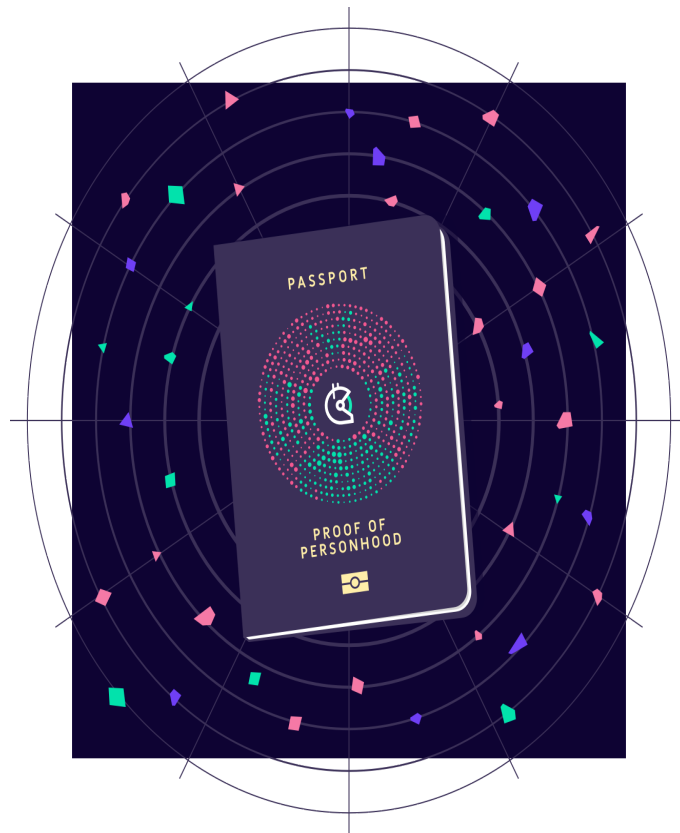


GITCOIN PASSPORT

Your Identity, Your choice



Introduction

Bots and fake accounts are a problem plaguing both web2 and web3 solutions. From fake reviews on popular web2 ecommerce sites to Sybil attacks against Quadratic Funding mechanisms, users controlling multiple accounts/bots try to undermine civil democratic functioning of sites. The need of the hour is an identity management solution that can trustlessly verify anyone's identity, while allowing us to choose how much of us we want to reveal to a third party site. Gitcoin passport, built on Ceramic, addresses this unique and multifaceted problem of intersectional identity management.

Contents

This guide, in keeping with the inclusive principles of Web3, has been prepared keeping both developer and non-developer audiences in mind.

- ***Getting Started***
- ***Web3 Identity and Ceramic***
- ***Ceramic : Composable User Data***
- ***Integrating Gitcoin Passport in Your Dapp***
- ***Gitcoin Passport Use Case Analysis: Defend Quadratic Funding***

