from Facebook's users to change the fate of the presidential elections, creating fake advertisements to change people's mind about who to vote.

We foresee that access to the metaverses and economic transactions within them will be allowed thanks to the blockchain technology and cryptocurrencies, which grant anonymity by definition.

Medusa has the potential to efficiently address the issue of identity theft, control over personal data shared, users' anonymity and a safer meta-environment.

Understanding Technology

Medusa develops a biometrically managed concept of Self-Sovereign Identification (SSI) on the Blockchain by merging Non-fungible Tokens (NFTs) with user identity.

Medusa, which is powered by an ERC-20 token, gives users back control and ownership of their digital identities. Through an NFT, Medusa enables users to own, verify, and keep complete control over the sharing and use of their identity and personal data. Our idea is simple: that users should be at the center of their identity management process: the Self-Sovereign Identity.

Data are stored on a token and then when the owner wants to, they can approve a third party to collect specific data. One can do this by confirming a notification on said device.

This idea ranks among the NFTs of nature: "Utilities". It promises to give people the freedom to build genuine societies in the metaverse but in the Web 3.0 in general

Our NFT will assigns top priority to its users' personal data, allowing them to take control of their data and identity. The blockchain that we have decided to use for the realization of our project is Ethereum. Ethereum has been created to be an entire integrated ecosystem and become a blockchain capable of running decentralized applications. this open environment is perfect for launching new projects such as Medusa.

The ERC 20 is the standard provided by the Ethereum blockchain that we have chosen to use. ERC-20 tokens are smart contracts that provide great flexibility and functionality, such as the expire function, which means that after a certain time the token will automatically vanish. This functionality helps us to always keep the biometric recognition valid. The rules of this protocol must be followed for the token to interact with other tokens within the network. We choose this token standard because the goal and need for ERC-20 tokens is the same of our project, to design a standard, to

create interoperability and compatibility between tokens and to foster improvements in the Ethereum ecosystem.

The main feature that convinced us to choose this standard is that each token has a name or an identifier and an associated symbol. Through these two values, it is possible to identify and differentiate the tokens from each other within the Ethereum blockchain.

Governance Category	What is it	How is implemented at Medusa
Proof of personhood and individuality	Proof that a user is an individual natural person who joined the system one time.	Thanks to a government-backed identity, that provide proof of liveness, we can allow to join the system only once.
Proof of participation	Users who participate in the network can have a say in governance proceedings.	Community users can report illicit behaviors.
Time delays	A delay in time where tokens cannot be transferred.	The token cannot be transferred for a period that can ensure non-transferability.
Individual reward	Governance rights to users.	Users that will contribute to the genuine growth of the network will gain a rank reputation that will enable to have governance rights and participate the decision process of rules and guidelines.
Punishment	Temporary or permanent disabling of the token	Users who break the rules will receive punishment. In severe cases, the token will be petrified forever.

Why Medusa?

The name of the project was not chosen by chance: we wanted to recall the story of Medusa, one of the three Gorgons. From the ancient Greek, Médousa, which means "protector" and "guardian", and from médō, "to protect". We have chosen this mythological figure to represent our project as we want to emphasize what are the main objectives of the project. Identity protection and behavior surveillance in the Web 3.0 environment.

Thanks to the Medusa project, anyone who performs improper behavior on the Web can be excluded from the system thanks to the elimination or petrification (like Medusa, in Greek mythology) of the NFT which acts as an access key.

Minting Process

Using the Medusa decentralized application, an identity NFT can be minted using a digital signature-like process, where the public key is the hash of personal IDs (namely *ID HASH*) and the private key is the user's biometric trace (*BIO HASH*).

The steps to create a user's meta-digital identity, stored in the *NFT HASH*:

1. Medusa enters into a partnership agreement with a trusted digital identity verifier such as SPID. The SPID platform will provide the hashed version of the user's personal information to Medusa. Medusa will only retain the hashed version and not the unencrypted (ex. ABC) version.
2. The user will provide a unique biometric trace i.e., fingerprint, which will generate a local hash, of which no other actor will be informed (123).
3. Medusa will generate a hash formed by combining the previous two hashes. This hash will be the identification code of the NFT and therefore of the digital identity (123ABC).
4. The NFT will be minted and uploaded to a wallet supporting the ERC-20 standard.
5. For each meta-platform, the user will be able to decide which of the data contained in SPID she wants to make available in plain text. It is possible, in fact, that in a meta-event the user will be required to be of legal age, verifiable only with a real identity document.

