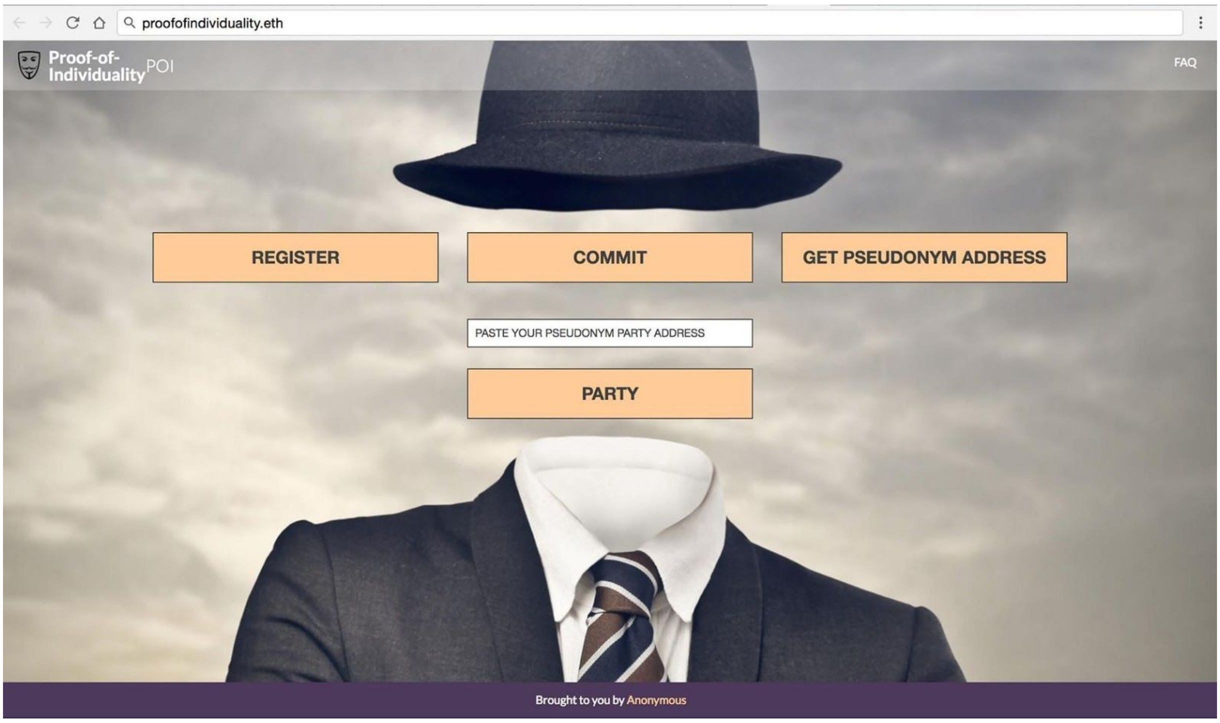
Online Pseudonym Parties: A foundation for proof-of-personhood in the web 3.0 jurisdiction

ABSTRACT: In 2008, Bryan Ford published *Pseudonym Parties: An Offline Foundation for Online Accountable Pseudonyms*, the idea to use global events where people all over the world verified one another, where the proof was that a person could not be in two places at the same time. Online Pseudonym Parties builds on Ford's idea, and does online events instead, that are used to provide global pseudo-anonymous proof-of-personhood (PoP) tokens, a sort of "temporary access tokens", similar to festival bracelets.

The PoP tokens are renewed monthly, untraceable from month to month, and disposable.


proofofindividuality.eth
Proof-of-Individuality POI
FAQ
REGISTER
COMMIT
GET PSEUDONYM ADDRESS
PASTE YOUR PSEUDONYM PARTY ADDRESS
PARTY
Brought to you by Anonymous

