DOCUMENTATION TO DESCRIBE THE GITCOIN PASSPORT FOR USE BY BOTH DEVELOPERS AND NON-DEVELOPERS.

It can be challenging for many social networks, especially those that are online, to make sure that each member is a distinct person who doesn't have several accounts. National identity cards are an example of a centralized digital identity solution. Most "self-sovereign" identity models are an example of an individualistic digital identity solution. However, identity is inherently intersectional and social; each person has various ties and data that they share with a particular group of people.

By preserving the depth of our widely shared lives, the Gitcoin Passport aspires to provide a more collaborative and secure framework for digital identity.

The Gitcoin Passport is an identity verification application on the Ceramic Network. Ceramic is an off-chain sovereign data network mapping decentralized identifiers (DIDs) to streams of user-controlled data. Data on Ceramic is public, permissionless, and verifiable, unlocking information access and interoperability between all platforms and services across the web. Using Ceramic,a software was written that enables people to grow personal collections of verifiable credentials about themselves and organizations to assess their identities to coordinate rights and responsibilities. Organizations define, verify, and utilize identity as functions of the networked records of the individuals.

THE GITCOIN PASSPORT

We need to grasp the old digital identity paradigm and the difficulties it encounters before we can fully comprehend the enormous advantages that gitcoin passport offers.

DIGITAL IDENTITY

Digital identity is made up of information about a person that is publicly available online; it is a collection of data that demonstrates how a person interacts with other entities in a digital environment.

In addition to personally identifiable information (PII) like complete name, address, date of birth, passwords, fingerprints, etc., digital identity also includes things like device information, behavioral analytics, transaction history, and other data.

DIGITAL ID EVOLUTION

Web1.0:

Basic authentications (username and passwords)

Web2.0:

shared authentications (users can sign up for new platforms using their login information from their current accounts), e.g. a standard sign-in button on a website that asks visitors to utilize their Facebook or Google accounts.

CHALLENGES WITH 1.0 & 2.0

- Low network diameter (all participants are connected to a central authority); information propagates quickly, as propagation is handled by a central authority with lots of computational resources.
- Usually higher performance (higher throughput, fewer total computational resources expended) and easier to implement.
- In the event of conflicting data, resolution is clear and easy: the ultimate

source of truth is the central authority.
- Single point of failure: malicious actors may be able to take down the network by targeting the central authority.
- Central authority can censor data, potentially cutting off parts of the network from interacting with the rest of the network.

WEB3.0 (self-sovereign identity SSI):

Identity solutions that use credentials held in mobile wallets, credentials can be queried by anyone seeking to verify identity. Gitcoin passport utilizes this model.

BENEFITS OF DECENTRALIZED ARCHITECTURE

- Without relying on centralized authorities, attestation can be checked.
- Decentralized identification solutions make it possible to validate and manage user identities in a seamless, private, and trustless manner.
- Anti-Sybil methods can recognize when a single person is claiming to be several people in order to manipulate a system thanks to decentralized identity.

The GITCOIN PASSPORT will now be discussed.

The internet needs a flexible public infrastructure where users can store verifiable information that is universally discoverable and available across all applications to overcome these web2 issues of duplication, fragmentation, and security. All participants can access identities, the data they are connected with, and the services by maintaining them in the public domain rather than on compartmentalized application servers. In this paradigm, users create and manage their own resources, decide whether or not to share them with others, and carry over their identities and metadata between experiences.

This concept not only gives users greater autonomy and power, but it also vastly eases the experience for developers.

Developers can concentrate on the value-add in their product rather than putting effort into managing data and connecting numerous services. Each application can easily request the information and access they require from an identity. Sharing data between products is simple and doesn't compromise privacy. Real-time experience composition is possible according to user choices. It is possible to do away with bilateral service agreements and signups in favor of frictionless payment methods for services.

All of this frees products and services from having to carry out non-essential tasks, match services and data, worry about user liability and trust, or struggle to draw and keep consumers by creating a lot of friction. Instead, programmers can simply create a product that integrates with an already-existing ecosystem of customers, data, and services. This will eventually lead to the development of more specialized micro-services and micro-applications as opposed to the behemoths we currently see.