In the login process, after minting:

1. The HASH ID is held locally by the Medusa app for 30 days. A new login (ABC) will be required every 30 days.
2. The user is prompted to log in to their wallet: Medusa will detect the presence of a NFT HASH: 123ABC.
3. The user will also be required to provide their biometric track, the hash of which is 123.
4. Medusa creates the hash given by the combination of ID HASH and BIO HASH: if there is a concordance between this and the NFT HASH the identity will be verified.

In case of an infraction reported by other users, Medusa will disable the NFT HASH of the "guilty" user: Medusa will not know his identity, but the individual will not have the possibility to join the metaverse again: each NFT HASH, being given by the combination of factors attributable to a single individual, will correspond to one and only one person.

It is relevant to note that if multiple metaverses adopted the Medusa standard, sanctions would extend for each of the meta-environments, making the digital world globally more secure.

SPID	MEDUSA	USER	METaverse
ID	ID HASH	ID & ID HASH	NFT HASH
		BIO & BIO HASH	
		NFT HASH	

sovereignty distribution of data

Identifying Market

Application sector and marketplace

Our project falls into the public sector, more in the specific in the Digital Identity application case, with a strong reference to Web 3.0 and the Metaverse. For this reason, no specific marketplace has been identified in order to sell our service, considering that the business model is based neither on selling the NFT's or extracting royalties from them.

According to Gartner, 25 percent of people in 2026 will spend at least one hour on the Metaverse. According to the firm, most of everyday activities might also shift on the metaverse: attending classes, courses, business meeting, and conferences. From the business side, the firm claims "30% of the organizations in the world will have products and services ready for metaverse" (Gartner 2022). These trends suggest an increasing popularity of the metaverse and a use of it as a two-sided platform. While the overall increase of the metaverse's market size "[...] may reach \$783.3 billion by 2024 vs. \$478.7 billion in 2020 representing a compound annual growth rate of 13.1%." (Bloomberg, Newzoo, IDC, PWC, Two Circles, Statista). Therefore, we might expect a parallel increasing demand for privacy and security as more business shifts to the metaverse and as more users start approaching it and its services. This is particularly true when we look at the fact that users are already concerned about data privacy and protection of their online identity (SpyCloud 2021, FRA 2020). These concerns might only increase in the emergent, and so far, unregulated, digital worlds of the metaverses.

Overall, we might state that there is indeed a customer base for our business idea. This is particularly true when one looks at other similar businesses and initiatives that are arising, such as Identity Coins (cryptocurrencies, coins and token that facilitate identity verification: <https://cryptoslate.com/cryptos/identity/>) .

Business model

Business Model Canvas				
Key Partners	Key Activities	Value Propositions	Customer Relationships	Customer Segments
Companies that invest on it and decentralized platforms. <ul style="list-style-type: none">• Wallet providers• Meta-Companies• Spid	Develop a biometrically managed concept of Self-Sovereign Identification ("SSI") on the Blockchain by merging Non-fungible Tokens ("NFTs") with user identity. Medusa, gives users back control and ownership of their digital identities. Data are stored on a token and then when the owner wants to, they can approve a third party to collect specific data. One can do this by confirming a notification on said device. Key Resources Software, databases, people, financial resources.	To efficiently address the issue of identity theft while also providing users with a more secure private environment. Through an NFT, Medusa enables users to own, verify, and keep complete control over the sharing and use of their identity and personal data. Thus, users are at the center of their identity management process.	Medusa allow to report unethical behaviours, giving the power to protect the environment. Medusa provides virtual forum where users can share their opinions and suggestions about the offered service, useful in order to make feel customers as satisfied as possible. Channels Website, App and other platforms that allow cluster clients in communities based on their interests.	Companies and more generally all users that are concerned about data privacy and protection of their online identity
			Revenue Streams <ul style="list-style-type: none">• <u>Mint Fee</u>: Users pay a once-off purchase fee, <u>in order to</u> mint an identity NFT and create the visual art identity• <u>Extension Fee</u>: identities provided by Medusa 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.• <u>Transaction Fee</u>: Partnering protocols or third parties that integrate with, or leverage, Medusa identities may pay a transaction fee per secure identity re-verification process	