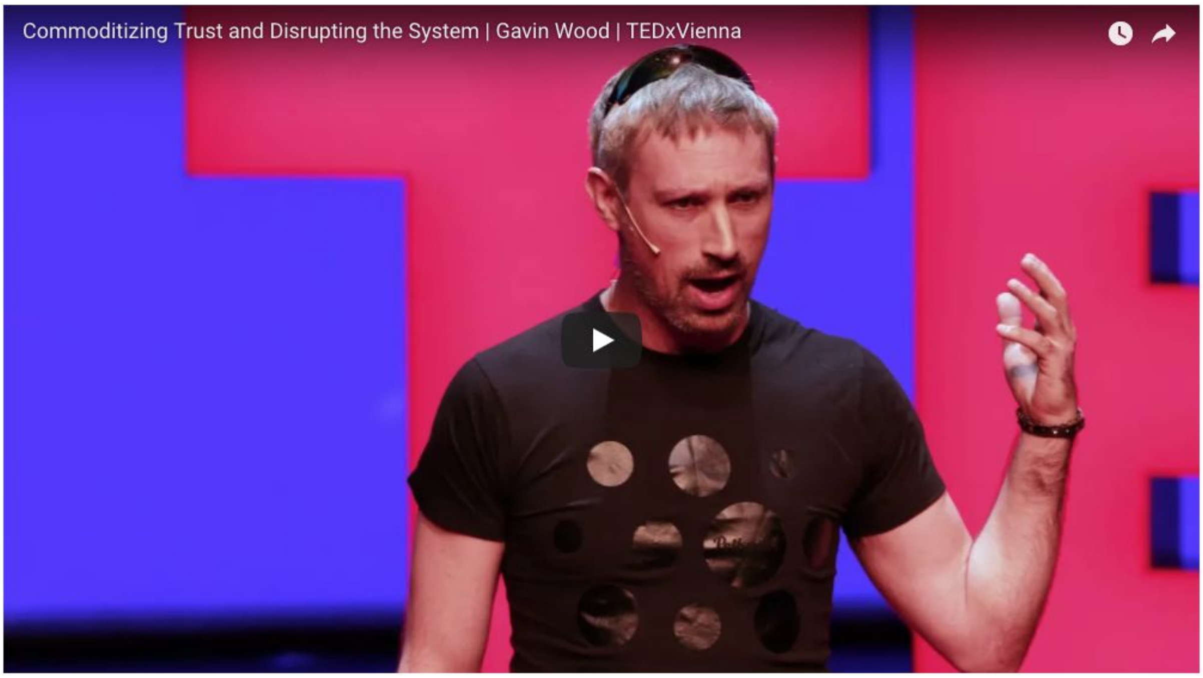
Proof-of-personhood tokens as commodities

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.

With recent developments in blockchain technology and what can be broadly defined as “network-states”, there is now global access to what Gavin Wood describes as a “rule space commons”, within which pseudonym parties could be an ideal medium for proof-of-personhood, as a form of commodity.


Commoditizing Trust and Disrupting the System | Gavin Wood | TEDxVienna

The proof-of-personhood (PoP) tokens are a bit like *IP addresses for people*, you are assigned a new one each month, fully anonymous, untraceable to your previous one.

An online pseudonym parties protocol with independent witnesses as a “web-of-people”

To achieve secure proof-of-personhood, the online pseudonym parties is built on a “web-of-people”, the same concept as “the people” in societal tradition, which in contrast to the idea of a web-of-trust provides global personhood similar to how the nation-state or religion has achieved that. Each pseudonym event, a person is verified by independent sources, in a fully peer-to-peer and pseudo-anonymous global consensus.

Proof-of-personhood tokens as a global medium for identity

The pseudonym event, which happens each month, gives out proof-of-personhood (PoP) tokens to people that are seen as a person by their peers, with 4 people in each pseudonym party (plus people from the BDR token pool that opt-in to the network.) The PoP tokens are disposable after a month, and every pseudonym event gives you a new PoP token on a new private key, not traceable to your previous one.

The pseudonym parties last 15 minutes.

The PoP tokens are mixed, making them fully anonymous

The proof-of-personhood (PoP) tokens that are handed out after the event are mixed, removing any trace to the pseudonym event, including any ties to video data that for each pseudonym has been shared only with a small population of a few people.

The pseudonym event and verification

4 NYM people in each pseudonym party

To avoid psychological biases that come with majority rule, the pseudonym parties are 4 people (plus people from the BDR token pool.)

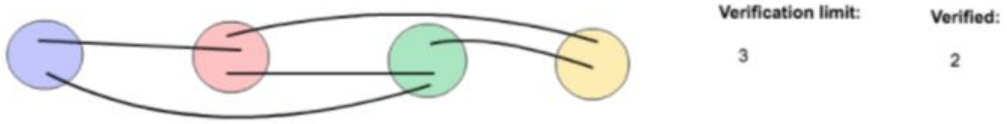
Hour of the event cycles through 24 hours

To be fair to all people on the planet, the exact hour of the event is selected by random, going through 24 different hours over 24 events, and then repeating that cycle.

