GITCOIN PASSPORT

PASSPORT

PROOF OF
PERSONHOOD

USER GUIDE

CONTENT

Introduction

The word passport is familiar to all of us. A passport is an official document issued by a government that contains a person's identity. Just like we use identity documents in real life, digital platforms also provide different identities in the form of usernames. Same person can use any username in any platform and at the same time they can create even more usernames and pretend to be different people and can abuse the entire system for their own needs.

There arises the need for identity verifications. Different platforms then started using verifying its users identity by different methods like phone number and email verifications and other methods, but later that also found not helping in making a valid identity.

The introduction of the Web3 and blockchain based applications rapidly increases in the recent years with a lot of advantages that ensures privacy, data protection and tamper proof transactions. But Web3 also lacks in providing proof of personhood in its ecosystem.

To overcome the situation, zero proof of personhood in Web3 and blockchain ecosystem, a new system is introduced by Gitcoin that allow users to collect various identity attestations from around both Web2 and Web3 and then called it Gitcoin Passport.

Identity Verification

Identity verification is a common process held almost everywhere in different organizations and institutions in order to verify the real identity of a person. It is a mandatory process to avail the service of those providers. Government approved identity confirmation documents like passports and other national identity cards are valid for these purposes and also, sometimes the identity documents provided by the concerned organizations are also taken into consideration. Just like that, in the digital world, there exists digital identity verification.

In the earlier days, digital environments, especially in Web1 and Web2, digital identity verification methods like phone number and email verification using OTPs were used. And in recent years, it has been improved and new verification methods like Know Your Customer – KYC have been introduced and started rolling across all platforms from finance sectors to even social media.

Even though the KYC verification methods are effective up to a limit, it has the worst case when it comes to privacy and security. For the process of KYC, the organization collects the government issued identity documents such as national identity card or passport of an individual and depending on the level of service, process the document images and the data extracted to verify identity and then keep them in their servers or in databases for the future references or needs. This method faces a real challenge when there occurs widespread data breaches and data theft. All the personal identification data of an individual might face a potential risk of losing one's privacy.

In the Web3 ecosystem, identity verification has an important role when it comes to the dApps and governance platforms. One of the common challenges faced by the governance platforms is the Cybil Attack.

Sybil Attack

A Sybil Attack is a kind of security threat on an online system where one person tries to take control over the network by creating multiple accounts, nodes or computers. It is just like one person creating multiple social media accounts, for example, a Facebook or Instagram account and trying to increase like counts of their original post and manipulating the system for their own sake.

In the world of blockchain, a more relevant example is where somebody runs multiple nodes on a blockchain network. The occurrence of the Sybil attack affects the blockchain networks and governance systems in different ways.

- Attackers may be able to out-vote the honest nodes on the network if they create enough fake identities. They can then refuse to receive or transmit blocks, effectively blocking other users from a network.

- In really large-scale Sybil attacks, where the attackers manage to control the majority of the network computing power or hash rate, they can carry out 51% attacks. In such cases, they may change the ordering of transactions and prevent transactions from being confirmed. They may even reverse transactions that they made while in control, which can lead to double spending.

The Sybil attacker then may take control of the entire governance system and can manipulate its rules and decisions according to their need.

The word *Sybil* in the name comes from a case study about a woman named Sybil Dorsett, who was treated for Dissociative Identity Disorder – also called Multiple Personality Disorder.

What is Gitcoin?

Gitcoin is a platform where developers and designers get paid to work on open source software and platforms. It is the community of builders, creators and protocols at the center of open web ecosystems. People come to Gitcoin to develop their future and the future of the internet.

People can pitch their project ideas on the Gitcoin platform and can receive crowdfunding. And at the same time they can start bounty programs for getting crowdsourced help for their project in return for bounty.

People can also participate in the different bounty programs initiated by others as well as participate in hackathons organized by different organizations and institutions from both Web2 and Web3. Which means, they can be both funder and a contributor in the Gitcoin platform.

