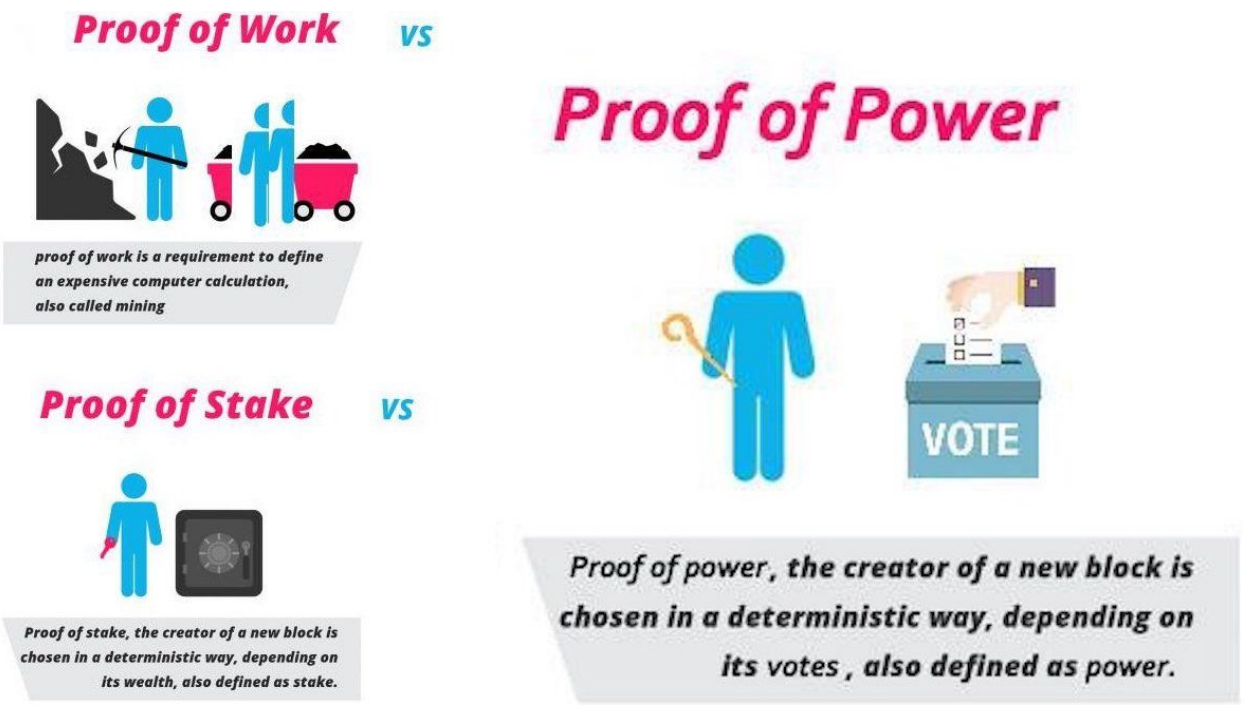
Proof-of-power, using a swarm to select miners through majority consensus

ABSTRACT: In 2008, Craig Wright published the Bitcoin whitepaper[1], and the idea to use proof-of-work as a trusted authority, provably distributed. This Nakamoto consensus allowed the Bitcoin ledger to extend itself in a way that was resilient to censorship as well as to servers being shut down, and in a way where as the security of the network grew, the number of users and therefore the value of the network also grew following Metcalfe´s Law. Bitcoin was the beginning of what can be broadly defined as “network-states”[2], successors to the nation-state consensus.