HOW IT WORKS

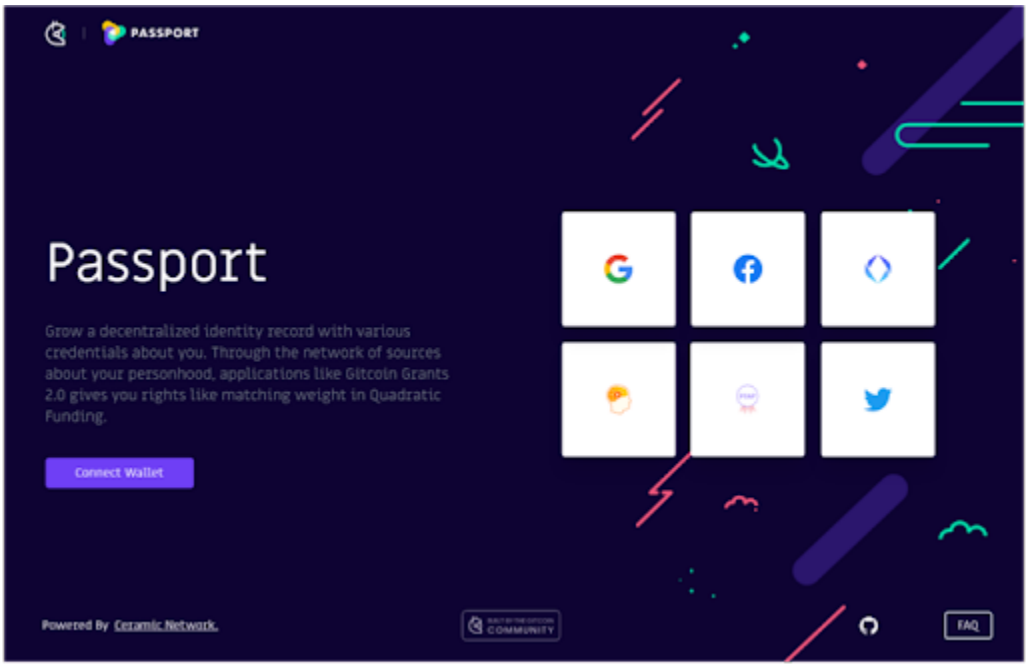
Requirements:

No matter which wallet users bring, which applications created the data, or where the resources are located, the composable web needs a permissionless, identity-centric interoperability protocol to give applications all the information they need to easily discover, route to, gain access to, and interact with a user's resources.

This include,

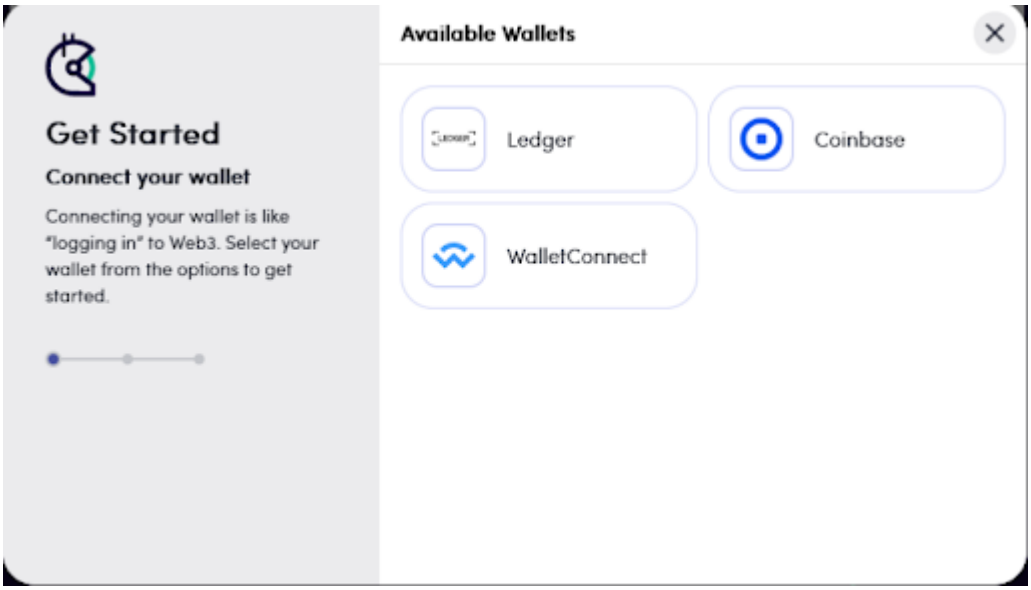
- Registering an interoperable identity (DID) without permission.
- Control this identity privately using multiple private keys;
- Assign public public keys and accounts to this identity;
- Assign resources to this identity either publicly or privately;
- Set resource permissions;
- Manage access to resources;

