# IDENTITY.ETH WHITEPAPER

*This document is a paper to highlight the vision and the goals of the identity system that is to be created. The original document will be created by Shane in 2021 and be updated periodically as the project evolves and changes.*

*Primary repository : https://github.com/Mahelaa/Identity*

## Introduction

Web3, DAO a word that has been signified as the future of the internet and technology. Bitcoin, Ethereum and Solana have laid the foundations for building different aspects of a decentralized web. Over the past few years the world has seen a technological revolution in the use of blockchain technology and transitioning the web2 services onto the blockchain to give users more control of their data. This move has created a stronger security and privacy benefit for the users involved. The main use case of using cryptocurrency as an alternative to finance. [Non fungible Tokens](https://ethereum.org/en/nft/)(NFT’s) have seen a huge boom in popularity over the last year, evolving out of this concept have created a large collectible market and have streamlined digital ownership. The concept of one signature can be used by a holder to verify your item has many potential use cases outside just of digital assets.

## Identity.ETH

The blockchain and web3 is the future. As we see the technical revolution and shift into a decentralized internet.

Identity.eth is a new generation DAO that focuses on creating a digital identity for every user on the internet. The fundamental idea is to create a connection between every source application to create a single authentication and login system for any DAPP/Website based on the blockchain. Users will connect their Ethereum wallet to serve as the gateway to the blockchain. The initial concept will allow users to link every platform necessary to your eth wallet. This will serve as your identity, allowing you to login to any and all supported platforms/DAPPS with a single auth token. Let’s take a deeper dive into how this works

Starting us off with a simple example. Let’s see how a user named John wants to login to a Web3 platform

John goes into the frontend enters his username and password, the browser makes an API call, which checks the central datastore for a account/password match and then returns a token which gives John access to the platform. The tokens contain the restriction of a session limit and logs in timestamps and may also contain location data among many other things.

Another look at the same process through the ID.eth system. John has the need to login to a user account which has the same requirements. John has minted his 64ID onto his Ethereum wallet. This is not limited to one website. A user is able to mint as many platforms that are supported. This is permanently stored within his wallet. With the popularity of applications such as metamask a user simply has to use their wallet to login to this platform and the platform will check the wallet for the matching user data which is within the user’s wallet. This would return an auth token. This token contains data that the user has a valid account on this platform and is authorized to login to this system and nothing else. We apply this same principle to as many web3 platforms as possible and over time a user only needs to carry one piece of technology. Their crypto wallet. There will be no need to carry around usernames and passwords. And 2FA will ensure the maximum security for the future of authentication.

## Technology

Working on a project like this we aim to bridge the gap with traditional websites and the blockchain. Connecting your account from existing websites such as Twitch, Google with the id platform would allow your unique ID to be minted in the process. In the current web standard usernames are associated with a unique ID, the process of transferring your domain onto the platform will solidify your access to it on chain, giving full ownership to the user that holds it in their wallet. This will allow users to claim ownership of their technology and their data. The identity.eth platform will allow users to thereby login to any new web platform by using our system. ID.ETH will act as a central point of authentication. The user’s eth wallet contains proof of ownership, the technology would generate a token similar to JWT to signal that the current user that is trying to login is correct and therefore will give access to services. By linking and using every website to one central service this allows ease of access and acts as a gateway.

The core concept on ID.ETH and the blockchain by extension is to give control back to the users. Any website requiring access will not have any data of the user and therefore will limit tracking.

The project will be open sourced and contain no centralized data store. This also allows virtually anyone to be able to clone the project and improve on it. By relying on community contribution and governance the project aims to give control to the people.

### How does this limit tracking?

User logins to a website create one of the most commonly used ways to track user activity in the form of cookies and sessions. ID.Eths platform will give the platform a token with a set timeout this token will be unique and cannot be duplicated. The reason being to obfuscate user data. Token style logins give access to the user data on a platform

## Identity Transaction protocol

The core concept of the ID platform is to simplify the authentication system. Each transaction that happens with the above protocols will be used to complete a set of steps that define a users data onto a wallet

* User logins to the ID.ETH portal/ any cloned portal / website that uses the auth protocols
* User data is verified with the standard authentication system which logs them into the platform.
* API call is retrieved to get the unique userID/account name. This data on success will start a claim process, user will be required to pay a one-time gas fee to mint.

The user is able to mint the userID as a permanent fixture thereby linking it to their ETH wallet.

* User Logs into a wEb3 platform that requires sign in/ and all they have to use is a platform such as metamask, wallet etc
* ID will search the user wallet for metadata and on success generated a random 256 encrypted token. Session time for this token can be set by the user of the platform to auto-destroy

## Security Concerns

Deleted accounts

Hacking

Central point of failure

## Why Ethereum?

A common trend that a lot of companies take advantage of the crypto space is to generate their own token or coin to compete with every currency out on the market. The vision at identity is to not create a value rather than utilize the underlying technology of the blockchain and apply it to a real-world scenario. This would lead to the

### Problems?

Gas. One of the main issues with the current vision of blockchain is the growing gas prices(transaction fee) using the Ethereum main net signals this as a problem for future iterations of what is supposed to be a service for the users. The minting process will be a one-time gas exchange. In return users gain access to the token within their wallet to the end of time. The appeal of this process is to keep the transaction at a low cost. The difference between a 10$ and a 300$ minting fee will be an inconvenience to the end user.

Legal