Understanding Decentralized Identity

A Missing Piece of Infrastructure for the dApp Ecosystem

Richard Chen Follow
Sep 7, 2018 · 10 min read

Every cryptographer's fantasy is that all of us are born with private key chips embedded in our brains so that we can always identify who we are without worrying about identity theft or fraud. Unfortunately, we don't live in such a cyberpunk utopia, so we're currently left with a broken system of passwords and social security numbers that keep on getting stolen.

Meanwhile, blockchain technology offers the promise to revolutionize digital identity by returning ownership of personal data from companies and governments to individuals, such that individuals have the power to share their data with others and revoke it as they please.

To dive deeper into why blockchain technology is useful for identity, we first need to understand the concept of identity from a philosophical lens. Consider the following thought experiment—two marbles that look and feel exactly the same are placed next to each other. While the two marbles have the same **essence** (bits and atoms), they are distinct in **identity** because we can label each marble with a unique identifier such as Marble A and Marble B.

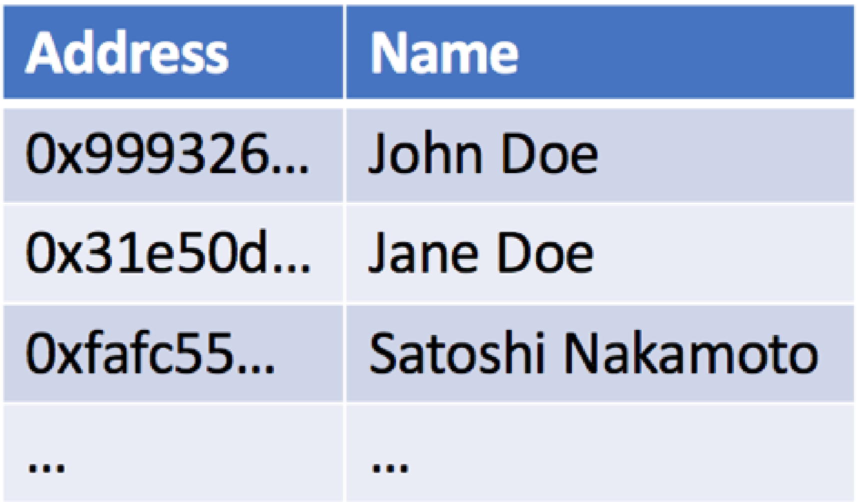
But such an identifier disappears once we mix up both marbles in a bag and are then asked to identify which is Marble A and which is Marble B. One solution to this identity problem is to have an omniscient watcher that always sees which marble is which even while they're being mixed. This works because **time**, as the fourth dimension of space, acts as a temporal indicator of identity. Blockchains, which are immutable logs of past states, provide temporal continuity and are thus useful for keeping track of identity even when physical circumstances change.

Identity is one of the most important missing pieces of Web 3 infrastructure, and there are a number of projects taking different approaches to building an identity layer that the entire dApp ecosystem can use. The two primary layers that entrepreneurs are focused on today are **namespaces** and **attestations**.

Namespaces

A key piece to decentralized identity is how people, devices, and other entities in the world are identified without a centrally owned registry.

For blockchains, right now we identify ourselves with addresses—a long string of characters such as 0x9992437898114d2770522e050883d6b2dfc48326 that is largely unmeaningful and difficult to remember. What if we could instead map each address to a unique, human-readable name?