- Interoperably sign and/or encrypt information; and
- Revocate private keys, public keys, and resource permissions.

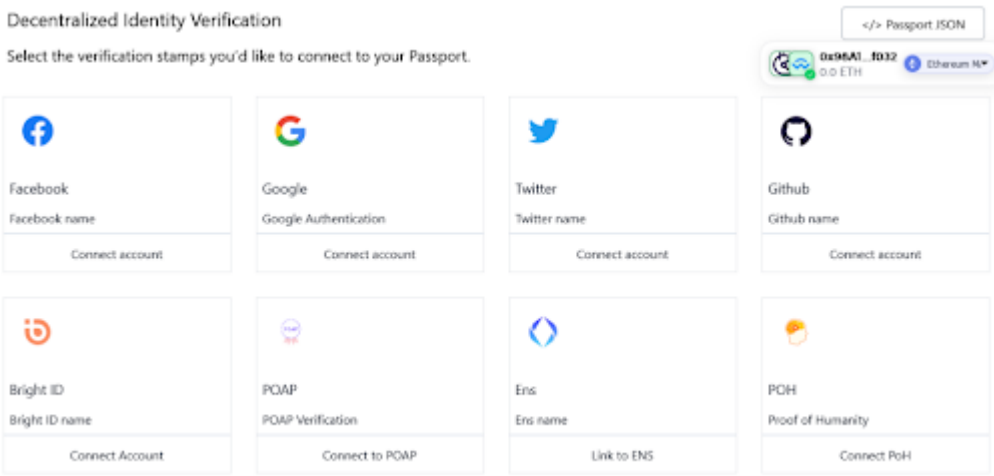


Visit https://passport.gitcoin.co

