A BEGINNER'S COMPLETE GUIDE TO UNDERSTANDING THE GITCOIN PASSPORT.

This writing covers all you need to know about gitcoin passport, the problem it solves and how it can become an essential building block for a decentralized society.

NB: understanding the decentralized web can be a little intimidating for the uninitiated, hence this writing was made as simple as possible.

THE GITCOIN PASSPORT

Gitcoin recently announced the introduction of the gitcoin passport which in the shortest of summaries is an "app that allow users collect identity attestations (stamps)

from web3 or web2 providers". Attestations are claims made by one entity about another entity, an example is certificate issue to an individual showing proof of (attesting) attendance and graduation from a particular institute.

Before diving in deeper into gitcoin passport we need to understanding the traditional digital identity model, the challenges it faces and then we would fully appreciate the huge benefits gitcoin passport offers.

DIGITAL IDENTITY

Have you ever shared a photo with friends online? watched a series on Netflix ? or perhaps shopped on Amazon then you own some sort of digital identity.

Digital identity is made up of information that is available about a person online, it is a composition of data showing the relationship/interaction of an individual with other entities in a digital environment.

Digital identity includes things like device information, behavioral analytics, transaction history as well as personally identifiable information (PII) such as full name, address, date of birth, passwords, biometrics etc.

EVOLUTION OF DIGITAL IDs

A. CENTRALIZED ARCHITCETURE

Web1.0: basic authentications (username and passwords)

Web2.0: shared authentications (users can register for new platforms using existing account credentials) eg. A typical button on a website asking users to sign in with google or facebook.

CHALLENGES WITH 1.0 & 2.0

- Multiple identities

Users can create multiple fake accounts in order to manipulate given scenarios to their favor

- Data protection and privacy rights

Sensitive user information can be accessed by third party providers who hold information regarding the user.

- Sensitive to security attacks

Centralized data are usually targets for security attacks

B. DECENTRALIZED ARCHITECTURE

WEB3.0 (self-sovereign identity SSI): identity solutions that uses credentials held in mobile wallets, credentials can be queried by anyone seeking to verify identity. Gitcoin passport utilizes this model.