Some of the services available on the Gitcoin platform are mentioned below:

Bounties — Fund your OSS bounties and get work done or contribute to exciting OSS projects and get paid.

Hackathons — Build a bunch of cool stuff, learn new tech, support the open source ecosystem and earn cash and prizes.

Grants — Crowdfunding for open source projects; get support for meaningful open source projects.

Quests — Fun, gamified way to learn about the Web3 ecosystem, compete with your friends, earn rewards and level up.

What is Ceramic?

Ceramic is a decentralized data network that brings unlimited data composability to Web3 applications. Applications connect to Ceramic's decentralized data network via an open API to store, modify and retrieve data. All data that exists on the network can easily be reused or repurposed within other applications, creating a network of connected applications running on composable data.

Ceramic enables static files to be composed into higher order mutable data structures, programmed to behave in any desired manner, and whose resulting state is stored and replicated across a decentralized network of nodes. Due to Ceramic's permissionless design and unified global network, anyone in the world can openly create, discover, query and build upon existing data without needing to trust a centralized server.

The Ceramic Network is a decentralized, worldwide network of nodes running the Ceramic protocol that communicate over a dedicated topic on the Libp2p peer-to-peer networking protocol. Ceramic is able to achieve maximum horizontal scalability, throughput and performance due to its unique design.

Gitcoin Passport

The Gitcoin Passport is an app built by Gitcoin on top of the Ceramic Network, allowing users to collect various identity attestations called Stamps from around both Web2 and Web3. It aims to provide an infrastructure which ensures security and privacy of its users while at the same time collecting data credentials from different identity providers like Google, Twitter, POAP etc. and storing it in the Passport as a JSON object and uses all the data credentials to generate a Proof of Personhood for that individual, created in line with the Decentralized Identifier – DID and Verifiable Credential – VC specifications.

The collected data is intended for broad interoperability for any system that wishes to issue or consume VCs to establish the personhood of an individual through their direct ownership of multiple accounts or Web3 assets.

A user can easily create their passport by visiting the Gitcoin Passport website and connect their wallet and then they can collect stamps from the organizations, dApps or platforms who provide the same. Applications that integrate Gitcoin Passport can use Passport Reader to read the Passport and verify the identity of the user.

Passport Lifecycle

Consider an app that has integrated with Gitcoin Passport and requires users to have a particular set of stamps to interact with their system. When arriving at this app, the user is prompted to connect their passport. The user signs a message in their wallet that controls their Passport, granting the app access to the public key, and the app can look up their DID.

The app then attempts to fetch the Passport data from Ceramic Network. If no passport is found, the user can be informed to create their Passport on the Gitcoin

Passport website. Once connected to a Passport application, users sign a message granting the app control of their Ceramic stream. New users will have a blank passport created, and existing users will see their passport data and existing stamps. They can then continue managing their passport, linking new services and connecting stamps to enrich their verifiable online identity.

If a passport is found, the app can read and score the passport. If the user's passport holds the set of stamps required by the app the flow is over and the user can continue on and safely participate in the app's ecosystem. If not, the user can be prompted to add any additional stamps to their passport before continuing.

When a passport is presented to an app, the app can easily read the contents from the Passport using Gitcoin Passport Reader SDK and decide if the user has collected the necessary stamps to continue into the system.

Reason behind Gitcoin Passport

Social organizations online, like Gitcoin Grants, have difficulty ensuring that every participant is a unique human and does not have multiple participating accounts. As it is because, the Gitcoin Grants works with the mechanism of quadratic funding in which fund allocations are based on how many individuals contributed towards a cause. However the system is highly susceptible to Sybil attacks, in which an individual creates multiple anonymous identities and divides their contributions into smaller ones and makes contributions to themselves, so that they get a larger share of the quadratic funding matching pool as the number of donations outweighs total amount donated.