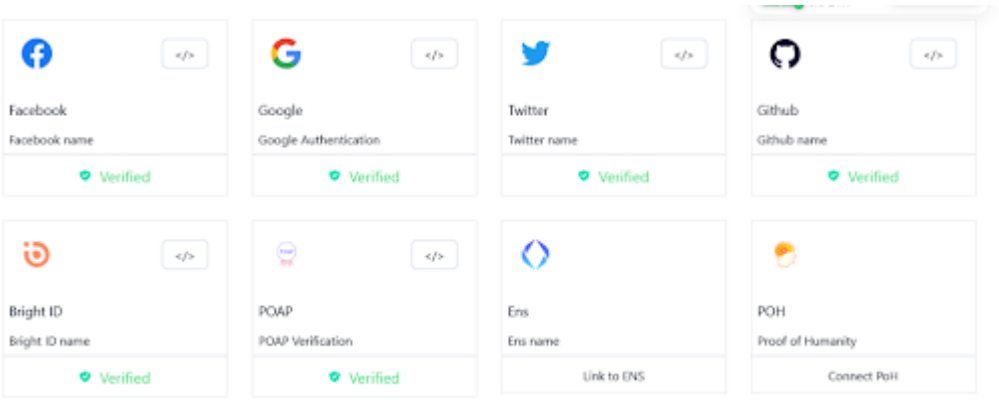
Scan The BarCode To Connect Wallet



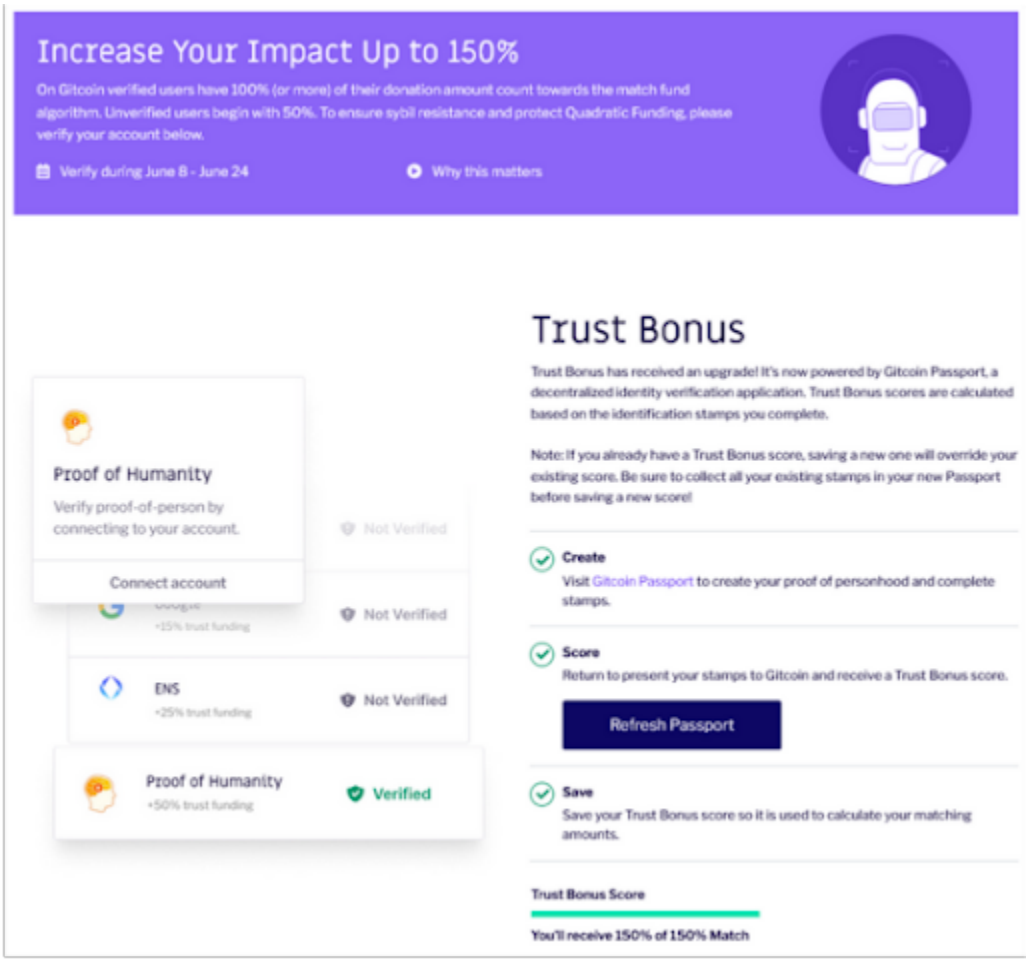
Click On The Desired Wallet To Connect Your Wallet



