**Byzantine broadcast**

no parties, \( t \) corrupt/malicious/Byzantine

---

**Commander**

(attack)

---

**Agreement**: No two honest generals take different actions.

**Termination**: Every honest general eventually either attacks or retreats.

**Validity**: If commander is honest, then output commander's order.

Intuition:
- If some honest party receives a value, share it with all honest parties.
- Eventually, one honest party learns \( \star \)

\[ \Downarrow \]
all honest parties learn \( \star \).

\[
\text{Round 1: Commander (sender) sends value } v \text{ to all parties.}
\]

\[
\text{Round 2: If I receive a value from the commander, then I send it to all parties.}
\]

\[
\text{Commit: If I receive exactly one value } v, \text{ then output } v.\]

\[
\text{output } 1.
\]

\[
\text{Round 1:}
\]

\[
\begin{array}{c}
\text{K} \\
\end{array}
\]

\[
\text{v, v'}
\]

\[
\text{c}
\]
Round 2:

\[ v, v' \]
\[ v' \]
\[ v, v' \]
\[ v \]
\[ v' \]
\[ v' \]

Attack 2:

Round 1:

\[ K \]

Round 2:

Solution:

Round 2: Do not consider commander's value.

If \( \leq 1 \) Byzantine:

\[ \geq 2 \] Byzantine parties.

Round 1:

\[ k \]
\[ \text{No messages.} \]
Round 2: nothing.

We can tolerate Byzantine faults.

Signature chains: \( p_1, p_2, \ldots, p_n \)

\[ \langle \langle \langle \langle V, \frac{1}{p_i}, \frac{2}{s}, \frac{3}{s}, \ldots \rangle \rangle \rangle \langle m \rangle \]

What is a valid signature chain:
- in round \( i \), the signature chain received should be length \( i \).
- the signers in this chain should be distinct.
- signature should be valid.

Distinct signature chains: "value" should be distinct

Protocol:
\[ \sum_{i=1}^{\infty} \langle \langle \langle \langle V, 1 \rangle \rangle \rangle \langle 0 \rangle \rangle \]
\[ \text{tends } \langle \langle V, 1 \rangle \rangle \text{ to all} \]
Round $n$: server $i$ sends $s_i$, other parties.

Rounds 2, ..., $t+1$: If a party receives a valid signature chain in round $(i-1)$ and it has not broadcasted 22 signature chains, then it appends to the chain & broadcasts.

Commit: if a party receives exactly 1 valid signature chain with value $v$, output $v$.

Agreement:

Termination: easy.

Validity:

Proof:
Agreement: If an honest party receives value $v$, all honest parties receive it.
Rounds 1, ..., $t$: $h'$ will send it to everyone.
$t+1$: the chain has length $t+1$.
If some honest party $h'$ in this chain, $h'$ would have sent it to everyone.
\( n, t \) Byzantine \( t \leq n-2 \)

Latency: \( t+1 \) rounds \( k \) rounds \( O(n^{2-k}) \)

Communication complexity:
- \( \frac{2n^2}{2n^2 + t} \)
- \( n^2 \) all-to-all
- \( \leq t \) message size

1. Are \( O(t) \) rounds necessary?
2. Is \( O(n^2 t) \) communication necessary?

Dolev-Reischuk: \( O(t^2) \) lower bound\(^\dagger\)

\[^\dagger\text{(deterministic)}\]

Any BB protocol needs at least \( \frac{t^2}{4} \) messages.

To prove: \( \leq \frac{(t/2)^2}{4} \)

If a protocol fewer messages, 3 out honest party who does not receive any message.

If \( \leq \frac{(t/2)^2}{4} \) messages are sent, consider any set \( V \) of size \( t \) parties. If each party in \( V \)
receives $\geq \frac{t}{2}$ msgs, then $\geq \left(\frac{t}{2}\right)^2$ msgs.

If at least one party in $V$ that receives
$\leq \frac{t}{2}$ msgs.

$\leq \frac{t}{2}$ different parties.

\[ \text{World 1: Designed sender is honest:} \]
\[ \text{Sender sends 0;} \]

Byzantine parties in $V$ behave honestly except:
(i) they ignore the first $\frac{t}{2}$ messages sent to them.
(ii) they do not send any messages to each other.

Honest parties should output 0.