Value proposition

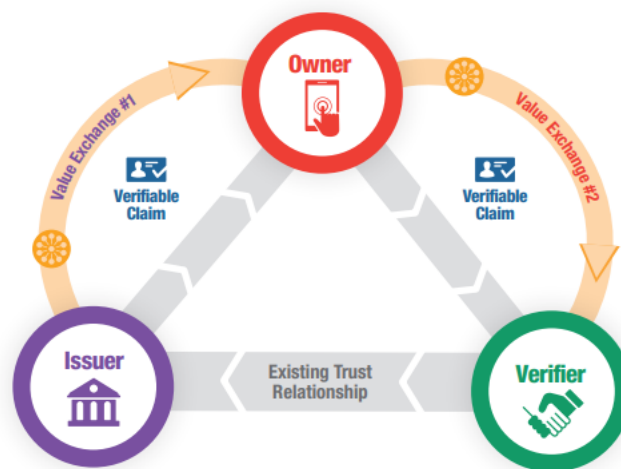
Medusa can enable the end-user to consolidate their data into a holistic picture, the user is empowered with identity autonomy, data dignity, and a consistent user experience while enabling separation of both public and private identity showcasing. The identity owner can share what the requesting party needs to know, but nothing more. For instance, a user could easily prove they reside in a certain country. Or a person might be able to prove they are over 18” without revealing more this information. These identity attributes are boundless and could also include something such as “professional investor”. The identity owner will be able to choose which piece of information to pass along to any relying party. The type of identity claims that can be attested is almost infinite.

Tokenomics

The NFT can be disabled temporarily or, in the most serious cases, permanently as a result of harmful behaviors such as bullying or racism, on the platforms that adopt the Medusa project.

Medusa will generate an income in the following ways:

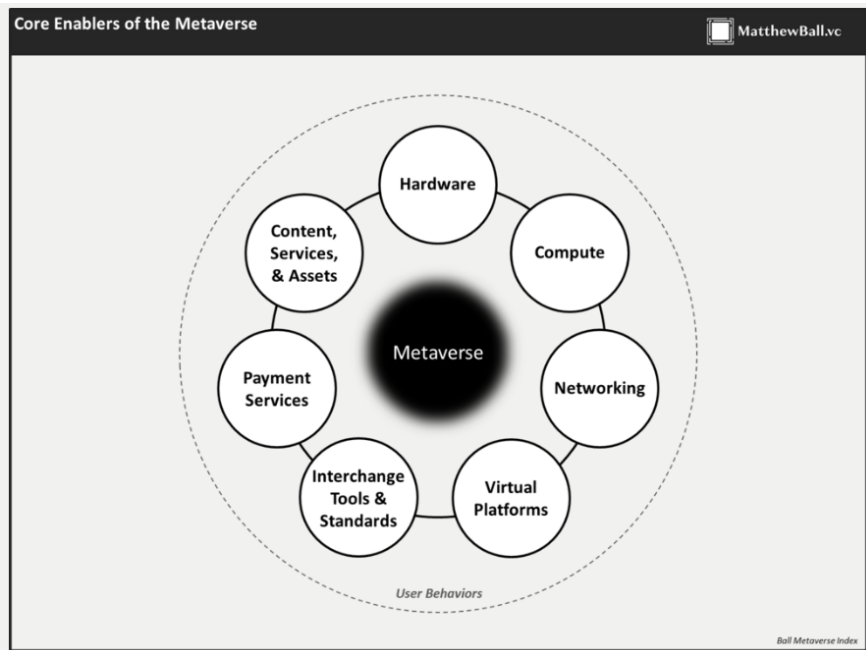
- **Mint Fee:** To mint an identity NFT and create the visual art identity, users pay a once-off purchase fee.
- **Extension Fee:** Medusa identities are valid for a fixed period and will need to be refreshed to ensure that the biometric verification and KYC process retain validity. The identity NFT will be extended annually by paying the extension fee.
- **Transaction Fee:** Partnering protocols or third parties that integrate with, or leverage, Medusa identities may pay a transaction fee per secure identity re-verification process.