Most existing digital identity solutions are either centralized like national identity cards or individualistic. However, identity is naturally intersectional and social; everybody shares different data and relationships with a unique set of others. While we've already experimented with a more plural identity concept through the Gitcoin Trust Bonus, the Gitcoin Passport aims to provide a more collaborative and decentralized infrastructure for this paradigm.

Gitcoin launched an alpha version of the Passport for Gitcoin Grants Round 14, alongside an open-source software development kit, to start the Passport paradigm with its builder community with a vision that builders should become first-class citizens of the Gitcoin Passport ecosystem.

Need for Gitcoin Passport

People are embedded in a network of relationships and communities. People will need tools that let them own and control their data, that they can bring with them around the internet. The Passport is your way to collect the data points that help establish who you are and what communities you travel within, to help projects like Gitcoin build the most transparent, legitimate, and fair governance systems possible.

Play to earn, Professional reputation and accreditation and Digital Democracy all rely on 1 human 1 account systems to function. Currently, this is an open problem space and the Gitcoin Passport helps to establish a standard way to bring evidence of personhood to these systems. Integrating the Passport into the application will help in lowering the surface area for Sybil attacks and enable new mechanisms for accrediting accomplishment and new mechanisms for governance, all while building re-usable reputation legos that the users can take with them around the Web3 ecosystem.

Gitcoin Passport can be used as a utility that can act as a Proof of Personhood in any digital platforms including Web2. The only required process is to integrate Gitcoin Passport to that application or platform and then using Gitcoin Passport Reader SDK, it can verify the identity of its users.

Setup Gitcoin Passport

Setting up a Gitcoin Passport is pretty easy. Follow the steps below to setup one.