Connect your identity by signing in and confirming your wallet ID



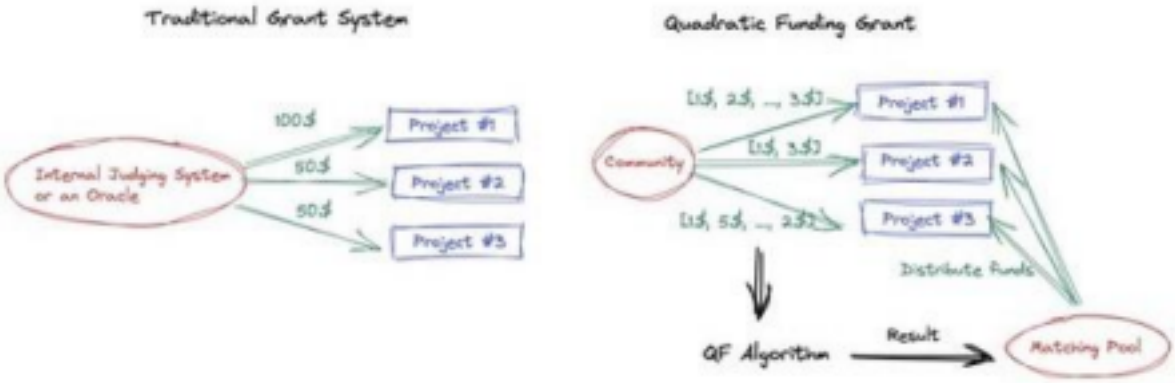
Verify your identities



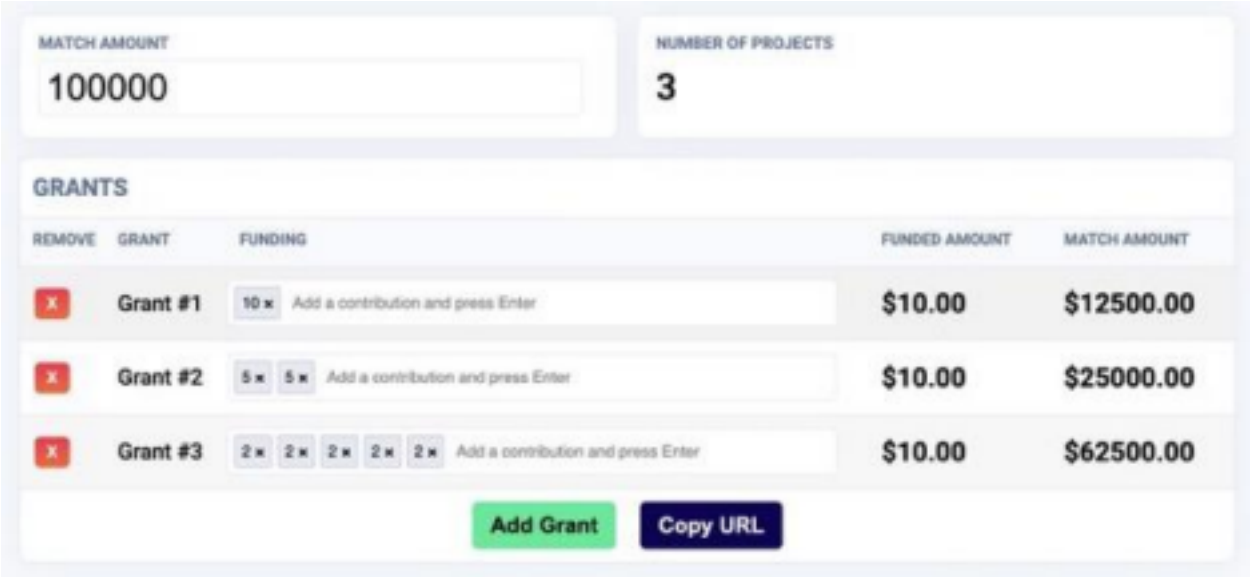
Score Your Trust Bonus To Match The Needed Points For Verification

WHY NEED A GITCOIN PASSPORT?

Gitcoin grants use a quadratic funding mechanism that distributes funds based on how many people contribute to the fund. Individuals must be distinct in such systems because the number of contributors is more important than the amount contributed.

