Part 3: Constitutional Consensus for Democratic Governance

Part 3: Constitutional consensus for democratic governance

1. **Digital democracy, Paxos, and Consensus**
2. Constitutional consensus
3. Digital democratic governance

Democracy and Consensus go together

- No dictator
- Need distributed agreement on democratic decisions

Democratic governance vs Consensus

- Democratic governance is based on majority or super-majority votes
- Consensus algorithms use majority or super-majority

Q: Are they the same?

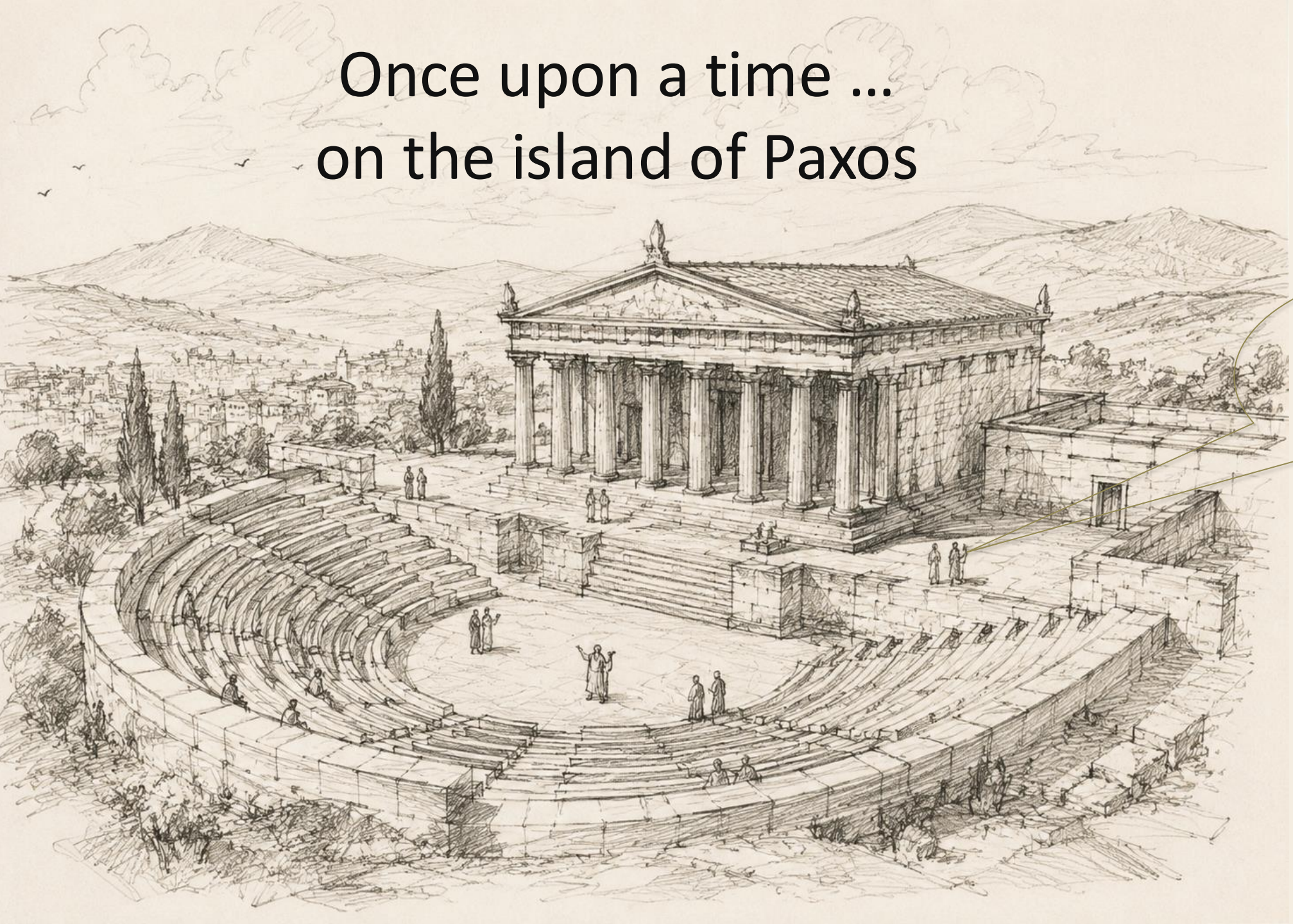
Democratic governance vs Consensus

Q: Are they the same?

