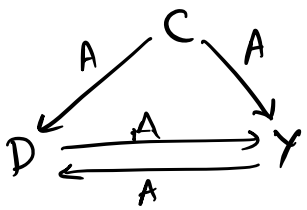
| Digital sig | Problem | Tolerance | Latency | Comm'n comp | Network | Det / Rand? |
|---|---|---|---|---|---|---|
| Nakamoto | SMR. | $< n/2^*$ | $k$ (fail. prob $e^{-k}$) | $O(n^2 k)$ | sync. | Rand. |
| Dolev-Strong | BB | $< n-1$ ($< n$) | $t+1$ | $O(n^2 t)$ | sync. | Det. |
| $O(1)$-round protocol | BB/BA | $< n/2$ | ~10 round (expected) | $O(n^3)$ ↓ $O(n^2)$ threshold sigs. | sync | Rand. |

⇓

Is this amt of communication necessary?

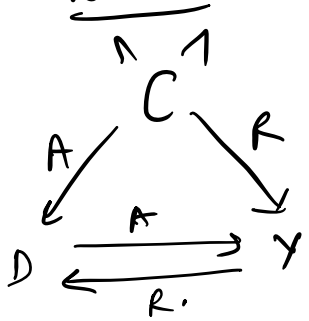
---

1980 : Lamport, Shostak, Pease:

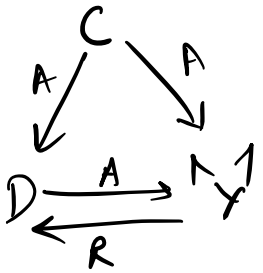



W/o digital sign, we cannot tolerate 1 out of 3 corruption. ($t < n/2$)

World 1




World 2




FLM bound

From D's perspective, it does not know whether C or Y are lying.

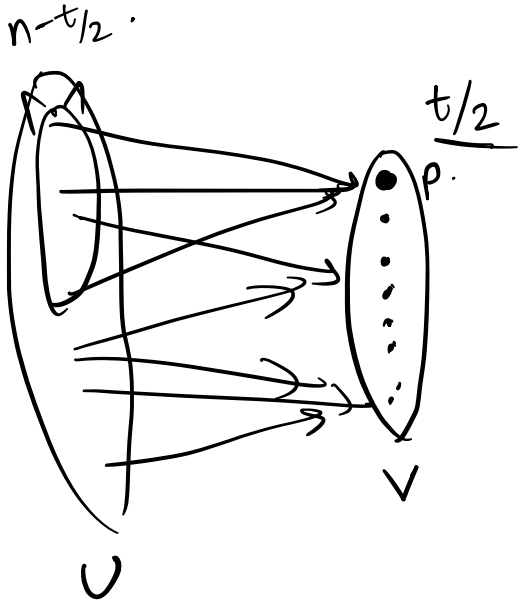
---

## Dolev-Reischuk bound:

Any deterministic BB protocol should have an execution that requires $> (\frac{t}{2})^2$ messages sent by non-faulty (honest) parties.

If some protocol requires $\leq (\frac{t}{2})^2$ communication then we can show an execution where the agreement property fails.
(termination)

To show: If a protocol has $\leq (\frac{t}{2})^2$ communication; There exists a party that does not receive any message for some execution.

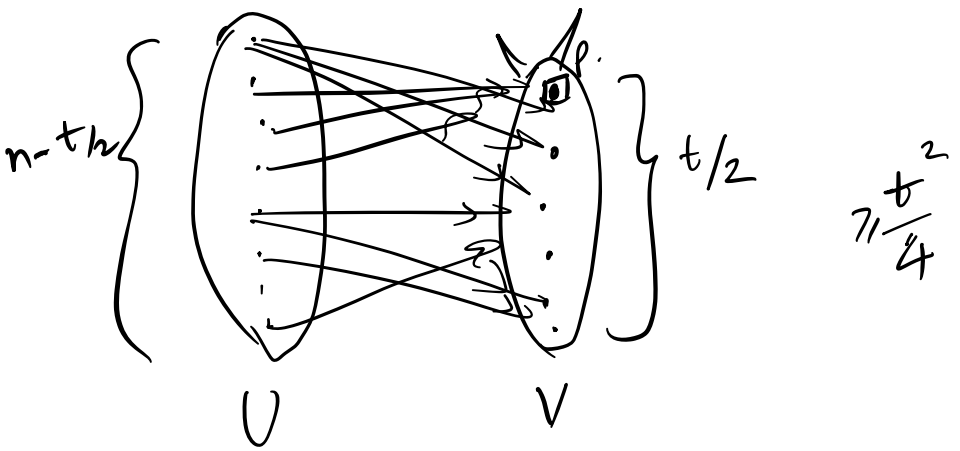


If each party in V receives $\geq \frac{t}{2}$ messages from parties in U, then the protocol sends. $\geq \left(\frac{t}{2}\right)^2$ messages.

