Pseudonym Pairs: a proof-of-unique-human system

The administration of provably unique person registration is the foundation of a social organization that relies on majority consensus among a population of people. This foundation for one-person-one-vote has traditionally been rooted in birth certificates and validation of a unique identity by a police system, but there is technically nothing preventing other game theoretical solutions to “proof-of-person”. Pseudonym Pairs is that new solution, and it is made possible by two of the most groundbreaking technologies of the past century: the internet, and digital ledger technology.

Pseudonym Pairs introduces a new mechanism that is the foundation of the whole system, global simultaneous verification events. The proof-of-unique-human is that the verification takes place at the exact same time, for every person in the population.

Because of the simultaneous events as a central coordination mechanism, Pseudonym Pairs does not have to verify a person to a specific record of that person, like in the traditional population registration system. Instead, it just has to verify that the person is participating in the event. Pseudonym Pairs is therefore able to rely on the population as a whole as the police system that validates identities. This also means that it removes any special control privileges that have been traditionally held by those employed in the police system. In Pseudonym Pairs, each person has the exact same amount of control, with no exceptions.

The verification is delegated to individual people, and organized through pairs, each person verifying another randomly selected person. The people using the system are entrusted the responsibility of judging one another.

This new mechanism, the global simultaneous verification events, that lets people be verified as a unique person without being verified to a specific record of that person, also means the proof-of-person can be anonymous. This means that the system can “reset” from month to month, without any traceability of a person from month to month. When compared to the traditional population registry system, people in Pseudonym Pairs are “born” every month, and “die” every month. The system operates completely compartmentalized from month to month.

Verification in the pairs has to be mutual. In case there is any conflict, a general problem solving mechanism is used. People can break up their pair, and be assigned under another pair each. These other pairs act similar to a “court”, and both people in the pair have to verify the person they were assigned. This mechanism is how the system can use pairs.

This general problem solving mechanism is identical to how people join the population to begin with. Similar to the traditional population registry, Pseudonym Pairs has a “border” around it. This border is the main security mechanism, just like in the traditional system. To get across this border, people have to “immigrate”, by being assigned to a random pair that acts as a “court” to verify that the immigrant is a unique person. This border prevents computer scripts from taking over the system.

To prevent attacks on the immigration mechanism by flooding the system with trillions of fake immigration requests, which could be used to make collusion attacks worse, immigrants have to acquire a permit. These are distributed by that any person in the population can give out one. To allow for mass-immigration during the launch of the Pseudonym Pairs population, there is also a rule that every time anyone registers to immigrate, a random person is given the ability to give out one more, so that the population can grow by more than doubling.

The system is very simple, and implemented as a computer program in a structure like the one below, except that it also maps the data to each month.

```
    uint entropy; // Block hash for first block in period

    mapping (address => bool) registered;
    mapping (address => uint) pair;
    address[] pairIndex;
    uint shuffled;
    mapping (uint => bool[2]) verified;
    mapping (uint => bool) disputed;
    mapping (address => uint) court;
    address[] courtIndex;
    mapping (uint => bool[2]) judgement;

    function register() {
        require(registered[msg.sender] == false);
        pairIndex.push(msg.sender);
        registered[msg.sender] = true;
    }
    function immigrate() {
        require(registered[msg.sender] == false);
        court[msg.sender] = courtIndex.length;
        courtIndex.push(msg.sender);
        registered[msg.sender] = true;
    }
    function shuffle() {
        uint randomNumber = shuffled + entropy%(pairIndex.length - shuffled);
        entropy = sha3(entropy, shuffler[randomNumber]);
        (pairIndex[shuffled], pairIndex[randomNumber]) =  (pairIndex[randomNumber], pairIndex[shuffled]);
        shuffled++;
        pair[pairIndex[shuffled]] = shuffled/2;
    }
```

Pseudonym Pairs is vulnerable to one type of attack, collusion attacks. These are relatively harmless because the probability of gaining control of a pair is low. The exact success of collusion attacks is *percentageColluding*^2, it decreases with an inverse square relationship as the total colluding population decreases. For example, if 10% of the entire population colludes, they get 1% fake accounts. Another way to look at it, each attacker gets *percentageColluding* more than they would otherwise. Collusion attacks are allowed as they cannot be completely prevented.

Another attack vector is man in the middle attacks. These can be defended against perfectly, but require an extra step. The ideal defense adds a "handshake" to secure the video channel. The mechanism for this, the pair schedules a “pre-meeting” at a random time before the event, by agreeing on a random number using a commit-reveal scheme. Their channel can be proven secure by validating that they both got the same number. The probability of the man in the middle attacking this in a way that both peers get the same number is *1/numberSize*. This defense is as "Turing safe" (same difficulty for breaking Turing test) as the actual event itself.

The central theme in Pseudonym Pairs is the coordination of the simultaneous global events. This has to be coordinated by a “leader” everyone can trust, a game theoretical problem that was solved with majority consensus historically, first implemented in digital form by Craig Wright. This “leader” also needs high bureaucratic capacity, why digital ledger technology is one of two groundbreaking technologies that enable Pseudonym Pairs.