Using "mem" points to verify each other in the pseudonym parties

The online pseudonym parties is an example of "memetic biometrics", and based on that people stay in joint attention for the entire duration of the pseudonym event, 15 minutes. To be given a proof-of-personhood (PoP) token, each person needs to be verified by their peers. The online pseudonym parties uses a verification game, with the rules that the person you verify also needs to verify you, mutual recognition of personhood. For the protocol to support pseudonym parties where less than 4 people show up or are verified, if 1 pair verifies one another, the limit is 1, if two pairs verify one another, it is raised to 2, if five pairs verify one another, it is raised to three.

In the image below, the colored blobs are 4 people in a pseudonym party. See Appendix for more examples.



To mediate attention in the event, a point system is used to give positive and/or negative rewards. The points are called "mem", from the concept of memes. Each person has 100 mem points for every other person in the party, and can verify another person by giving them 100 mem, and the mem can be used to reward joint attention similar to filling up a fuel meter.

Each person also has 100 negative "mem" points that are used to ostracize a person that month (in case they do not show up, or show up too late, or is not participating). To be ostracized, a person needs to be given 100 negative "mem" points by 100% of the people who are verified.

How bots are kept out of the network

The NYM security token keeps bots out of the network

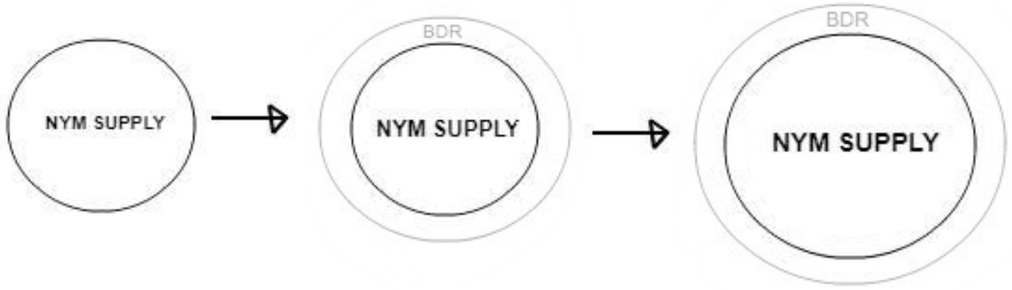
The NYM security token is used to keep bots out of the network, with a deposit of 1 NYM to register for the pseudonym event. The NYM token is burnt unless verified, and so it is abundant if you are a human, as the “online pseudonym parties” network will continuously provide new NYM from verified “border tokens” (BDR) as long as humans want to join the network, and scarce if you are a bot.

Having a separate token to register for the pseudonym event makes it possible to anonymize (by mixing) NYM while using your current PoP token for governance services (dApps), and also to have the “border token” (BDR) as a “virtual border” to keep bots out by going from BDR to NYM and then in the next event a PoP.

Using border (BDR) tokens for people to opt-in to online pseudonym parties

To let new people into the network while keeping bots out, “border tokens” (BDR) are issued each pseudonym month. When below 25% growth, the BDR tokens add people as singles to pseudonym parties, and when above 25% begins to add people as doublets, then as triplets when above 50% growth, and so on. BDR token people lack the the ability to give out mem points, and a person needs to be seen as a person by all NYM people in the pseudonym party that are verified.

When verified, a person is given 1 NYM and their BDR is burnt, and BDR that has not been used to verify a person that pseudonym month is burnt.



Supply of BDR self-regulated by demand

To let the NYM token pool increase, the “border tokens” (BDR) are issued using an algorithm, described below, that self-regulates based on demand (measured from people being verified in the pseudonym event, and not counting bots.)

No upper bound to maximum growth of the NYM token pool

The maximum growth of the NYM token pool is not limited, and is meant to be self-regulated by the network. With 25% growth, 1 BDR token person is in each pseudonym party, together with 4 NYM people, at 50% growth, 2 BDR token people are in the party, 4 BDR at 100% growth, and so on, with no upper limit.

The BDR token people have no "mem" points and can only be verified, with 100% verification needed, 4 NYM people, or in case all four NYM people in the pseudonym party are not verified then from those who are.

Autonomous auction to determine the price of BDR

The BDR, sold via autonomous auctions where the funds are distributed on existing NYM holders, does not give a Proof-of-Personhood (PoP) token, and only after being verified once does it become standard NYM. This prevents people from selling their NYM to bots, then buying BDR.