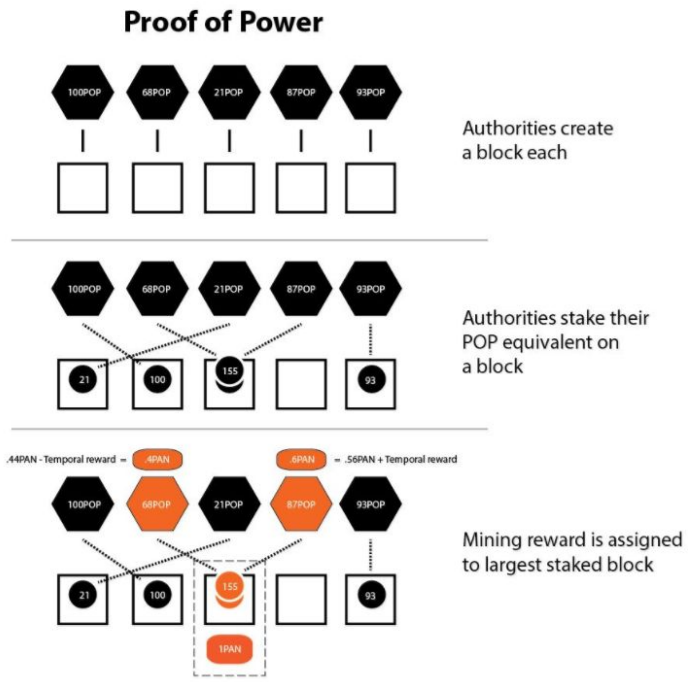
Proof-of-power as a third generation of the Nakamoto consensus, is a natural evolution of the second generation, proof-of-stake, and resolves the issues that people have with previous systems[3], perfectly combining the best of the legacy system of representative democracy, with the advances in permissionless state-technology, market economics and the non-aggression principle (NAP). The overall social consensus is very simple, equivalent to proof-of-stake, but using people-vote instead of stake, validators are "powered" with people-vote using proof-of-suffrage and proof-of-personhood.

Note that proof-of-power is not democracy, there is no mob rule, rather, a permissionless, unbiased state, for what Paul Emile de Puydt conceptualized as Panarchy in 1860[4], a free market for government.



Casper with proof-of-power, “representative consensus-by-bet”

Proof-of-power is interchangeable with proof-of-stake overall, and as an example, it can run on Vlad Zamfir’s Casper. In “representative consensus-by-bet”, people “power up” validators using proof-of-suffrage, and proof-of-personhood, and operate as a swarm or self-organizing collective. The validators then bet with their power, in the consensus-by-bet game that Zamfir invented. Mining rewards are shared between validators, and the people they represent.



The Nakamoto consensus and proof-of-work as miners showing consent (“to feel with a state”)

The Nakamoto consensus (Wright, 2008), is a way to signal consent, and to come together to form a social consensus, not for the the technology itself to agree on a state, but for people to agree on which state to use. Like the Bitcoin whitepaper[1] says, *the longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power.* The main innovation behind Bitcoin and blockchain technology was how to do social consensus, using proof-of-work as a social signal to know which state to organize around, similar to the rhetorical capacity of a president, a shaman, or the display of dominance from a monopoly on violence.

The reward incentive (“mining reward”) makes miners feel with a certain state, and it makes them open-minded towards it, similar to how flowers use pollen to reward bees, allowing a free market for governance services (permissionless state) which is not possible without the use of technology because of genetic bias. With proof-of-power, a third generation of the Nakamoto consensus, the reward incentive is distributed via proof-of-suffrage and proof-of-personhood, to potentially every human on the planet, for maximum oversight of the state (that it follows the protocol) as well as opt-in, explicit, consent to distribute responsibility.[5]

Proof-of-power as a new, voluntary, social contract

Social contracts, as a tool, are cybernetic really, a way to extend social cognition through the use of external state and mediation. Proof-of-power is the first social contract with actual consent, and makes it possible to signal, voluntarily, that you choose to coordinate around a state, allowing the production of global consensus for a “network-state” that can be used to extend social cognition (i.e attention) through the use of governance.