1: Go to the official Gitcoin Passport website passport.gitcoin.co and then click the **Connect wallet** button.
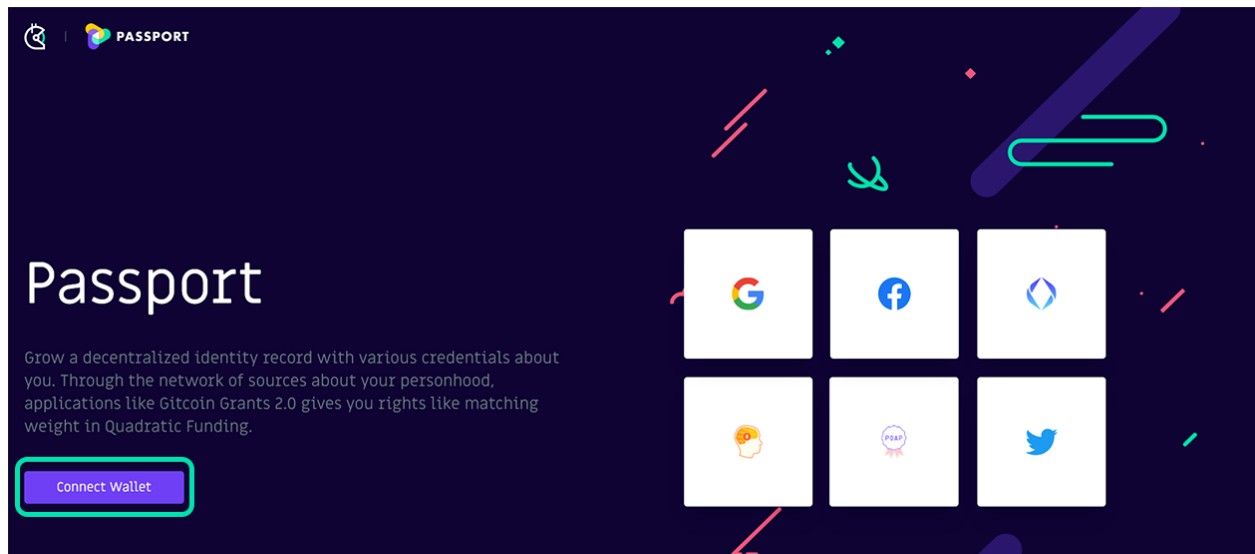
2: Click on our preferred wallet option. Here we are choosing **Metamask** wallet.