The supply of BDR that is auctioned out each month is set by how many people were verified from the BDR pool in the previous pseudonym event, and the price is set by demand, where total money invested is divided on total number of tokens, similar to the EOS token sale.

To allow an increase in growth, a second batch of BDR is issued at 1.5x-2.25x the price that was set in the auction, and the size of that batch is self-regulated with the `rate_multiplier` parameter so that there is no need to have either an upper or lower limit to BDR issuance, or the lower limit can be set at 2 BDR which is really low and the upper limit is the maximum integer size (256 bits).

Mechanism to avoid having an upper or lower bound to BDR tokens

To not have an upper or lower limit of how much BDR is issued, the growth increase stacks from one pseudonym event to another. The second batch of BDR, with a lower bound of 2 BDR and then exponential increase based on demand, allows the growth to increase or decrease using a parameter `rate_multiplier`, where `rate_multiplier *= percentage_verified * 2`, so that if more than 50% of the second batch is verified then `rate_multiplier` increases, otherwise it decreases.

`Percentage_verified` is calculated from the mean number of BDR people verified by each pseudonym party.

The second batch is issued as `second_batch * rate_multiplier,` where both `second_batch` and `rate_multiplier` are exponential (`second_batch` is set by how many BDR people were verified from the second batch in the previous pseudonym event, and therefore increases as a result of an increase in `rate_multiplier`.)

To avoid having an upper limit to BDR supply, the first 50% of `second_batch` sold is priced at 1.5x the price of `auctioned_tokens` and the latter 50% at 2.25x the price, so that in the case the `rate_multiplier` mechanism is pushed up too high the biggest cost of that is carried by those who bought from the latter 50% at 2.25x the price.

Proof-of-commitment using selfie-videos (off-state) and relayers

Selling/exchanging keys on a black market to get bot majority in pseudonym parties

Before the pseudonym event, people who have a majority in a pseudonym party could sell their keys to bots, the bots could verify one another by majority, and the people could join the pseudonym parties where the bots were registered and be verified as singles from unsuspecting peers.

That is prevented with "proof-of-commitment", using independent witnesses and selfie-videos, so that each person commits to the pseudonym party they are later assigned to, with the proof that is registered with the witnesses.

Proof-of-commitment with selfie-video hashes

To prevent an attack where a majority of a pseudonym party colludes and sells their private keys to bots, and join as singles in parties where the bots had registered, a hash of a selfie-video, proof-of-commitment, is sent to witnesses, who act as relayers and forward the proof to the pseudonym party once people have been assigned to it.

The proof-of-commitment prevents a person from switching to another party, since proof-of-commitment for all people in that party have already been registered.

Since the witnesses only receive a proof in the form of a hash, and not the selfie-video itself, all personal data is kept off-state, including the hashed proofs, and there is plausible deniability (the verification is fully subjective.)

Enforcing people to both relay, and have others relay

To participate in the pseudonym event, each person needs to both act as a relayer for the selfie-video hash (proof-of-commitment), and have their own selfie-video hash successfully relayed. This incentivizes that proof-of-commitment is generated for the every person in the NYM pool (people who hold the security token that prevent bot attacks.)

During the witness phase for proof-of-commitment, each person can select from 5 people (in sequence, with no knowledge about who the next person will be), relay three hashes, and also flag two scammers. The game theory is that you always gain from flagging a scammer, and you always gain from relaying an honest person.

To be verified for proof-of-commitment, you need to have three relayers, and to be flagged as a scammer, you need to have three flags, and to have successfully relayed others, you need to for three people in total have either relayed people that were verified (three relayers) or flagged people that were marked as scammers (three flags).