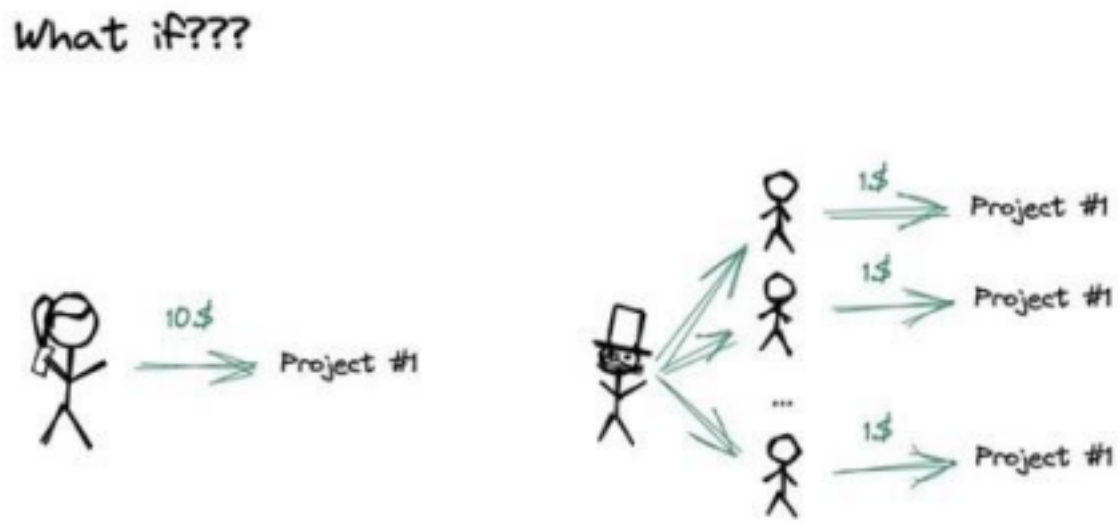


This approach was developed to combat plutocracy (governance/influence based on financial capacity), as funds are allocated regardless of contribution amount.



This system, however, is highly vulnerable to Sybil attacks, which involve an individual creating multiple identities and dividing his contributions among them in order to obtain a larger share of the QF matching pool because the number of donations exceeds the amount donated.

As an example, instead of contributing $10 from a single account, a user creates multiple identities and divides the $10 among them.



DEALING WITH SYBIL ATTACKS

The following are some effective methods for dealing with Sybil attacks:

- identity validation,
- social trust graphs,
- economic costs, and
- personhood validation.

We will investigate personhood validation in greater depth.

PoP (proof of personhood)

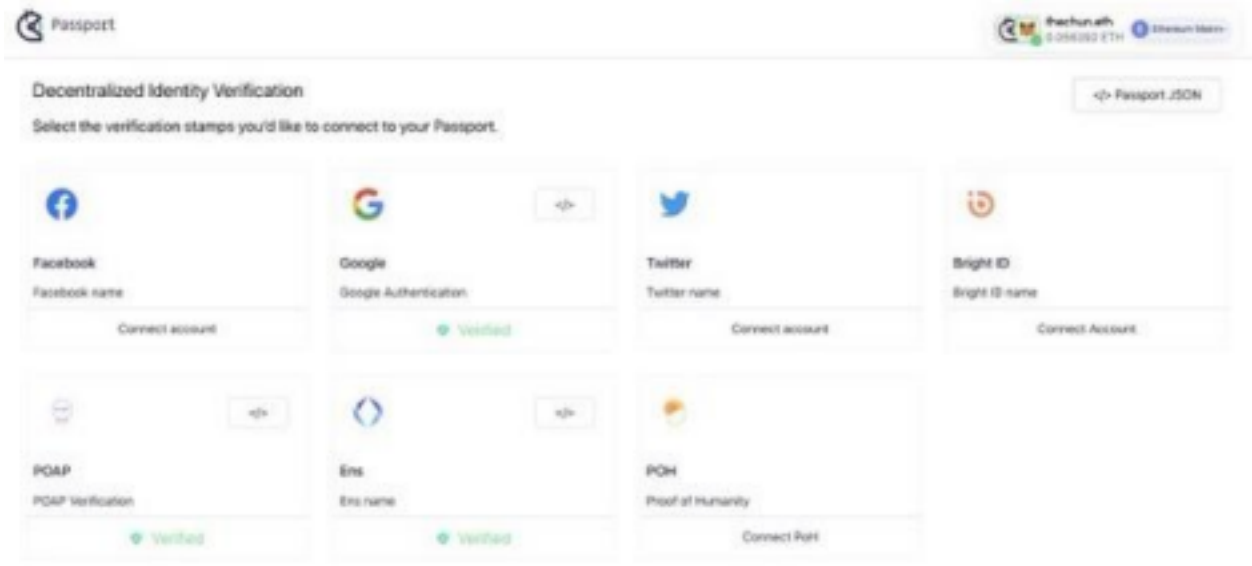
Is a permission-less consensus resistance method in which each unique individual human participant receives one unit of voting power or associated rewards, in this case a matching score. It is a protocol for validating personhood by connecting various attestations.