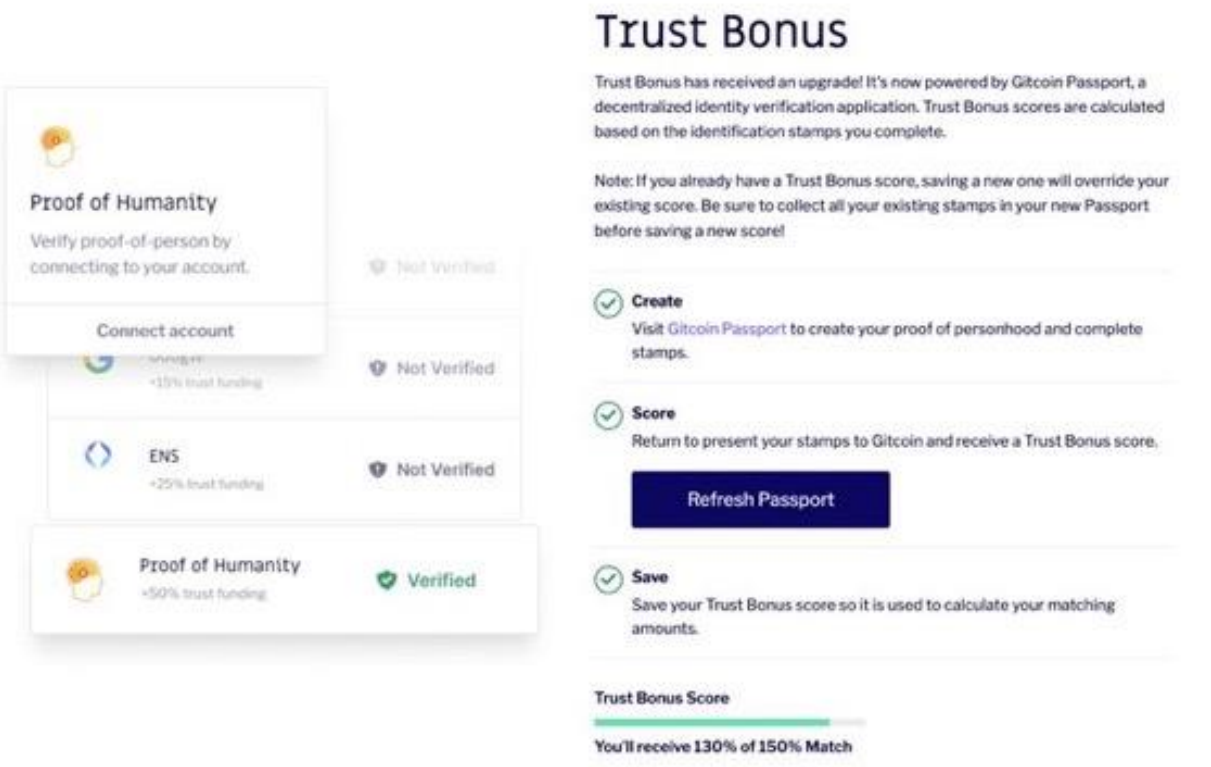
BENEFITS OF DECENTRALIZED ARCHETECTURE

- Attestations can be verified without relying on central authorities
- Decentralized identity solutions facilitate a trustless, seamless and privacy-method for verifying and managing user identity
- Decentralized identity enables anti-Sybil mechanisms to identify when one individual is pretending to be multiple humans to game a system.

Now back to the GITCOIN PASSPORT

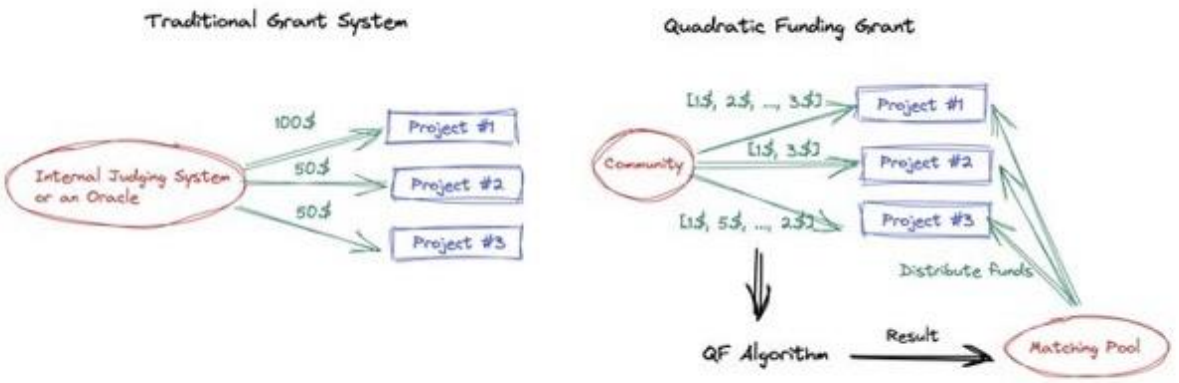
The gitcoin passport is a **decentralized** application that allows users to verify their identities by collecting attestations about identities otherwise called stamps from prominent web2 & web3 providers (google, facebook, ENS, brightID etc) identifying such users as members of the given provider.

Verifying identity rewards users with a trust bonus or a personhood score, the more stamps a user collects (the more providers you verify identity with) the more personhood score you get.