If you come up with a protocol with lesser comm$^n$, then $\exists$ a party $p \in V$ who receives $< \frac{t}{2}$ messages.

---

Wald 1: $t/2$ parties that output 1 when they receive no messages.




$\pi \frac{t^2}{4}$

Set of parties in V are Byzantine. They follow the protocol specification except:

(i) They are not going to send messages to each other

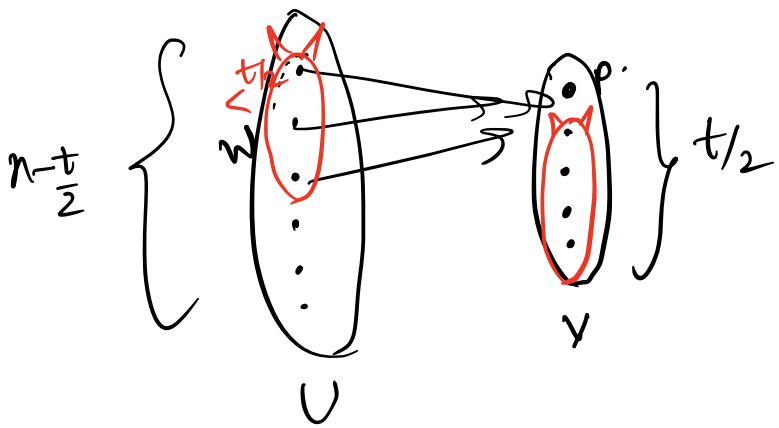
(ii) They will ignore the first $t/2$ messages sent to them.

The protocol state ~~sat~~ has $< t$ Byzantine faults.

So, agreement, validity, & termination should hold.

If the sender sends a 0 as input, all honest parties output 0 (validity).
+ termination.

World 2:




If $< \frac{t^2}{4}$ messages are sent from U to V,

$\exists$ a party $P \in V$ who receives fewer than $t/2$ messages.

- Everyone in V except party P are Byzantine.

Byz Parties in V behave exactly the same as in world 1.

(i) Ignore the first $t/2$ messages received from V

(ii) They will not send messages to parties in V.

Parties in W will not send any messages to P; otherwise W will follow protocol specification.

From the perspective of parties in $U \setminus W$, they have the same view as in World 1.

Hence, they output 0.

P does not receive any message. Party p will output 1 if it receives no messages.

Hence, an agreement violation.

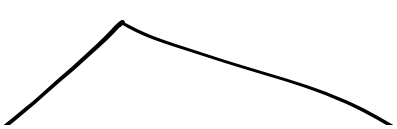
---

Network assumptions:

Synchrony: If an honest party p sends a message to a party p', it will arrive within a known bounded delay $\Delta$.

Asynchrony: If p sends a message to p', it will eventually arrive.

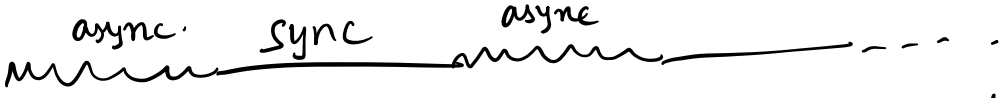
FLP: "For a deterministic asynchronous protocol, we cannot have agreement, validity, & termination that can tolerate $> 0$ faults."



Randomized async protocols

Relaxing asynchrony defn. (partial synchrony) (DLS '88)

Partial sync: There are periods of asynchrony & synchrony.




1. Unknown $\Delta$ world: N/w is sync but we don't know the bounded n/w dely.

2. Unknown Global Stabilization time (GST): (unknown)
Until GST, n/w is asynchronous. After GST n/w has $\Delta$- bounded delay. (known)

---

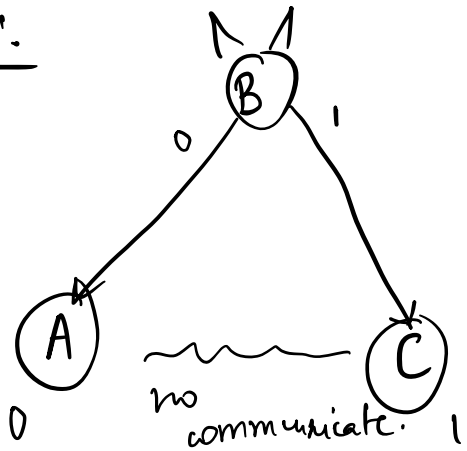
DLS lower bound: (1988):

Dwork Lynch Stockmeyer

Under partial synchrony, it is impossible to tolerate $t \geq \frac{n}{3}$ Byzantine faults.

