Identity Based Consensus for Self-Governing Systems

Defence and Security Doctoral Symposium 2020

Data on a Blockchain is grouped in blocks, each of which contains multiple transactions. Blocks have to be resistant to replication over a ‘byzantine’ network. On those networks, writers can act maliciously in different ways:

- Attempt to store incorrect/invalid transactions on the Blockchain
- Use one input multiple times (‘double spend’)  
- Censor the Blockchain by systematically withholding particular transactions

The selection of members responsible for data replication is a challenge in decentralised record-keeping systems.

### ‘Byzantine’ and ‘Sybil’ Actors

Lampert et al. (1982) show how a decentralised system (S) behaves when actors (m, n) spread incorrect or conflicting information, or withhold information. They describe how a system tolerates a limited fraction of these actors, often referred to as ‘byzantine’ actors. Doucure (2002) describes how a single faulty entity (m), often referred to as a ‘sybil’ actor, can gain control of a redundant network by ‘presenting multiple identities’ (sm).

### Membership Selection Strategies

- **Proof-of-Work (Bitcoin; Nakamoto, 2008):** Select a ‘miner’ to validate transactional data and to act as an ordering authority of transactions. Participants qualify as miners by expending computing resources.
- **Proof-of-Stake (Conceptual Bitcoin forum post, later formalised by King et al., 2012):** Being able to prove ownership of currency determines the difficulty of creating a new block, thus making participants who have held larger quantities of currency for longer more influential.
- **Delegated Proof-of-Stake (Larimer, 2016):** A variation to proof-of-stake, introducing a delegation scheme, in which ‘shareholders may delegate their voting power to a representative’.
- **Proof-of-Authority: Membership selection ‘by policy’, i.e. through a pre-defined list of privileged actors (i.e. Schwartz et al., 2014, Hearn and Brown, 2019, Libra Association, 2020).**

### Arithmetic Properties of Personhood Tokens

Members can endorse or discourage gatekeeping authorities via a broadcast message. These actions directly impact the reputation of the authority and thus the personhood score the authority can grant. Per authority A, a vector of endorsement scores da and a vector of discouragement scores de are kept publicly. Participants add to either of the vectors via a message they broadcast. This means that the influence a participant can exert on the reputation of another authority is proportional to their reputation.

### Future Work

The protocol proposed lacks formalisation, intuition suggests that the concept of evolving constituencies, backed by identity authorities, that can be added to and removed from a network dynamically, has merit.

Future work must focus on formalising the protocol to evaluate its robustness. A formal approach will ultimately prove or disprove its advantages over existing membership selection protocols, in the context of attacks.

### Constituencies Evolve Over Time

Through messages of approval and rejection, authorities (A) are voted onto the system and removed from it. Authorities issue personhood tokens to their constituents (C).

### Counteracting Sybil Attacks

A single malevolent authority can flood the network with sybil actors, who can disrupt any record-keeping and record-keeping activity on the network, permanently. We therefore need to implement countermeasures:

- **Temporal normalisation can mitigate sybil attacks that go along with a sudden influx of bogus identities**
- **An overall constituency size ceiling that limits the total number of identities, created by one authority, is introduced.**
- **A quantitative safeguard enforcing diversity is introduced.** This gives reputational signals from diverse sources more weight.
- **A lower bound for personhood scores is introduced.**