Ecosystem

Medusa includes 5 primary parties 1) the identity owners, 2) relying parties and 3) verifiers (or original claims issuers), wallet and blockchain technology provider.

According to Ball M., in the “Framework for the Metaverse”, the ecosystem of metaverses is composed around eight core categories. Our project would be a candidate for the Metaverse Content, Services, and Assets category. That is, the design/creation, sale, resale, storage, secure protection, and financial management of digital assets, such as virtual goods and currencies, linked to users' data and identity.



Our Pie Model

Risk: Red (high), Yellow (medium), Green (low)



Plan to create communities











The implications of enabling a stable and secure digital identity in virtual worlds are enormous. Enabling a solid and secure digital identity in virtual worlds has significant ramifications. It claims to provide people the flexibility to create actual metaverse societies, complete with social, economic, and even political interaction based on the same recognized rules that we enjoy in real life.

Medusa proposes a self-sovereign identity system as the best model for our evolving global society. Allowing people to freely migrate – as the same individual – between distinct virtual worlds with drastically diverse characteristics, cultures, and game rules is one of the most crucial implications of supporting identity in the metaverse.

As popular social networking sites strive to impose their own closed-loop worlds on the metaverse, community growth will become increasingly important (controlling data, behaviors and membership). Instead, NFT-enabled user-created metaverses could help usher in a new era of openness and transparency in cyberspace.

Competitors:

Our competitors are identified as those who seek to offer identification tokens that implement the SSI concept. The image below lists the current top 10 companies providing Identity Coins according to the CryptoSlate platform.

#		Name
1		Syscoin #151 SYS
2		Civic #261 CVC
3		Metadium #323 META
4		KILT Protocol #505 KILT
5		SelfKey #591 KEY
6		Metaverse ETP #1047 ETP
7		BaaSid #1106 BAAS
8		Project Pai #1202 PAI
9		Vetri #1223 VLD
10		Idena #1249 IDNA

Prototype

We built a fully working prototype, either from the back-end side and the front-end using Proto.io and Python 3.*

<https://share.proto.io/U8HNNR/>

https://github.com/vincenzojrs/Personal/blob/main/medusa_nftcreator.ipynb

12:17



powered by 



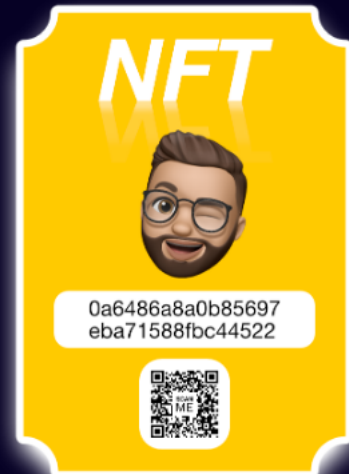
MEDUSA

Be yourself

13:10




Wonderful!



Your personal identity has been
correctly encrypted and uploaded to
your wallet.

Choose you public information

powered by 

Bibliography

Alison Grace Johansen, "Biometrics and biometric data: What is it and is it secure?",

<https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html>

B. Armstrong, A. Reeve, "How Coinbase thinks about the Metaverse", December 2021

<https://blog.coinbase.com/how-coinbase-thinks-about-the-metaverse-16d8070f4841>

Matthew Ball, "Framework for the Metaverse", 2021

<https://www.matthewball.vc/all/forwardtothemetaverseprimer>

FRA(European Union Agency for Fundamental Rights, 2021

<https://fra.europa.eu/en/news/2020/how-concerned-are-europeans-about-their-personal-data-online>

Gartner press release 2022 : <https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026>

Sovrin, "Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust", January 2018. <https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf>

SpyCloud, 'Annual Credential Exposure Report, 2021

https://f.hubspotusercontent20.net/hubfs/3791228/PDFs/2021-Credential-Exposure-Report_SpyCloud.pdf