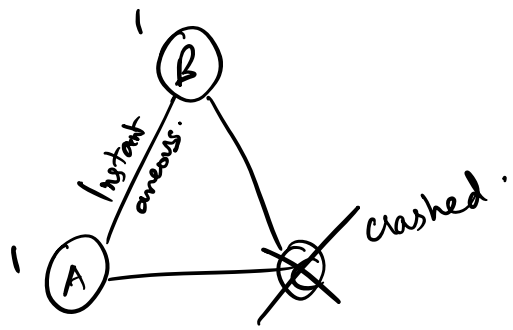
$n \geq 3t+1$


Intuition:



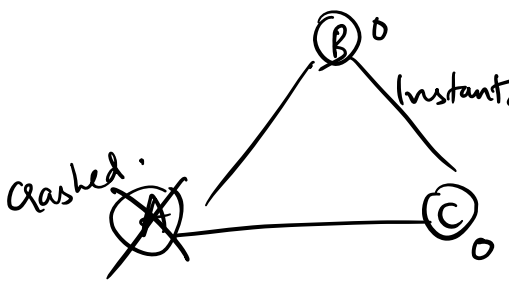

---

World 1: A & B start with input 1.



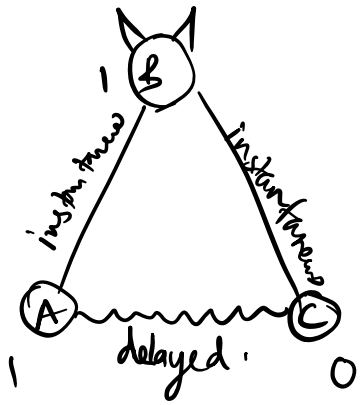

By validity & termination A & B output 1.

World 2: B & C start with input 0.




By validity & termination B & C output 0.

World 3: A & C are honest. B is Byzantine.




B's behavior: It behaves with A exactly the same as in world 1.

" C " "

" 2

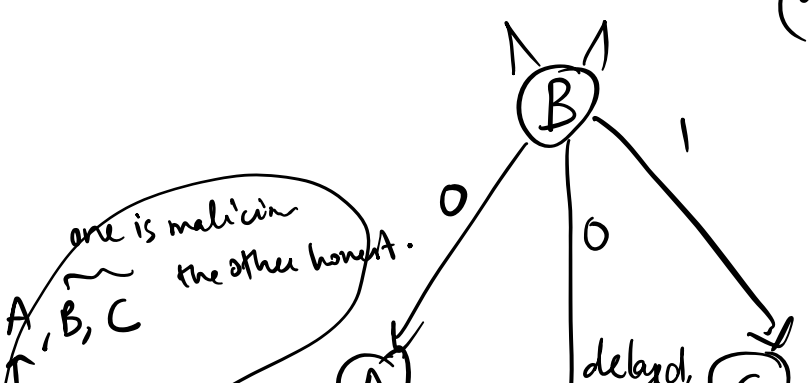
A: Its view in world 3 & world 1 are indistinguish
So A will output 1.

C: Its view in world 3 & world 2 are indistinguish
So C will output 0.

Agreement violation.

---

What happens if we have four parties? (one fault)




$n = 3t+1$

$2t+1$


SMR/BA world

| | Async (Det) | (Rand) Async / Partial sync | Sync |
|---|---|---|---|
| Dig. Sign. (PKI) | $t \geq 1$ is not possible. (FLP) | $t \geq n/3$ is not possible (DLS) | $t < n/2$ (O(1) round protocol) |
| No PKI | FLP | $t \geq n/3$ is not possible. (DLS, no PKI). FLM. | Cannot tolerate $t \geq n/3$ faults. (FLM bound) |

PBFT: Practical Byzantine Fault Tolerance

↓

Ethereum, Tendermint, Algorand.

Castro & Liskov, 1999.

↓

MSR. (CCF)

↓

Turing award.

Primary-backup paradigm:

primary/leader: drive progress in the system

Replicas: ensure agreement (safety) holds. & primary is doing its job correctly.

pros: In the good case, progress - streamlined.

cons: subtle attacks - reordering.