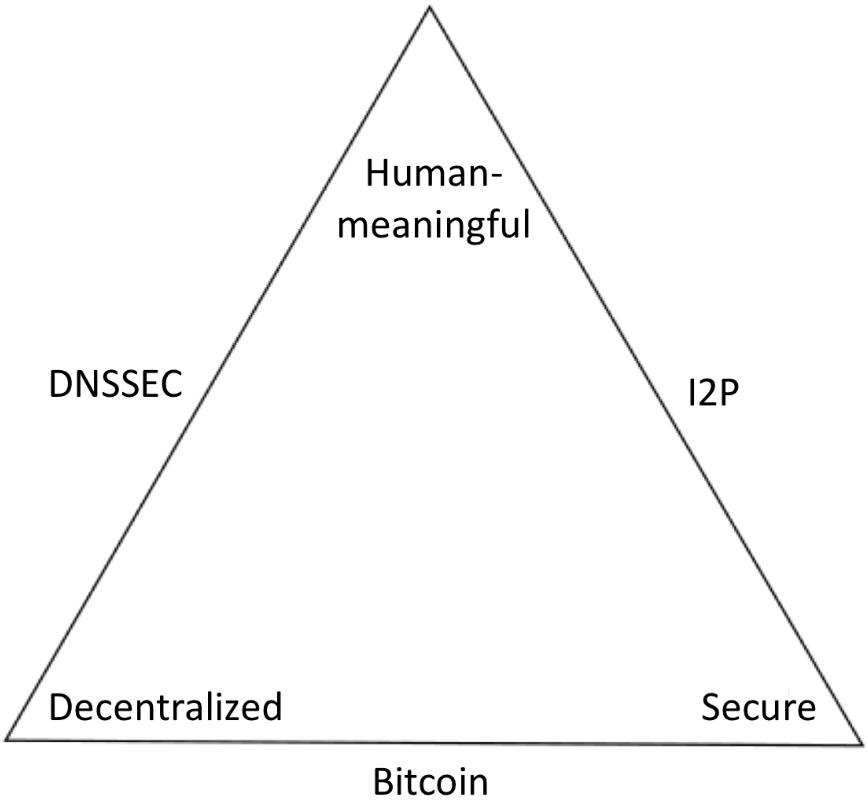


Address	Name
0x999326…	John Doe
0x31e50d…	Jane Doe
0xfafc55…	Satoshi Nakamoto
…	…

In computer science, **namespaces** are used to organize objects such that they can be identified without name collisions between multiple objects that share the same name. Examples of namespaces include file systems (assigning names to files) and DNS (assigning names to websites).

Similarly, for blockchains we want to maintain a global table of unique key-value pairs of addresses and names. Furthermore, we ideally want such a table to be secure, decentralized, and human-meaningful all at the same time. Is this even possible? We're running straight into Zooko's triangle.

Zooko's Triangle



Zooko's Triangle, named after the CEO of Zcash Zooko Wilcox, is a trilemma of three desirable properties for a naming system in a network.

- **Secure:** When you look up a name you get the correct value and not that of an impersonator.
- **Decentralized:** No central authority controls all the names.
- **Human-meaningful:** The name is something you can actually remember instead of some long random string of characters.

Zooko claimed that no digital name can achieve more than two of the above properties. Some examples examined with this framework in mind:

- **DNSSEC**, a security extension to DNS, offers a decentralized human-meaningful naming scheme but is not secure against compromises to the root server.
- **Bitcoin** addresses are secure and decentralized but are not human-meaningful.
- **I2P**, a protocol for anonymous censorship-resistant peer-to-peer communication, uses name translation services that are secure (by

running locally) and provide human-meaningful names but need to use authorities in a decentralized network.

Squaring the triangle

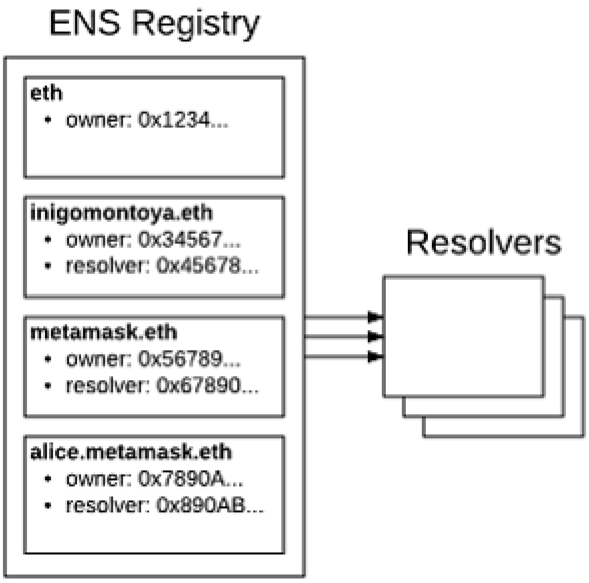
Ever since Zooko conjectured his trilemma, there have been several solutions to Zooko's triangle. Nick Szabo first proposed a solution in his paper "Secure Property Titles with Owner Authority", which illustrated that all three properties could be achieved up to the limits of Byzantine fault tolerance.