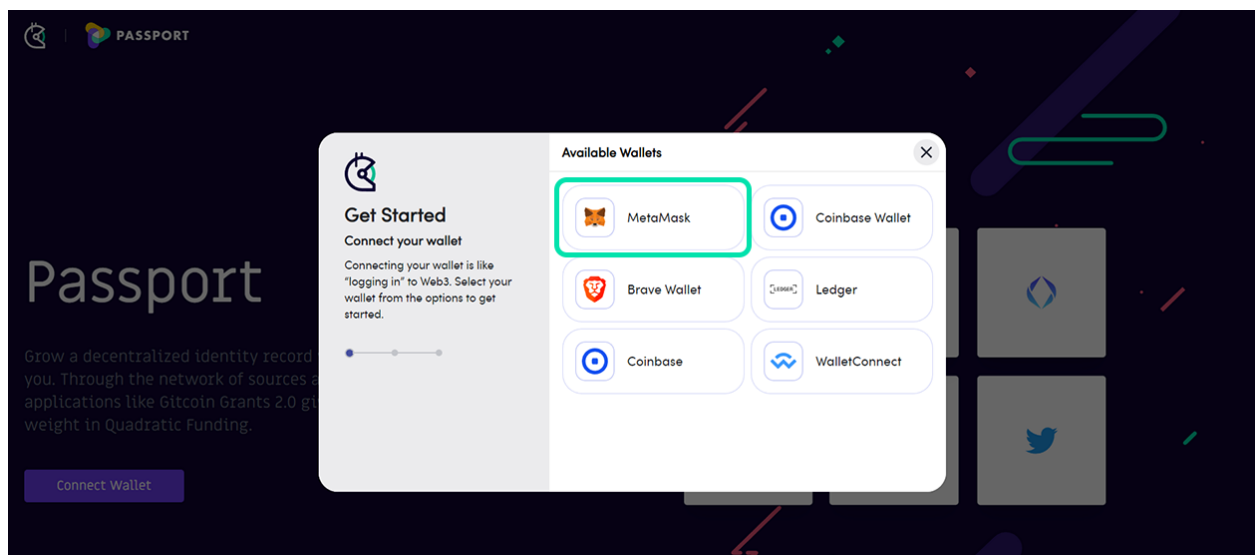
3: Click the **Next** button in the Metamask wallet dialogue box.
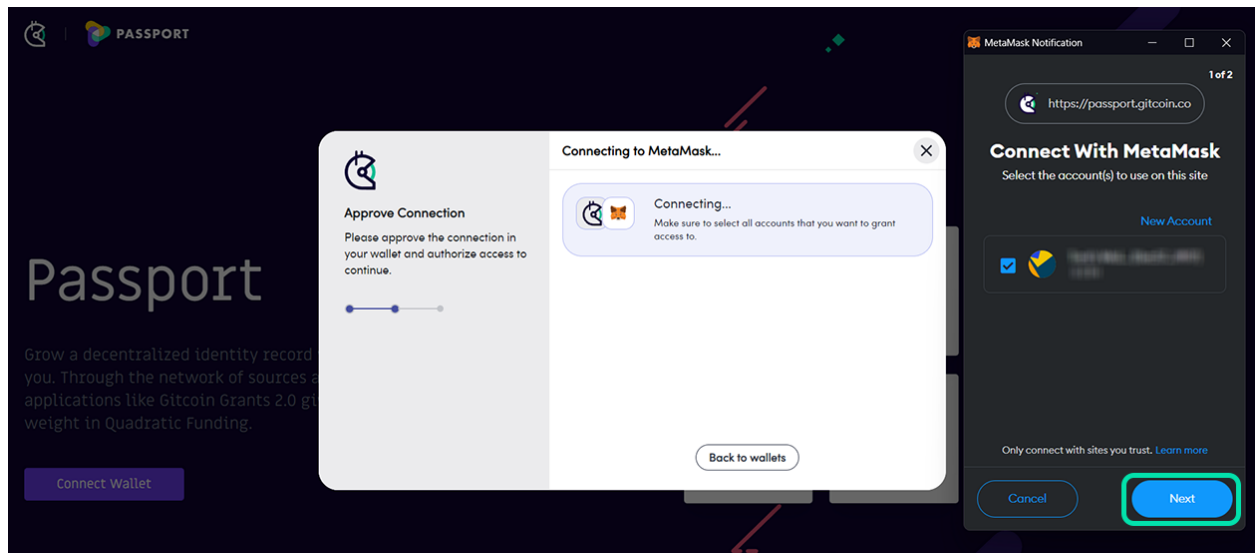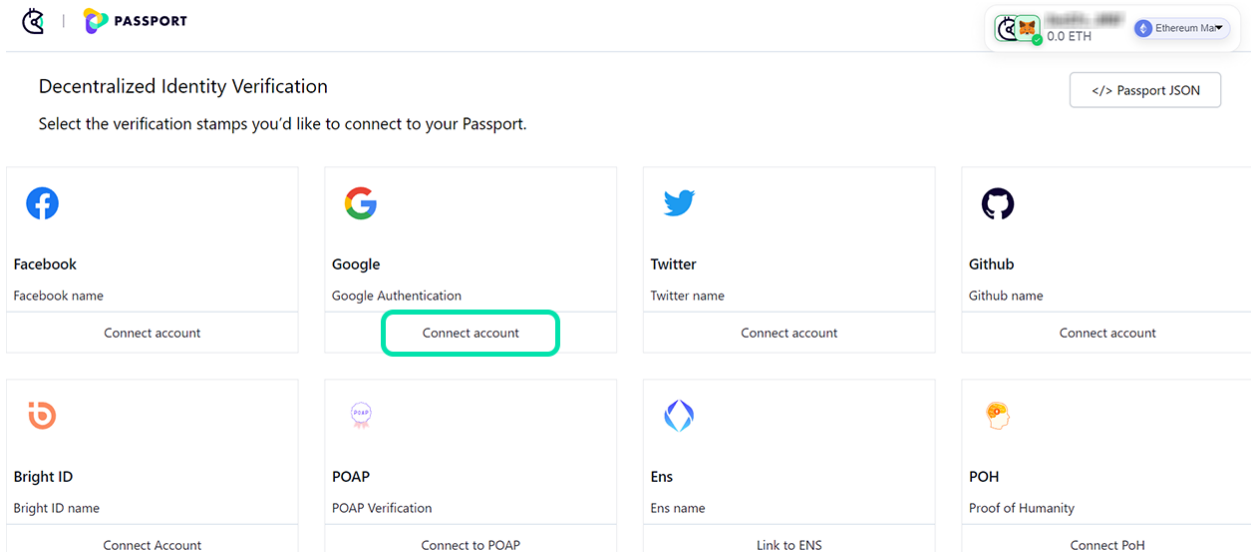