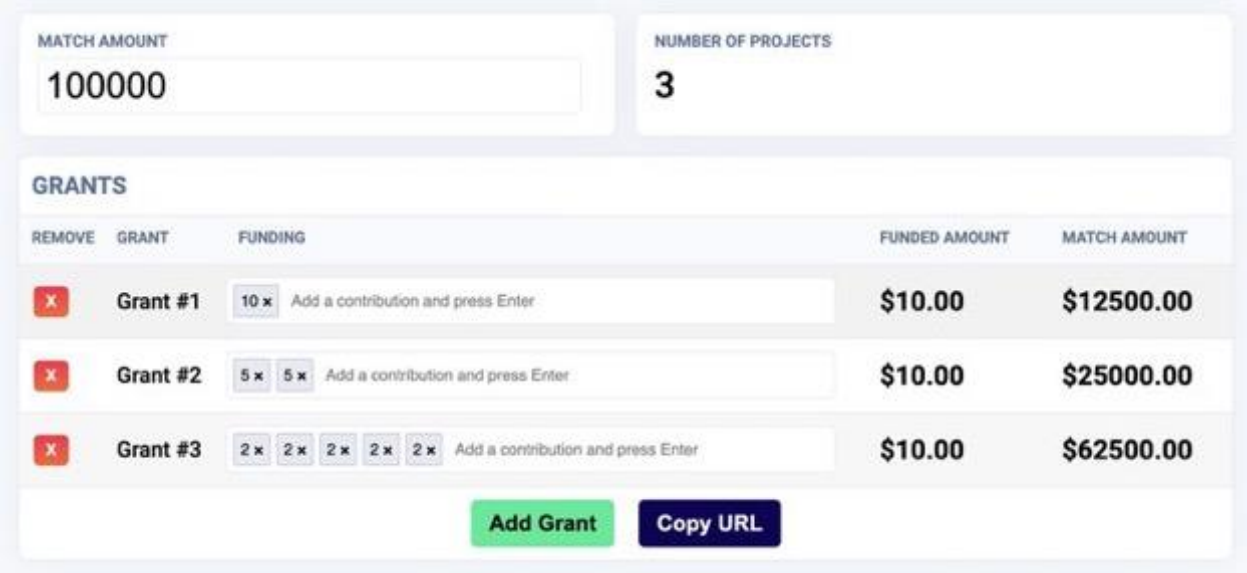


WHY THE GITCOIN PASSPORT?

Gitcoin grants operates a **quadratic funding** mechanism that allocates funds based on how many individuals contribute to the funds. In such systems there is need for individuals to be unique as the number of contributors are more significant than amount contributed.

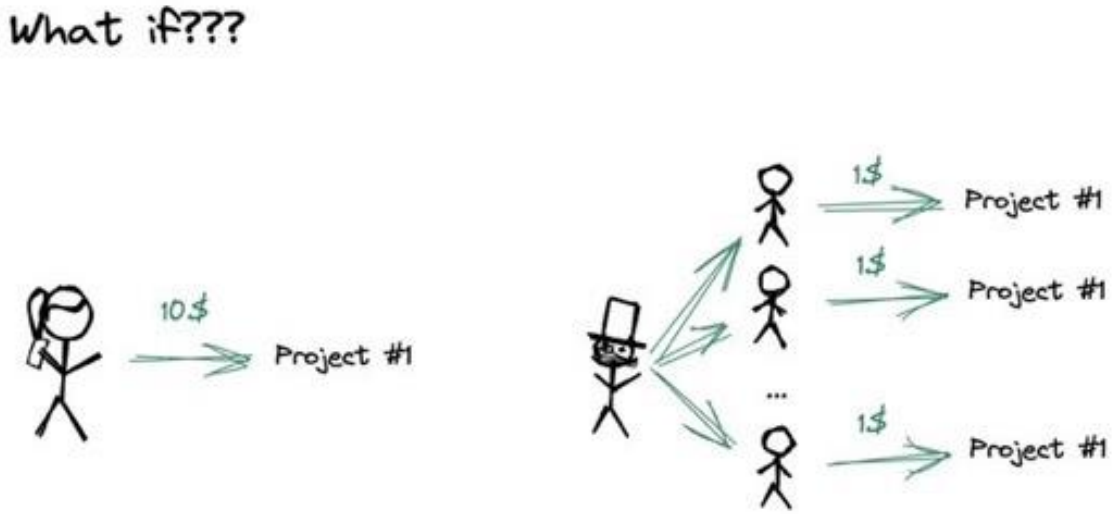


This approached was created originally to combat plutocracy (governance/influence on the grounds of financial capacity) as funds are allocated independent of amount contributed.



However this system is highly susceptible to Sybil attacks which involves an individual generating multiple identities and dividing his contributions amongst them using them to get a larger share of the **QF** matching pool since number of donations outweighs amount donated.

An example is a user instead of contributing $10 from a single account creates multiple identities and divides $10 between them.



DEALING WITH SYBIL ATTACKS

Below are some methods to effectively handle Sybil attacks

- Identity validation
- Social trust graphs
- Economic costs
- Personhood validation

We will look more closely at personhood validation.

PoP (proof of personhood)