Aaron Swartz later described a naming system based on Bitcoin that uses PoW to establish consensus of name ownership. This solution inspired the creation of Namecoin. Namecoin was the first fork of Bitcoin and was the underlying blockchain for Dot-Bit, the first implementation of a decentralized DNS that squares Zooko's triangle. Dot-Bit works by allowing users to forward their current domains to .bit addresses.

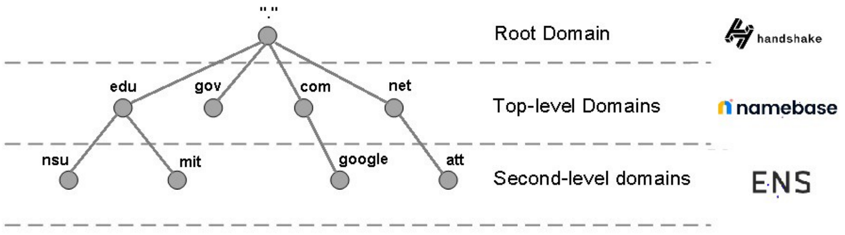
Since its release seven years ago, Namecoin has had very little adoption mainly due to a poor user experience. There are hundreds of thousands of squatted domains but only about 30 developed Dot-Bit websites. There are also rumors that Namecoin developers approached Google and ICANN at some point for potential partnerships, which defeats the purpose of building a decentralized DNS to replace central authorities.

Onename, later developed in March 2014 by Princeton researchers Ryan Shea and Muneeb Ali, is another identity system that stores usernames and personal profile data on the Bitcoin blockchain. Today, Onename is the registrar (like GoDaddy) for namespaces on the Blockstack dApp platform. Onename is also the technology that enables Blockstack users to retain ownership of all their personal data across various dApps, reducing the data monopoly power that Google and Facebook currently have.

ENS is a DNS for Ethereum that is simultaneously secure and decentralized. A smart contract serves as the registrar that manages and updates Ethereum names instead of using a centralized service like GoDaddy. Anyone can create a human-readable .eth subdomain, and the ENS resolver acts as a translator that converts names to addresses. For wallets that support ENS such as Metamask, MyCrypto, and Status, you can send money to a memorable name like 'alice.eth' instead of '0x4cbe58c50480…'. Since its launch, ENS has over 160,000 names registered with over 3.2 million ETH deposited to bid on names.



Handshake is a new, exciting project led by Joseph Poon (creator of Lightning Network and Plasma) to decentralize DNS root zones and replace ICANN and certificate authorities. Handshake is built on a new UTXO blockchain where all peer-to-peer full nodes are root servers that host the root zone file, making the root zone uncensorable, permissionless, and free of gatekeepers. Already, projects such as Namebase are making Handshake easy to use by allowing users to register top-level domains on the Handshake blockchain and by building a wallet and exchange for Handshake coins (HNS).



From the diagram above, projects such as Dot-Bit and ENS are decentralizing .bit and .eth addresses respectively, while Handshake takes it a step further to decentralize ICANN, the gatekeeper for root zone files. Source: zk Capital

Overall, Handshake is a very ambitious project that has the potential to change how DNS and naming services operate. Gaining adoption will be very difficult given operating system defaults for DNS in addition to disrupting the monopolies of incumbent certificate authorities such as Verisign.

Other projects attempting to come up with a solution to Zooko's triangle include OpenAlias and Portal Network.

Attestations

Having a namespace that is secure, decentralized, and human-meaningful all at the same time isn't enough for a decentralized identity system. To illustrate, when OneName launched someone immediately claimed the username +gavin, so OneName later had to reserve +gavinandresen for the Bitcoin core developer himself.