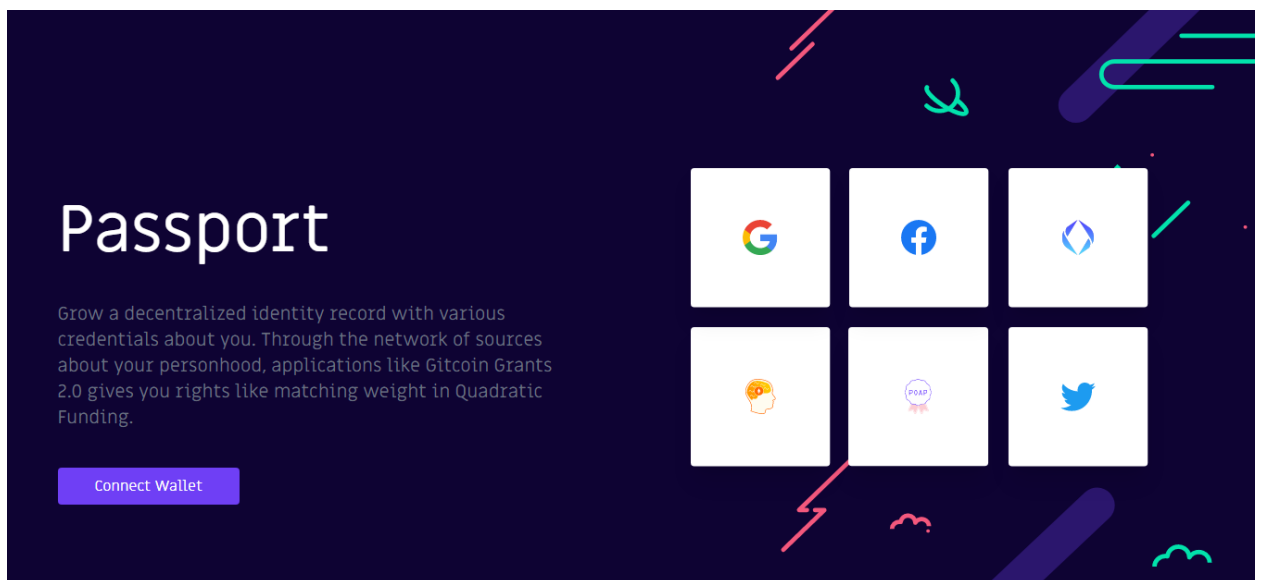
Getting Started

1. A Wallet

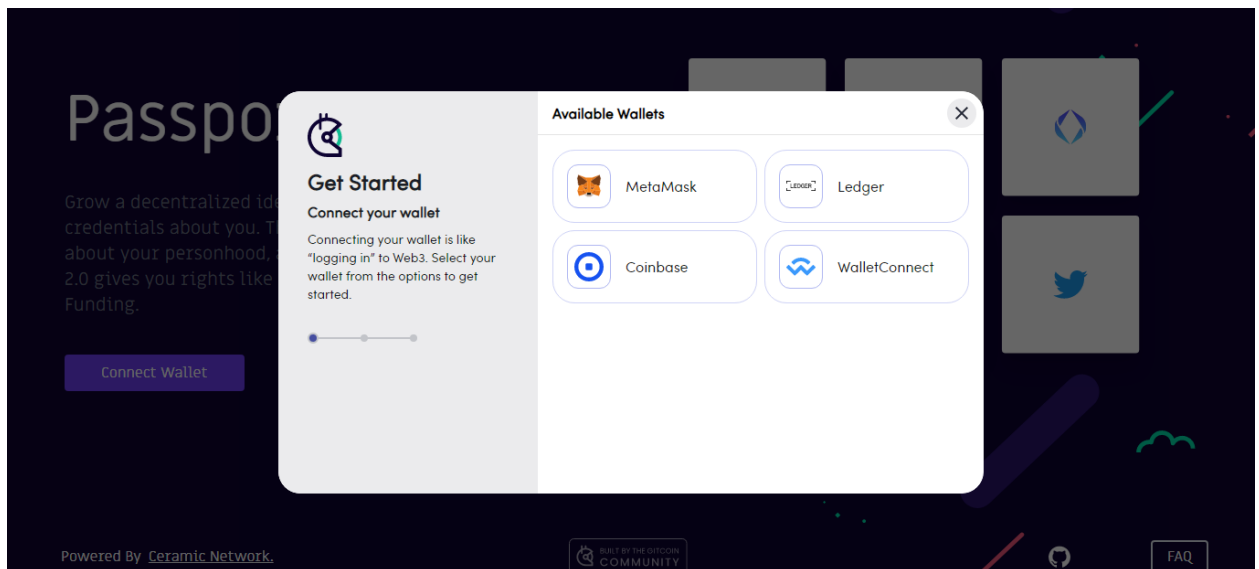
You need to have a wallet (like [Metamask](#)) installed and set up. A wallet is your gateway to the Web3 world