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

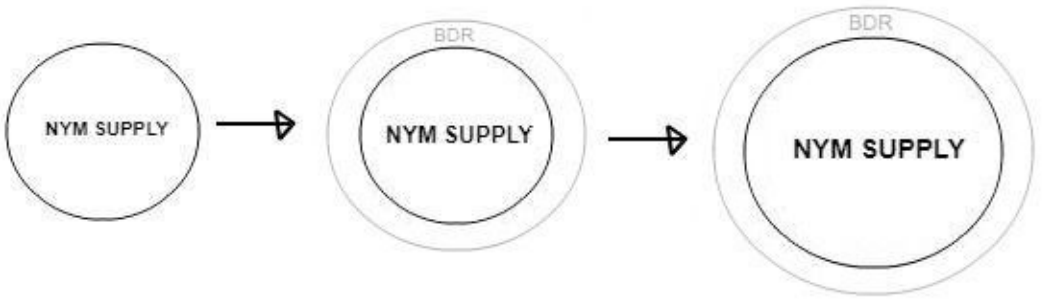
ABSTRACT: Pseudonym Pairs is a dApp for global proof-of-personhood, through monthly pseudonym events that last 20 minutes, where every single person on Earth is randomly paired together with another person, 1-on-1, to verify that the other is a person, in a pseudo-anonymous context. The events provide NYM tokens, global personhood tokens, untraceable from month to month and disposable, a sort of “temporary access tokens” similar to festival bracelets. The proof-of-personhood is that you are with the same person for the whole event.

1-on-1 verification of (pseudo-anonymous) personhood

Within the 1-on-1 pairs, people can socialize as they want, and can be seen as being employed in government positions, expected to stay within the pair for the entire duration of the pseudonym event. The 1-on-1 pairs is the standard organization, requiring mutual verification. In the case of a problem, such as a bot attacker, or, a person not showing up, people can break up their pair, to be assigned to be verified by another pair (2-on-1), similar to how people are verified at the “virtual border”. (see below)

How to opt-in to Pseudonym Pairs

The population is used to secure a "virtual border" around the network, and “border tokens” (BDR) can be bought to apply at the “virtual border” and meet a random pseudonym pair, that verify the person that opts-in. The “border tokens” are distributed through the population, each person can issue 1 BDR, and each time BDR is issued, the ability to issue one more BDR is given to a random person within the pseudonym pool, distributing the ability to invite new people onto the population as a whole, making it possible for the network to accept new people multiple times its population size, so that it can grow from 0 to potentially 5 billion people.



The population sorts themselves into pairs

The pair sorting is invoked by each person, people are sorted into two lists (together forming pairs), and the lists are continuously shuffled with each new person who invokes sortMe(). This sorting mechanism keeps the computational cost per person low, and forms complete pairs regardless of how many of the people who registered choose to commit with sortMe().

```
function sortMe() atTime(0, pseudonymEvent) {
    uint8 idx;
    uint totalSorted = pairingUtility[0].counter + pairingUtility[1].counter;
```

```
        if(totalSorted % 2 == 1) { pairingUtility[0].counter++; idx = 0; }
        else { pairingUtility[1].counter++; idx = 1; }
        totalSorted++;
        pseudonymID[msg.sender] = totalSorted;
        uint pos = pairingUtility[idx].counter;
        uint randomNumber = 1 + labyrinth.generateRandomNumber() % (pos - 1);
        pairingUtility[idx].index[pos].push(randomNumber);
        pairingUtility[idx].index[randomNumber] = pos;
    }
```

Profitability of collusion attacks

The only attack vector I see in Pseudonym Pairs, collusion attacks, they follow an inverse square law, the return decreases more and more the fewer people attack the network.

$$\frac{population}{colluders}^{-2}$$

If 25% of the population attacks the network, they get 4^-2 = 6.25% bots, if 10% of the population attacks the network, 10^-2 = 1%.

References

1) Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf (2008)
2) Teleport - The Network State, https://teleport.org/blog/2015/07/the-network-state/ (2015)
3) Edward Snowden Explains Blockchain to His Lawyer — and the Rest of Us, https://www.aclu.org/blog/privacy-technology/internet-privacy/edward-snowden-explains-blockchain-his-lawyer-and-rest-us (2018)
4) P. E. de Puydt, Panarchy, first published in French in the Revue Trimestrielle, Bruxelles, July 1860.
5) Who is liable for the blockchain? https://www.avocats-mathias.com/technologies-avancees/who-is-liable-for-the-blockchain (2017)