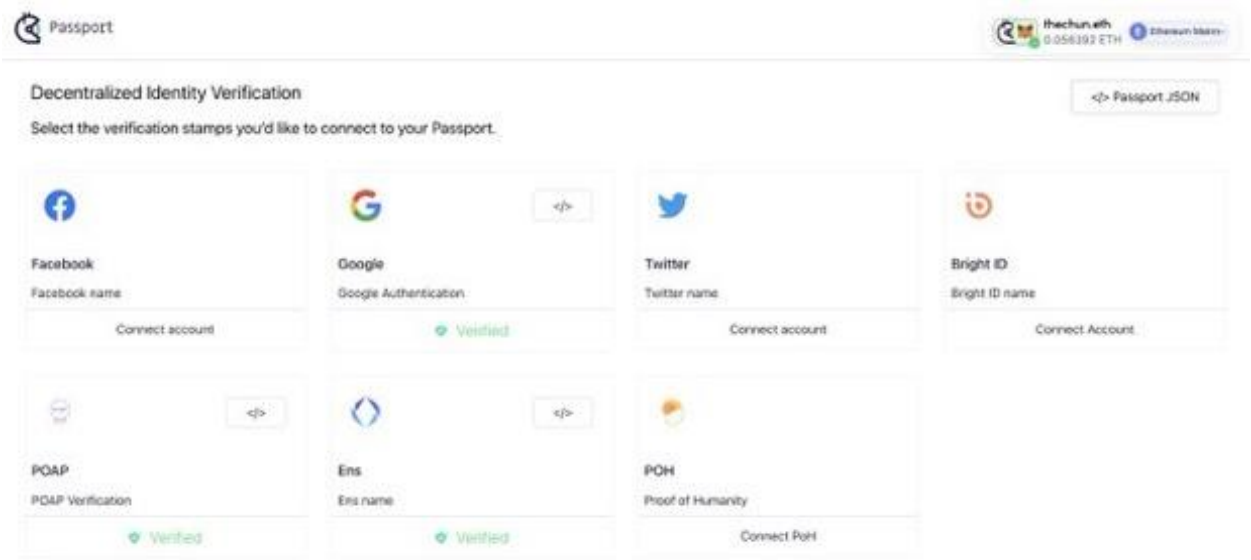
Is a resistance method for permission-less consensus in which each unique individual human participant obtains one unit of voting power or associated rewards in this case a matching score. It's a protocols that validates personhood by linking various attestations.

PoP increases the effort to impersonate identities by verifying based on an identity's past activities and reputation that means an impersonator needs not just to create multiple identities on gitcoin but also multiple identities with same names on different other providers in order to verify these identities.

PROOF OF HUMANITY

HOW IT WORKS

Gitcoin passport allows users verify their identity by linking their identities on other providers, the linked identities are signed and issued a stamp or identity attestation. This stamps are hosted on ceramic network as verifiable credentials (VCs) in form of json data which 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 the ceramic network.

Ceramic is a decentralized permissionless protocol for creating and accessing unstoppable documents that serve as the foundation for a connected interoperable web without silos. Ceramic is ideal for storing information that requires guaranteed trust, cross-platform, interoperability, and multi-party consumption.

BENEFITS OF CERAMICS

- Data on ceramics is public, permissionless and verifiable, unlocking information access and interoperability between platforms across the web
- Scalability
- Mutable data storage

IDENTITY MANAGEMENT

A Passport is a self-sovereign data collection, created in line with the Decentralized Identifier (DID) and Verifiable Credential (VC) specifications.
This 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 (Twitter, BrightID), or web3 assets (ENS).

AUTHENTICATION

Lets 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

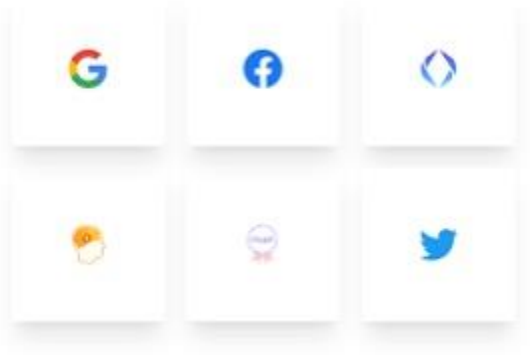
Step1
user is prompted to connect their passport.
Step2
The user signs a message in their wallet that controls their Passport, granting the app access to public key, and the app can lookup their DID.
Step3
App then attempts to fetch the Passport data from Ceramic.

- 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 leverages Ceramic to link a user's Ethereum address to a Decentralized Identifier (DID) which enables them to control streams of data on the network. As users verify their identity with various trusted third-parties, PoPP signs and issues "stamps" to the user's Passport that publicly attest to the user's claims. Behind the scenes, these are Verifiable Credentials (VCs) that are stored on the user's Ceramic streams. These credentials are then used to calculate a weighted Personhood Score that secures the Quadratic Funding mechanism.

Passport are used to determine the level of contribution matching a user receives. Users with higher personhood scores or trust bonus will receive more contribution matching (150%) while users with a lower score will receive less (50%).

Conclusion

Gitcoin passport will be essential for

- Fair Quadratic funding
- Private identity and reputation systems
- Other future use cases !


GITCOIN