4: Then click the **Connect** button in the Metamask wallet dialogue box.
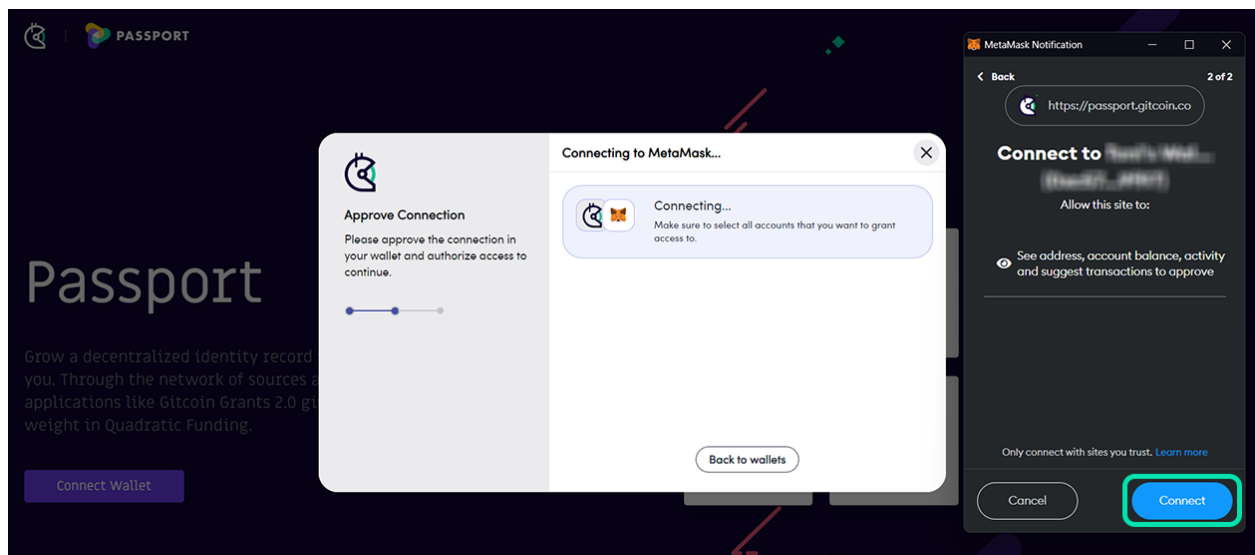
Now you have completed creating our Gitcoin Passport. The next is, we have to connect our Web2 and Web3 applications to our Passport.