PoP increases the effort required to impersonate identities by verifying based on an identity's past activities and reputation. This means that an impersonator must create

not only multiple identities on gitcoin, but also multiple identities with the same names on different other providers in order to verify these identities.

HOW IT WORKS

Gitcoin passport enables users to verify their identity by linking their identities on other providers; the linked identities are signed and a stamp or identity attestation is issued. This stamp is hosted on the Ceramic Network as verifiable credentials (VCs) in the form of json data that is publicly visible and can be queried by anyone looking to verify identity or claim.



CERAMIC AS UNDERLYING TECHNOLOGY

Gitcoin passport is built on top of the ceramic network.

Ceramic is a permissionless decentralized protocol for creating and accessing unstoppable documents, which serves as the foundation for a connected interoperable web free of silos. Ceramic is ideal for storing data that must be trusted, cross-platform, interoperable, and consumed by multiple parties.

CERAMICS' BENEFITS

1. Data on ceramics is open, permissionless, and verifiable, enabling information access and interoperability across platforms on the internet.
2. Scalability
3. Mutable data storage

IDENTITY MANAGEMENT

A Passport is a self-sovereign data collection that was developed in accordance with the Decentralized Identifier (DID) and Verifiable Credential (VC) specifications.

This data is intended for broad interoperability with any system that wishes to issue or consume VCs in order to establish an individual's 'personhood' through direct ownership of multiple accounts (Twitter, BrightID), or web3 assets (ENS).

AUTHENTICATION

Let's consider an app that has integrated with Gitcoin Passport and requires users to have a minimum value of trust bonus to interact with their system

Step1

the user is prompted to connect their passport.

Step2

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.

Step3

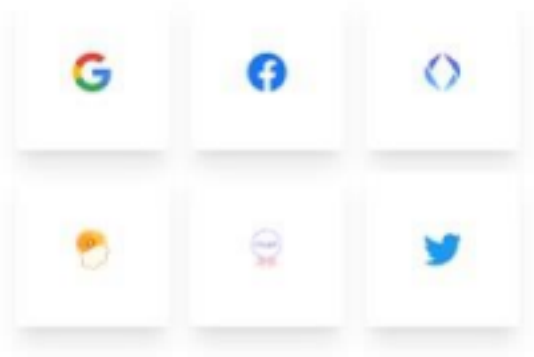
App then attempts to fetch the Passport data from Ceramic.

- If no passport is found, the user can be informed to create their passport on a frontend such as passport.gitcoin.co
- If a passport is found, the app can read and score the passport. If the user's passport reaches the minimum trust bonus 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 increase their trust bonus before continuing

VERIFICATION SOURCES AND TRANSLATION TO CERAMIC

Third party providers like google, facebook, twitter, linked in, ENS, brightID etc. all serve as verification sources.

Gitcoin passport intends to continue expanding the passport to accommodate more providers increasing the number of stamps individuals can collect.



Verified credentials (VCs) or stamps are translated to ceramic as json data where they are publicly visible and accessible

CALCULATION OF PERSONHOOD SCORES AND IMPACT ON QF IN GITCOIN GRANTS

PoPP uses Ceramic to connect a user's Ethereum address to a Decentralized Identifier (DID), allowing them to control data streams on the network. PoPP signs and issues "stamps" to the user's Passport as they verify their identity with various trusted third-parties. These "stamps" publicly attest to the user's claims. Verifiable Credentials (VCs) are stored on the user's Ceramic streams behind the scenes. These credentials are then used to compute a weighted Personhood Score, which is used to secure the Quadratic Funding mechanism.

Passports are used to determine a user's level of contribution matching. Users with higher personhood or trust bonus scores will receive more contribution matching (150 percent), while those with lower scores will receive less (50 percent).