2. Visit the [site](#) and connect your wallet

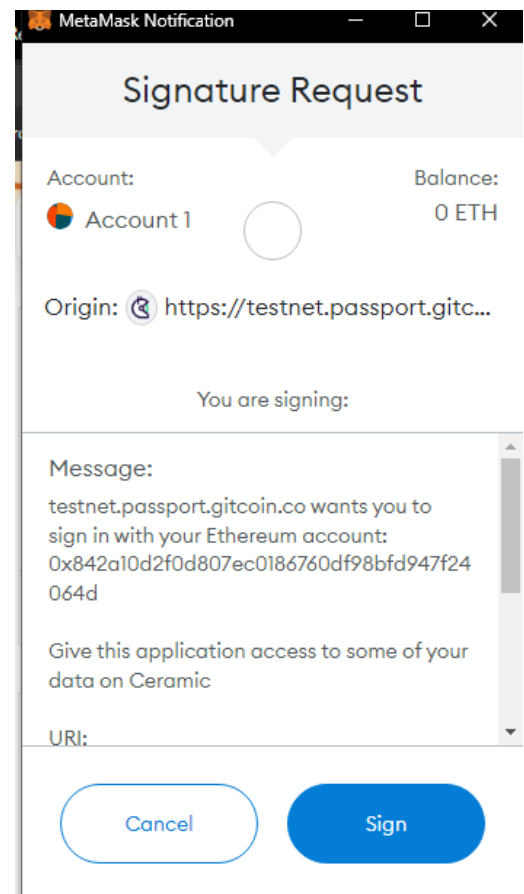
Visit <https://testnet.passport.gitcoin.co/#/> and you should be greeted with this page :



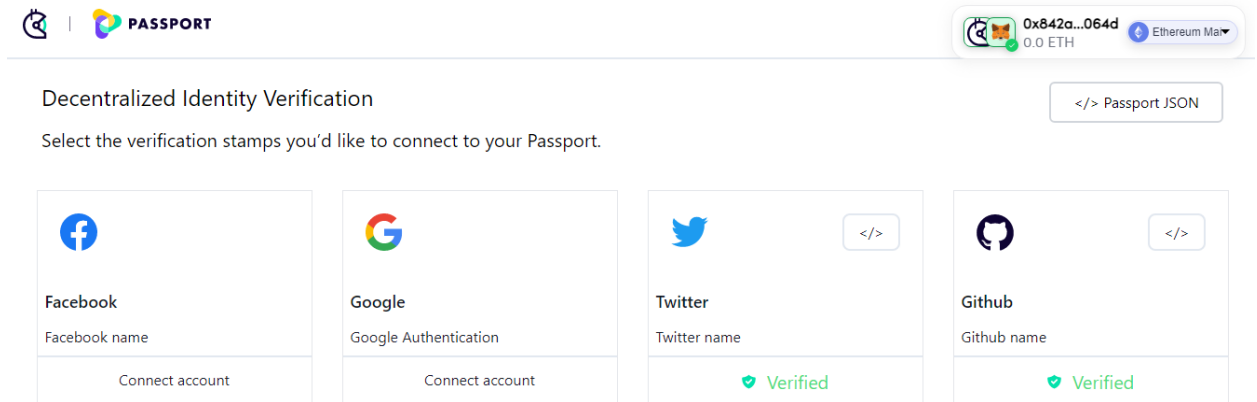
Click on Connect Wallet which should open a popup like this:



Select Metamask and you'll be greeted with a pop-up asking you to sign your message. If you're new to this, this step is basically to confirm that you own your wallet.



And that's done



As you can see I've already verified my Twitter and Github here.

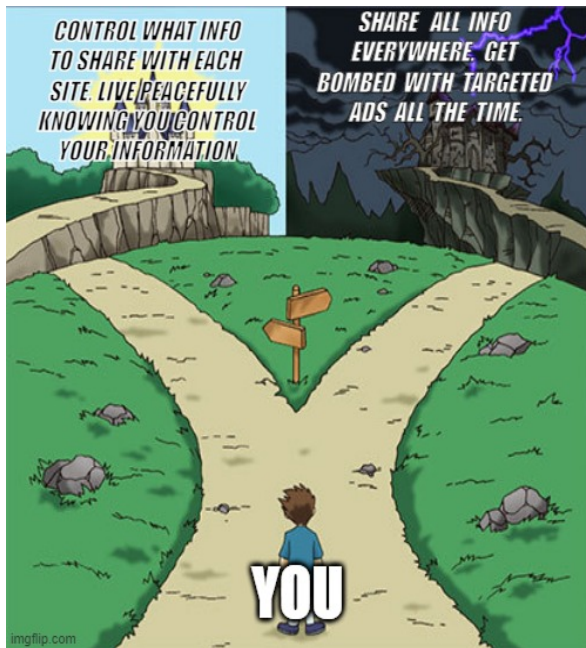
Now that you've set up your Gitcoin passport, you can start using it on any site that accepts it.