5: Choose an account of our choice that we would like to connect with our Gitcoin Passport. Here we are choosing the Google account. Click the **Connect account** button.

6: Select the **Google account** that we prefer to connect with our Gitcoin Passport.

7: Now that we can see the Metamask wallet opens a dialogue box with an open to sign. Click the **Sign** button.
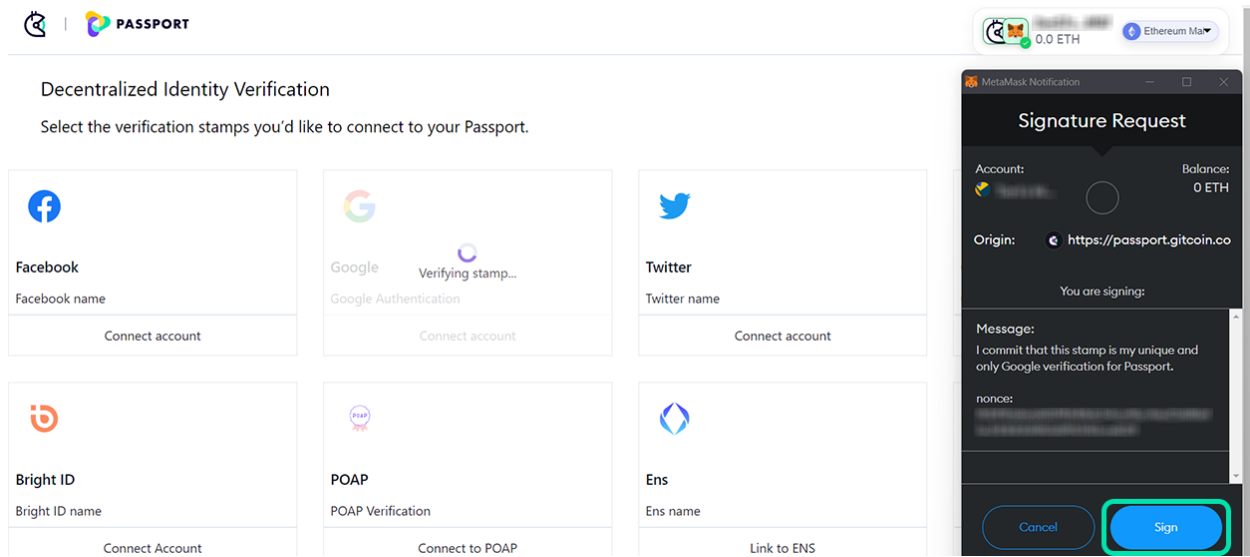
8: Now we can see that the Google account is **Verified**.
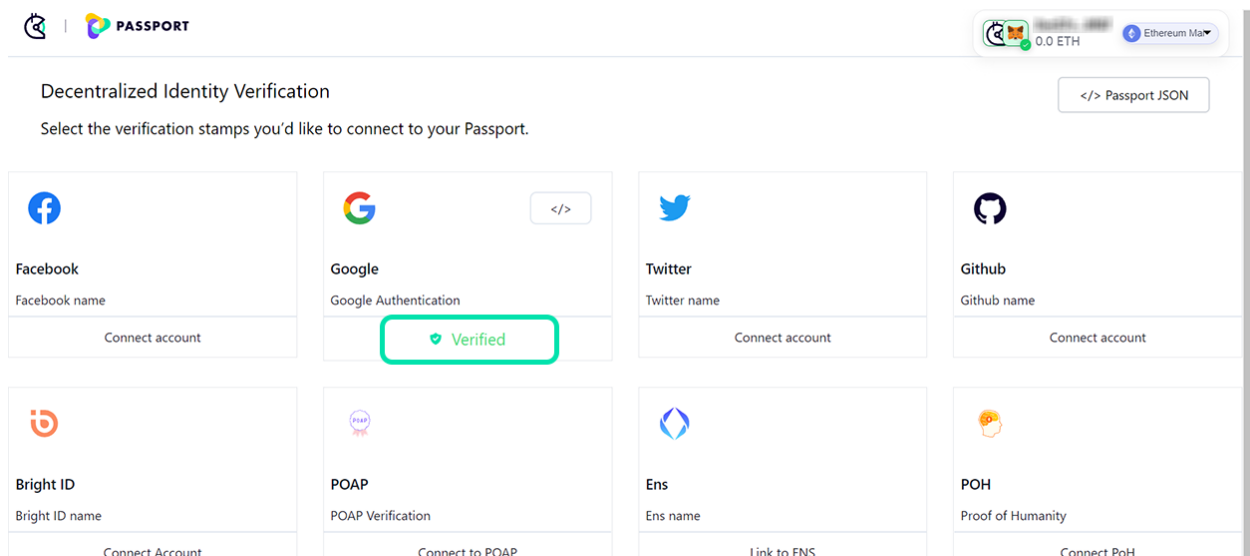
And that's it. We have successfully collected our first verification stamp!

Now that we have successfully completed setting up our Gitcoin Passport and we collected a stamp from an identity provider. We can now use our Gitcoin Passport wherever it is supported.

Gitcoin also integrates the passport to power the Gitcoin Trust Bonus, the Trust Bonus flow is available on your profile or once logged in, visit gitcoin.co/trust

There you can connect your Gitcoin Passport.

Conclusion

Gitcoin Passport is a decentralized identity verification utility, which is built on top of the Ceramic Network to store personal Verifiable Credentials and make them portable across both Web2 and Web3 ecosystems. It is one of the top high potential products that was introduced in the recent months that can bring a lot of difference in the blockchain ecosystem as well as in Web2 which can be easily adopted.

We can look forward to seeing a lot of organizations and platforms adopt the usage of Gitcoin Passport which helps every internet user to protect their identity from being abused and to preserve one's privacy and security with the advancement of a completely decentralized ecosystem.