A1: Consensus super-majorities do not reflect volitional agreement of participants, whereas democratic governance does.

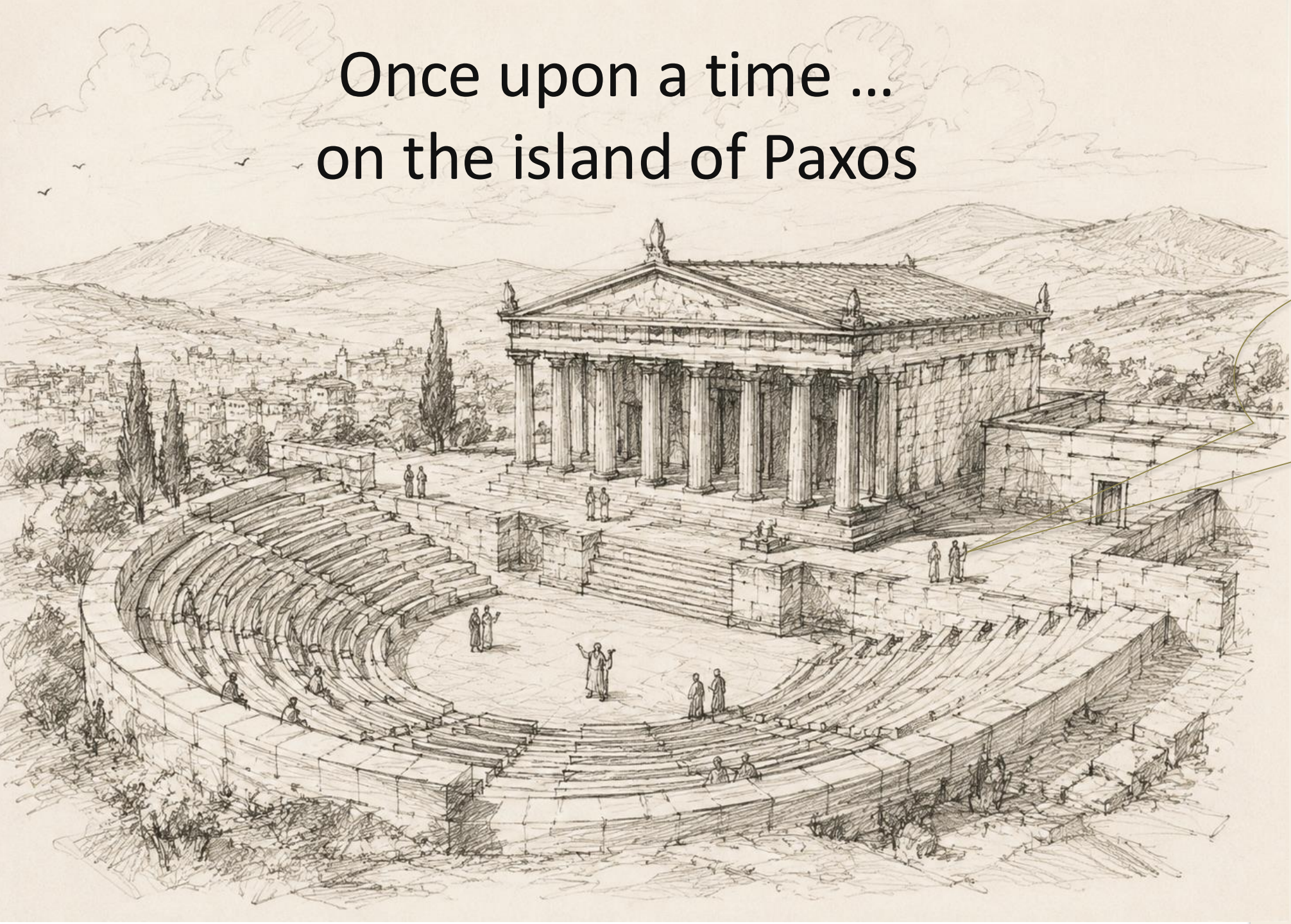
A2: For a majoritarian democratic decision to be accepted by everyone (including the losing minority), we need consensus that it is valid.