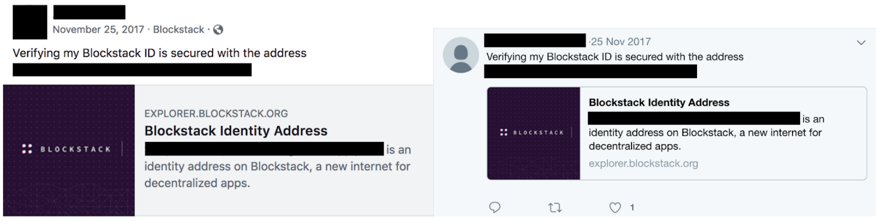
To prevent someone from impersonating someone else online, we need to verify that each person is actually who they claim to be. As an example, before you can rent a property on Airbnb, you must verify your email and phone number and optionally your Facebook, LinkedIn, and Google accounts. In this case, Airbnb acts as the trusted intermediary—both buyers and sellers trust that Airbnb has done the verification process properly. But in the dApp world, we no longer have trusted third parties, yet we still need to verify someone's identity before allowing smart contracts to execute.

As a result, attestations are the backbone of trust and reputation in a decentralized identity system. In the physical world, we attest our identity with documents like a driver's license or passport. These documents assert facts about us such as our name, age, or eye color. But driver's licenses don't exist on the Internet. Instead, we need to somehow find a way to link real-world identity to cryptographic identity. The jury is still out as to how to best pull this off, and many groups are pursuing a range of approaches.

Self-sovereign identity products

One solution is to have a standalone identity product. Such an identity product would need to support four essential features:

1. An identity has some sort of unique identifier. (The best architecture for storing such identifiers is a namespace described earlier that squares Zooko's triangle.)
2. Third-parties can make claims about an identity. Claims are attributes such as name, address, email, etc.
3. There is some way of asking a user for their identity.
4. There is some way of looking up claims about an identity.



[redacted] [redacted]
November 25, 2017 · Blockstack ·
Verifying my Blockstack ID is secured with the address
[redacted]

EXPLORER.BLOCKSTACK.ORG
Blockstack Identity Address
[redacted] is an identity address on Blockstack, a new internet for decentralized apps.

[redacted] ·25 Nov 2017
Verifying my Blockstack ID is secured with the address
[redacted]

Blockstack Identity Address
[redacted] is an identity address on Blockstack, a new internet for decentralized apps.
explorer.blockstack.org

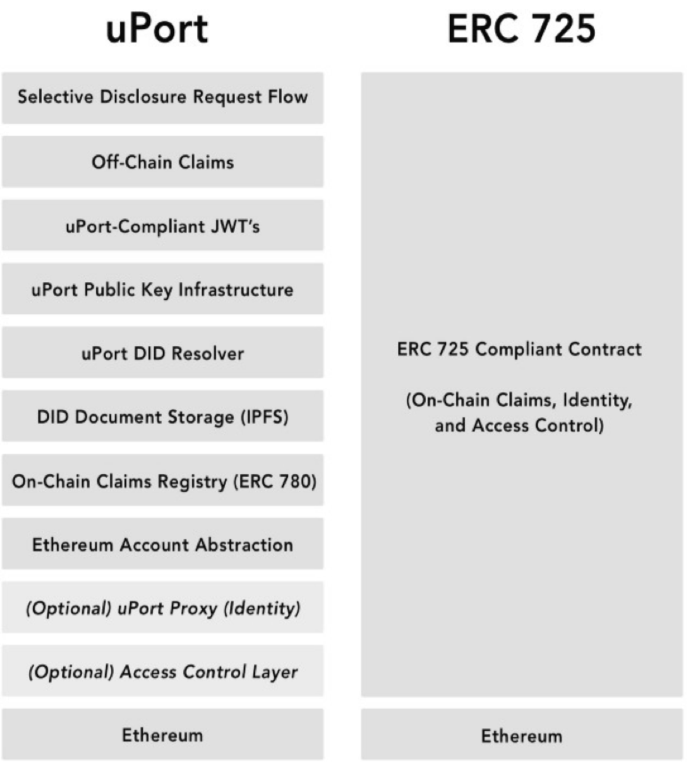
Facebook and Twitter are attesting claims to someone’s Blockstack identity.

A standalone product for identity has the benefit of being **self-sovereign**. A self-sovereign identity is a digital identity that is portable across different dApps, does not depend on any government or company, and can never be taken away. Unlike in the current Internet, as soon as you give your social security number to someone, it can be used anywhere without your consent which could potentially lead to identity theft. Self-sovereign identity allows you to connect to dApps while retaining control of attributes such as social security number that attest your identity without ever having to make a copy of that data.

There are numerous groups trying to build the de-facto standard for self-sovereign identity.