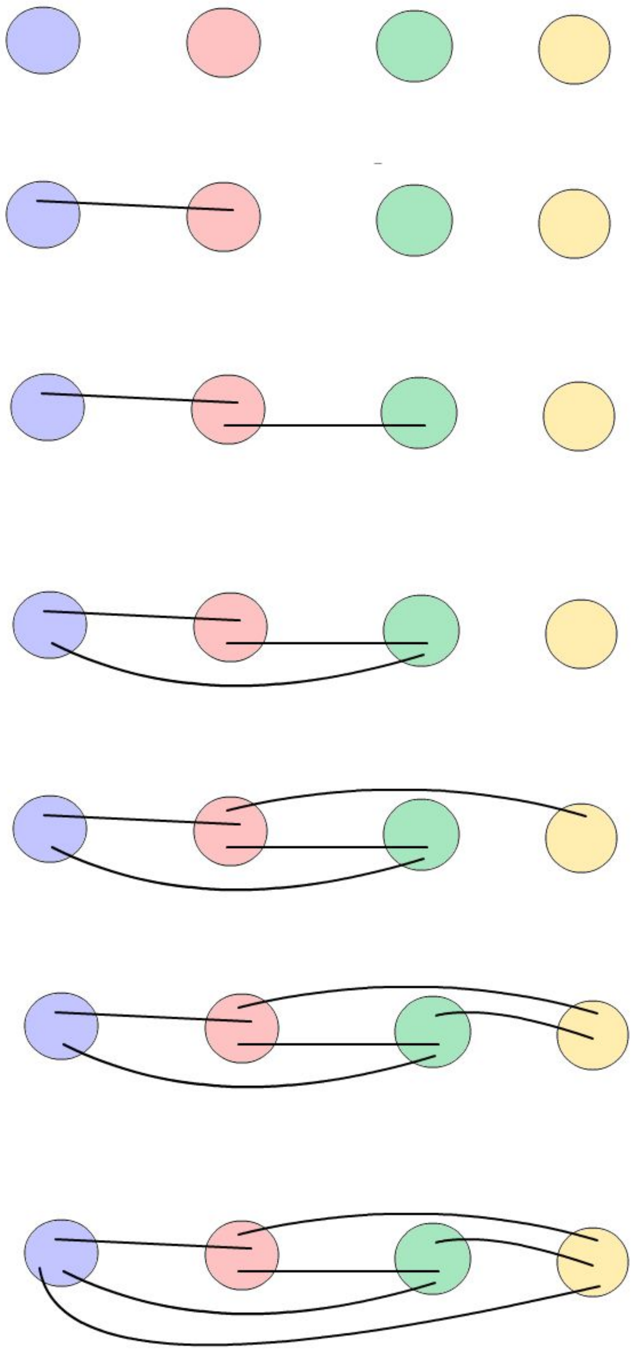
Using off-state keys for “proof-of-commitment” to have “subjective proof”

The idea to use relayers instead of just uploading the hash on-state (objective proof, what can also be called consensus proof), is that all subjective data should be off-state, so that there is plausible deniability.

So that the pseudonym party participants can know that a certain selfie-video hash came from a specific person, a separate set of public-private keys are used, off-state keys, making it possible to have “subjective proofs”. These off-state keys are then used to sign data in ways that each participant can know that which on-state key the data originates from, without having “consensus proof”.

In online pseudonym parties, the on-state keys would be used to generate a symmetric key, in other words, an end-to-end encrypted channel where any data is also authenticated to the people who hold a specific on-state key. That channel would then be used to exchange the off-state public keys, which are then used to sign/encrypt all data in the pseudonym party, including the selfie-video hash.

Appendix



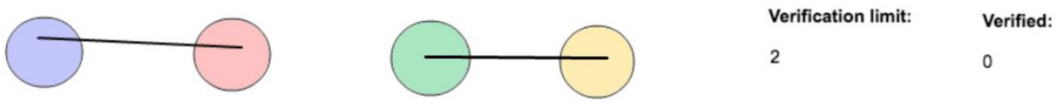
Verification limit:	Verified:
1	0
1	2
2	1
2	3
2	3
3	2
3	4

Appendix 2

On the “stalemate”

The pseudonym parties has a group-size of 4 people, avoiding psychological biases that come with majority rule. A noteworthy game theoretical case is “the stalemate”. The verification game (which uses the “mem” point system to reward joint attention) is balanced so that people can verify one another even if not all four people show up to the pseudonym party, and the more people are verifying one another, the more people each person needs to be verified by (see Appendix).

In the case two pairs verify one another, with no intent of verifying either person from the other pair, then that causes a “stalemate” where no one is verified.



References

Pseudonym Parties: An Offline Foundation for Online Accountability, http://ww.bford.info/log/2007/0327-PseudonymParties.pdf (2008)

Anti-sybil protocol using virtual pseudonym parties, https://www.scribd.com/document/339117426/Anti-sybil-Protocol-Using-Virtual-Pseudonym-Parties (2015)

Proof-of-Personhood: Re-democratizing Permissionless Cryptocurrencies, https://ieeexplore.ieee.org/document/7966966/ (2017)

Behavioural biometrics – the future of security, https://www.techradar.com/news/world-of-tech/future-tech/behavioural-biometrics-the-future-of-security-1302888 (2015)