Web3 Identity and Ceramic

Under the hood, Gitcoin passports are powered by Ceramic. Ceramic is a decentralized, censorship resistant public network for managing mutable information on the open internet without databases and servers.

Web2 identity solutions suffer from the following flaws :

- They are inherently siloed.
Reputation built up in Instagram does not automatically move over to YouTube. On each platform you need to be starting from scratch.



- You don't control what aspects of your identity are shared. Big Tech has oversimplified your identity sharing into either share everything with a site or share nothing. When you OAuth into a service you cannot choose what portions of your identity you can / cannot share.

-
- You cannot truly “establish” your identity. You establish your name, date of birth, graduation degree etc. but what about your contributions to a community? Your work? You’ll probably need to upload separate certificates for those. Again the information silo-ing we already discussed means you have to repeatedly keep uploading these to any new service you sign up to that requires them, and each of them will be verifying them separately.

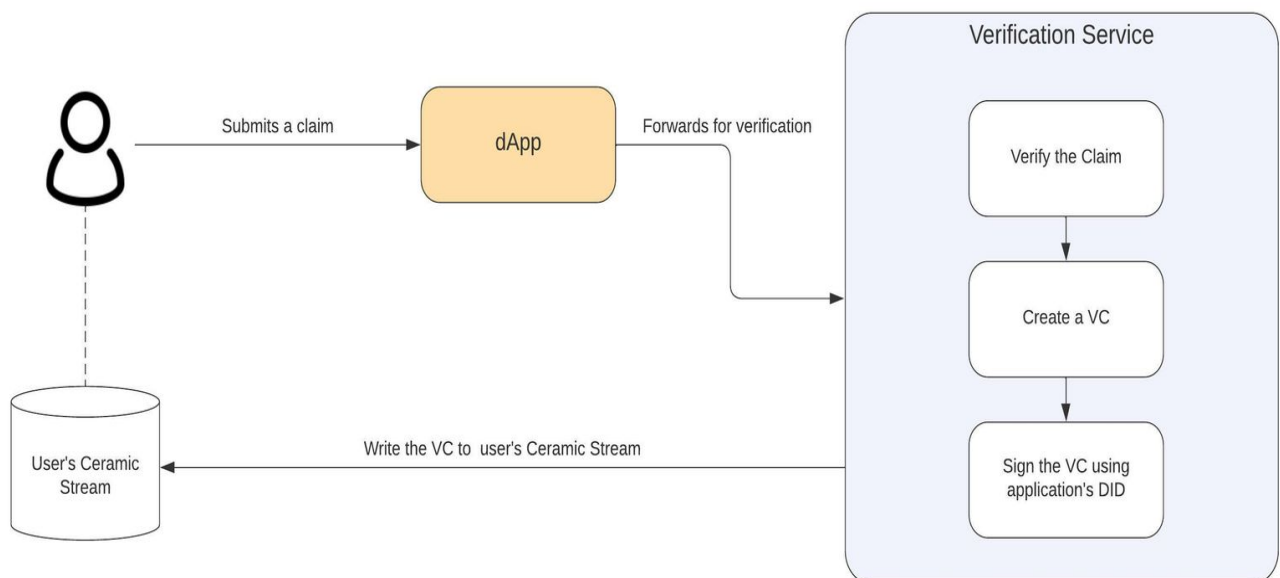
In light of these issues, the W3C (World Wide Web Consortium) announced 2 standards for identity management : Verifiable Credential (VC) and Decentralized IDentifier(DID). If you read the [FAQ](#) of the Gitcoin passport, you’ll see that these standards are basically what is being used.

For non-developers, a DID is a higher level representation of all their verified wallet accounts. An off-chain organization (say your university) can issue a credential as a VC to your DID . The following section explains how Ceramic implements VC and DID to enable this user centric reality.