ERC 725 is a proposed standard for managing on-chain identity on the Ethereum blockchain. Created by Fabian Vogelsteller, who also created the widely successful ERC 20 token standard, an ERC 725 identity contract contains a cryptographic signature proving that the owner of the contract controls a particular claim to their identity such as an email or phone number. Origin Protocol, a protocol for creating shared economies without intermediaries, uses ERC 725 to verify claims on identity before allowing smart contracts to execute.

uPort is a self-sovereign identity wallet that gives you complete control over your identity and personal data. Developed by ConsenSys, uPort lets you create an identity on Ethereum, securely login to dApps without passwords, manage your personal information and verifications, and approve Ethereum transactions and digitally sign files. uPort also recently developed a new decentralized data storage solution called 3Box, which allows Ethereum users to upload and share their information across dApps using any wallet. uPort has partnered with the Swiss canton of Zug to offer digital IDs to residents to connect real-world identities to the blockchain.


uPort
ERC 725
Selective Disclosure Request Flow
Off-Chain Claims
uPort-Compliant JWT's
uPort Public Key Infrastructure
uPort DID Resolver
DID Document Storage (IPFS)
On-Chain Claims Registry (ERC 780)
Ethereum Account Abstraction
(Optional) uPort Proxy (Identity)
(Optional) Access Control Layer
Ethereum
ERC 725 Compliant Contract
(On-Chain Claims, Identity, and Access Control)
Ethereum

uPort improves upon the ERC 725 standard by decomposing the monolithic identity smart contract. Their new layered architecture proposal is ERC 780. Source: uPort

Civic, led by serial entrepreneur Vinny Lingham, is a dApp built on Ethereum for identity verification. In Civic's decentralized ecosystem, a user needs to have their identity verified before a requester, such as a company selling a service, can accept the user as a customer. To do so, validators verify the user's claims by cross referencing documents with government databases. Once validators verify the user's identity, they attest this information with the root of a Merkle tree that has the user's claims as the leaves.

Other similar identity products include Sovrin, Evernym, and Nuggets. Given how many groups of people are trying to tackle the identity problem, the Decentralized Identity Foundation, which counts more than 50 partner organizations, is coordinating various attempts at decentralized identity with the goal of making these systems interoperable so users aren't left with their personal data fragmented across multiple protocols.

Will decentralized identity become centralized again?

An issue with self-sovereign identity is what to do if a user's private key gets lost or stolen. Should the attacker get the keys to the kingdom? Remember, we don't live in a cyberpunk utopia where we have private keys embedded in our brains. Maybe this issue would require identity to be held by trusted third parties.

Coinbase recently acquired a startup called Distributed Systems, which is developing a decentralized identity standard for dApps called the Clear Protocol. In doing so, Coinbase may look to build a "Facebook Connect" for crypto to make it much easier for users to sign up and connect their crypto wallets. Given that Coinbase has KYC data on its 20 million customers, Coinbase could leverage its treasure trove of identity data for dApps.

Web 3 identity could eventually look something like this.

It is also speculated that Facebook's blockchain team is building an identity and single sign-on platform for dApps given how much personal information about us Facebook owns. This became apparent during the #DeleteFacebook campaign when users downloaded .zip files of all their personal data and were shocked by how much Facebook knew about them.

Telegram Passport is another unified authorization method for services that require personal identification. Using Telegram Passport, you can upload all your documents once and instantly share your data with services that require real-world ID.

So what?

Although anonymity and pseudonymity are frequently cited as use cases for cryptocurrencies, identity solutions are still strongly needed for many new crypto native behaviors like on-chain governance and token curated registries. In particular, voting systems, such as quadratic voting, rely heavily on verifiable, separate human identities because an individual could multiply his or her effective influence dramatically by misrepresenting him or herself as multiple individuals. Likewise, identity continues to be the bottleneck for these systems to be resistant to Sybil-like attacks and work effectively at scale.

In my view, a layered identity architecture that combines the best **namespace** product and the best **attestation** product is the most promising approach. It'll be interesting to see what identity solution the crypto community converges on moving forward.

. . .

About the author: Richard works at 1confirmation, an early-stage crypto venture fund based in San Francisco. Sign up for the 1confirmation newsletter and don’t hesitate to reach out on Twitter.