ANTI-SYBIL PROTOCOL USING VIRTUAL PSEUDONYM PARTIES

ABSTRACT.

Bryan Ford proposed **pseudonym parties** – gatherings across the world – to verify the individuality of the participants. His pseudonym parties algorithm is based on doing *simultaneous* and *randomly assigned* pseudonym parties all over the world, and doing them repeatedly throughout the year. The proof behind it is that *you cannot exist in two different spaces at the same time*. The protocol is **trust-less**, you trust the algorithm, and you don't need to trust the people you verify.

The **Proof-of-Individuality** (POI) system is a digital version of Bryan Ford's pseudonym parties algorithm. It moves the gatherings into the digital space. The protocol is agnostic about what technology is used to hangout, and possible interfaces range from simple chat application like Google Hangouts to the latest Microsoft Holoportation technology for a more immersive virtual reality experience with higher resolution co-presence.

1. INTRODUCTION

Bryan Ford wrote in his 2008 white-paper *Pseudonym Parties: An Offline Foundation for Online Accountability* that

> 'The right to *anonymity*, often seen as a necessary component of free expression, has long seemed at odds with the principle of *accountability*, an equally basic foundation of social justice and the rule of law. This tension between anonymity and accountability may not be fundamental, but merely an indication that our *current mechanisms to provide them are too primitive*. '

He then went on to propose pseudonym parties as a new form of anti-sybil mechanism.

Recent advances in smart-contract technologies make it easy to deploy and experiment with Ford's pseudonym parties algorithm. The POI system is a first attempt at deploying a pseudonym parties system, and it takes Ford's ideas into the digital space and the digital age. The digital version transcends some of the problems that the Ford's IRL version faces, such as people creating fake regions and populating them with fake meet-ups.

2. CONCEPTS

Pseudonym parties happen at set intervals throughout the year. Possible time-frames are monthly events, or even weekly. The more frequent the events, the smaller the cost of missing out on one. The PoC uses a time-period of 28 days, and 13 events per year.

Users can register for a round as soon as the previous round has expired. The registration is open until mere hours before the pseudonym party event, and once registration has closed, users are assigned by random into groups. The PoC has a group-size of 5 people per group.

Upon registering, a user puts in a deposit that is later returned in full once that months POIs have been issued. These deposits prevent a majority attack.

3. THE POI TOKENS

The proof for being successfully verified comes in the form of a POI token. The token is issued to the address that was verified, and is valid for the full period of time leading up to the next pseudonym party event. The tokens are anonymous by design, and cannot be traced to 'who you are'. The proof is instead that it's very hard to obtain multiple of these tokens.

Each round gives you a new POI token, that is not traceable to your previous token. The POI tokens are similar to Bitcoin as 'digital-gold' in that sense, each POI is completely public but its very hard to find a pattern in who they have belonged to.

4. MAJORITY ATTACK

If someone gains access to an entire hangout group, then they could have their accounts verify one another. Owning *n*-x total number of accounts gives one a chance to control multiple accounts in a single hangout, and this chance increases with *n*. For example, controlling 100x total accounts would let you control a majority of the hangouts and own a majority of the POIs each round.

The majority attack is prevented with **anti-spam deposits.** Each user puts in a deposit upon registering, and this makes it expensive to own *n*-x total number of accounts.

5. GOVERNANCE OF SIZE OF ANTI-SPAM DEPOSIT

The size of the anti-spam deposit is managed by the users. New deposit sizes can be proposed and voted on by community members. New proposals are voted on using ether. Users can vote using the deposit that they put in upon registering for a POI round. To attack this governance system and gain a majority vote, an actor would have to own more ether then the combined supply of the *current deposit * the number of users,* plus private ether that users are willing to put in to prevent an attack.

All deposits are returned in full after a round has finished. Deposits will never stay in the system longer than the period of time that stretches from one pseudonym party event to the next.