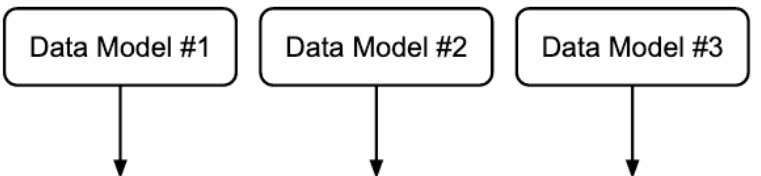
Ceramic : Composable User Data

A Verifiable Credential is a piece of contextual data that is generated and signed by a trusted party, creating an attestation for any piece of information.

A Decentralized Identifier (DID) is a uniquely generated identifier that is controlled by either single or multiple public keys. DIDs are a useful chain agnostic abstraction to sign off chain attestations such as VCs or to link to various on-chain assets. Since DIDs are chain agnostic they allow users to build a comprehensive view of their identity in a multi-chain world.

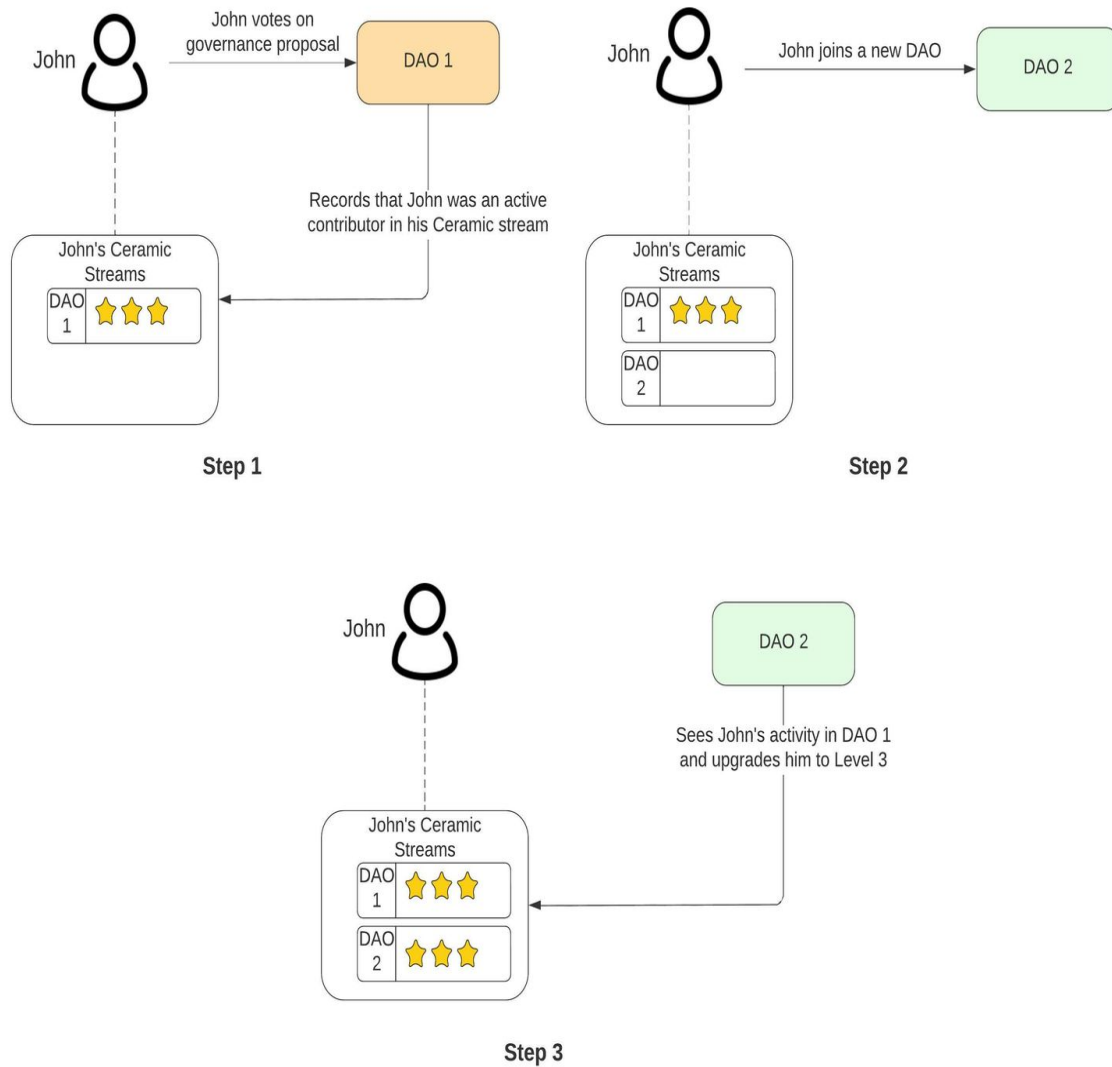


Data points collected as VCs are can be aggregated into a DID Datastore like the following:



DID	kjz123...	kjz456...	kjz789...
did:pkh: <u>eip155</u> :1:0xab12...	Alice	{ key1: "nft", key2: "wizard" }	Y2lwaGVydGV4d GZld8Ko...
did:3:kjzv4r3ujm6...	Bob	{ key1: "foo", key2: "bar" }	ZmV3cWZhc2Rm ZXdmE5...
did:nft: <u>eip155</u> :1:0xcd34...	Carol	{ key1: "defi", key2: "ape" }	w7ZvcDg0ZzM5N 2hzcw43...

Each row is a DID and each column is a data model (created by an app). Both can be discovered by any user or application and expanded indefinitely. Each user has full sovereign control over their row and can choose which data they wish to bring over to a new app. Consider the following illustration which shows an example of how an user can bring their data over from one DAO to another and immediately get promoted in the latter based on their proof of participation in the former.



Integrating Gitcoin Passport in Your Dapp

Visit the [Passport SDK site](#) to see how to integrate the SDK into your dapp.

Gitcoin Passport Use Case Analysis: Defend Quadratic Funding

Quadratic funding is one of the most democratic forms of funding out there for projects of public good. It gives more weightage to the number of votes received by a project rather than the total amount donated to the project. This achieves the goal of ensuring that the projects receiving the maximum votes get the most funding, rather than a project with just one or two large benefactors.





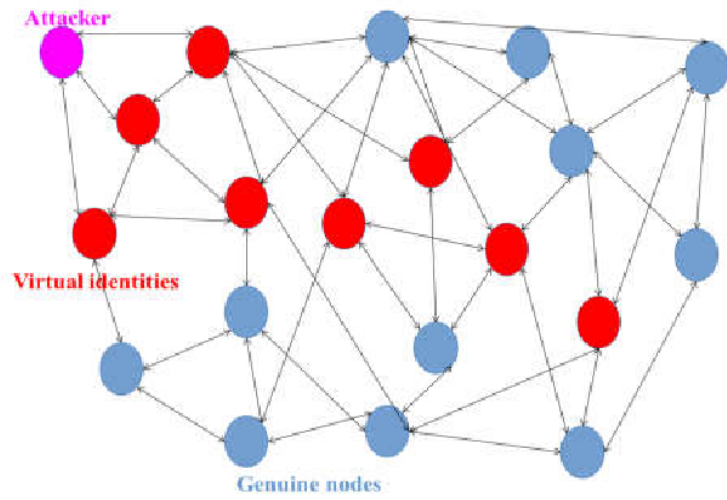
	\$10,000 MATCHING POOL 		
	A	B	C 
FUNDING	\$1000	\$1000	\$1000
NR. OF CONTRIBUTORS	5 ((\$200 EACH))	2 ((\$500 EACH))	20 ((\$50 EACH))
 MATCHED AMOUNT	\$1,851.85	\$740.74	\$7,407.41
% OF INITIAL AMOUNT	~185%	~74%	~740%

Image Source: [Finematics](#)

Quadratic funding is susceptible to Sybil attacks. Here, the attacker creates a large number of pseudonymous identities and uses them to gain a disproportionate influence on the system.



In the previous example, assume if the 2 funders of project B were malicious actors. Instead of 2 accounts donating \$500 each, they could make 250 accounts each donating \$4, or 500 accounts each donating \$2. The Quadratic Funding matching pool would give them the majority portion of the pool being fooled that it was the vote of the majority.

This is where solutions like Gitcoin Passport come in. The basic underlying idea is to increase the cost associated with creating such numerous fake identities. Having checks like Proof of Personhood immediately brings down the potential number of attacks. The ideal scenario is when the cost of attacking the network itself becomes greater than the value that can be stolen by attacking the network.