## Steady-State Protocol $n = 3t+1$

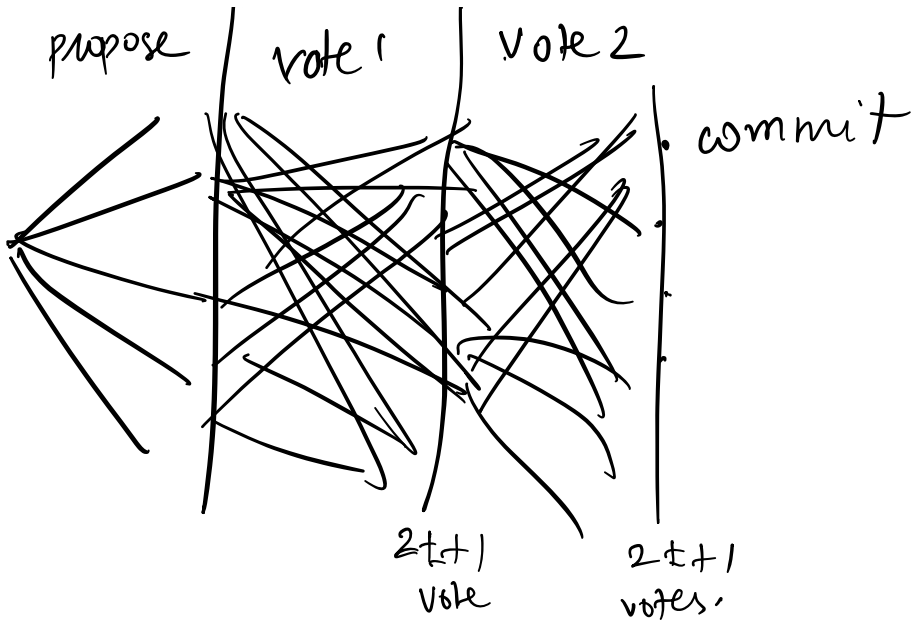
**Propose**: Leader $p_i$ proposes $\langle propose, B, v \rangle$

- $B$: value / cmd / txn.
- $v$: view.

**Vote 1**: Send vote 1 $\langle vote\ 1, B, v, \rangle$ to all replicas. "if it is safe to vote for it".

**Vote 2**: If replica $i$ collects $2t+1$ vote 1's for the same value $B$, then we say replica $i$ is locked on $(B, v)$.
Replica $i$ sends a $\langle vote\ 2, B, v \rangle$

**Commit**: Replica $i$ collects $2t+1$ vote 2's for value $B$, then it commits $B$.




If I commit a value B, I received 2t+1 vote 2 messages:

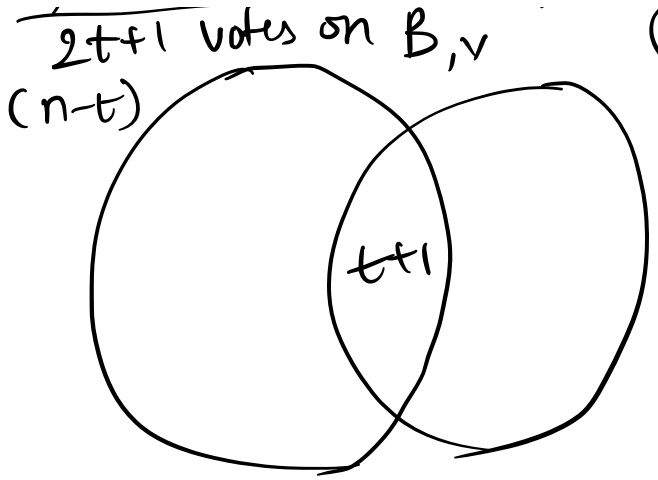
- There are t+1 honest replicas who have locked on value (B, v). They will guard the safety of my commit.

---

<u>vote 1 guarantees uniqueness within a view</u>

If I lock on a value B, then no other honest party can lock on a value $B' \neq B$ in the same view.

Quorum intersection




$n = 3t+1$

$n+t$ votes.

$(4t+1)$

For both B & B' to receive a quorum of $2t+1$ vote 1's, we need $4t+2$ votes.

---

Q: Is this possible?

- Some honest party $h$ commits B'
- some other honest party is locked on B in the same view.

A: $h$ receives $2t+1$ vote 2 messages. $t+1$ honest parties are locked on B'. Due to uniqueness from the first

round of votes, no party can be locked on to $(B, v) \neq (B, v)$.

---

If some party commits $B$ in view $v$,

- $\geq t+1$ parties locked on $(B, v)$ in view $v$. (second round of votes).
- no other party locked on $B' \neq B$ in view $v$ (first round of votes)

---

## View-change protocol: Change the leader

"Blame the leader"

- send $\langle \text{blame}, v, \text{lock}_i \rangle$ to the next leader.

## New leader:

On receiving $2t+1$ blame messages (locks), start a new view.

↳ If some party has committed value B, then the new leader can only propose B (agreement / safety).

↳ The new leader should be able to propose the value that has been committed earlier (liveness / termination)