Dolev-Reischuk: Any deterministic protocol requires $O(n^2)$ communication.

Idea: One party $p$ that does not receive any message. $P$ will disagree with other honest parties.

Q: Can we obtain a sub-quadratic communication protocol if we assume randomization?

$n = 1$ million parties.

1000 parties.

"Every party to every other party": $O(n^2)$

"Every party in the committee sends to every other party": $O(kn)$

Coin $c \cdot (256 \text{ bit})$ "Common coin".

$HC(id, p, c) \Rightarrow$ if this value is "small enough," then the party is in the committee.

If we set $k$ as the expected committee size, since every party is elected uniformly & independently,
at random, we can argue that the committee size \((\frac{1}{3}) < \text{committee} < (1 + \delta) \frac{1}{3}\) except with probability \(\epsilon^{-O(\delta^2)}\) (Chernoff bound).

If we start off with \(\frac{1}{3} - \epsilon\) Byzantine parties in the entire population, then the committee will have \(\frac{1}{3}\) Byzantine parties.

---

**Protocol**

Secure against a static adversary.

- Elect committee \(\mathcal{C}\) of size \(k\). (no communication)
- Run the agreement protocol within the committee. \(O(k^2)\) communication
- All parties learn the output by communicating with sufficiently many committee members. \(O(\text{nk})\) communication

\[
O(nk + k^2) = O(nk) = \]

Identities of committee members are public:
- An adversary can attack all committee members
- Bribe
Adaptivity of the adversary.

Static: Adversary corrupts up to $t$ parties at the beginning of the protocol.

Adaptive: Adversary corrupts parties during the execution.
- A party can be corrupted at the start of a round.

Mobile:

Bitcoin: Static or adaptively secure?

✓

"A miner useful now is not useful at a later point."

✗

I do not know whether I am "in the committee" until I mine first.

(Vari.)

Once I do win, I can prove to the world that I am the winner.

An adversary cannot modify the contents of the block (even by corrupting me).

Randomized / fair

Verifiable random function:

\[ \begin{align*}
VRF(\text{sk}, r) \quad \rightarrow \quad \text{O/P} \quad \rightarrow \quad \text{VRF prove} (\text{sk}, \text{O/P}) \quad \rightarrow \text{O/P} \\
\text{VRF verify} (\text{O/P}, \text{pk}) \quad \rightarrow \text{1, 0}
\end{align*} \]
(→ Uniformly random.
→ Verifiable.
→ Unique.

Change secret keys frequently: Key evolving signatures.

( pk_i, sk_i^x ) \quad \text{Round } x \quad \Downarrow

( pk_i, sk_i^{x+1} ) \quad \text{Round } x+1

→ If I am elected, create a local msg/proposal.
→ Evolve my key sk_i^x \rightarrow sk_i^{x+1}.
→ Delete sk_i^x.
→ Send the proposal to everyone.

Player - replaceability:
→ Use subquadratic comm protocol from earlier.
→ Elect a different committee in each round.

vote North Status.
Player-replaceability: Sub-quadratic comm + adaptive adversary.