Once upon a time …
on the island of Paxos



155: The olive tax is 3 drachmas per ton

Once upon a time …
on the island of Paxos



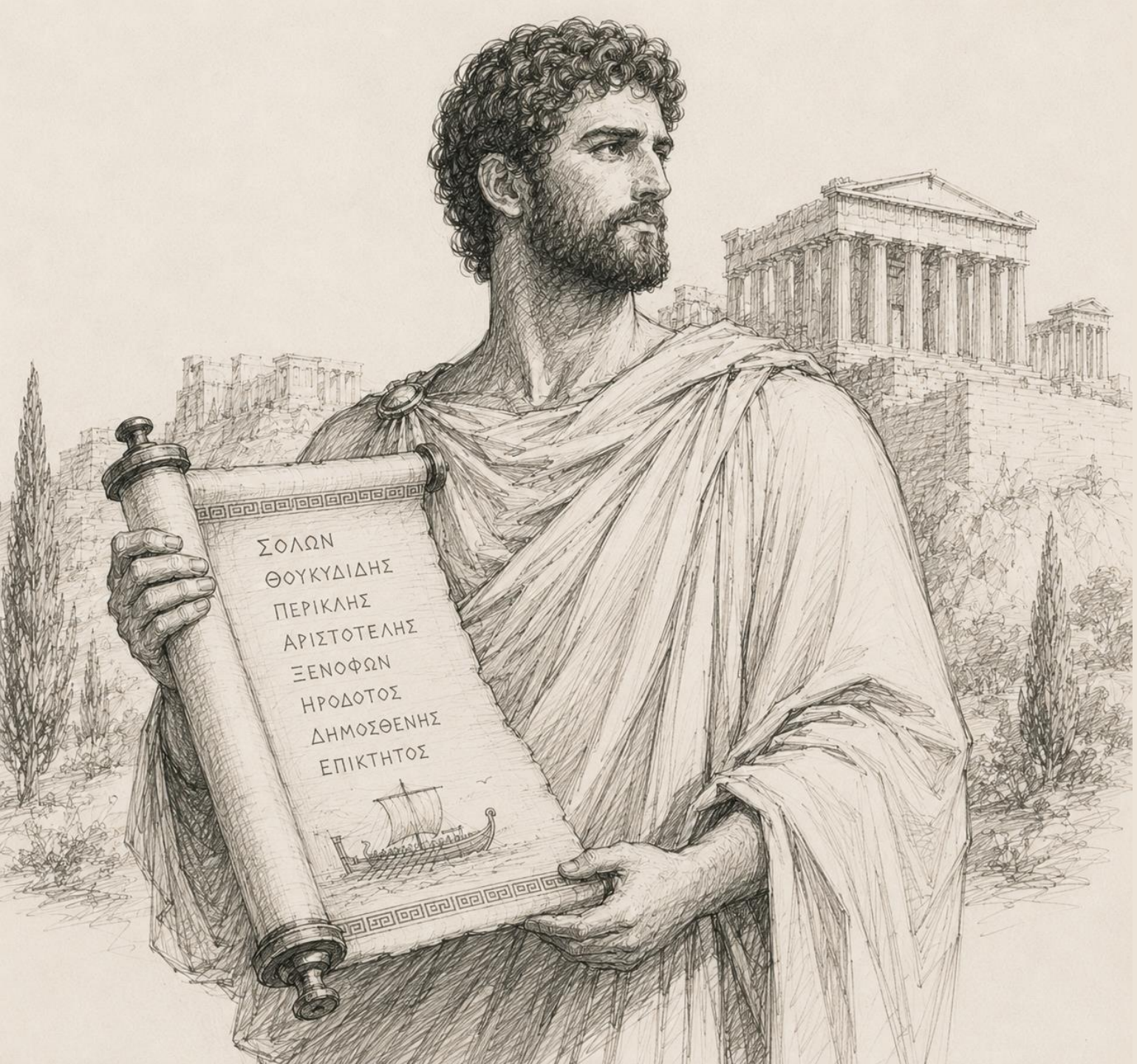
3252: Στρωνγ is now a legislator

Digital democracy using Consensus

1. Agree on a sequence of transactions
   - Consistent parliamentary record as in Paxos
2. Agree on the constitution and its amendments
   - Still a challenge in Paxos

From “The Part Time Parlament” Lamport 1998

In fact, the mechanism for choosing legislators led to the downfall of the parliamentary system in Paxos.



Because of a scribe’s error, a decree that was supposed to honor sailors who had drowned in a shipwreck instead declared them to be the only members of Parliament.

From “The Part Time Parlament” Lamport 1998

In fact, the mechanism for choosing legislators led to the downfall of the Parliamentary system in Paxos.

…

Its passage prevented any new decrees from being passed— including the decrees proposed to correct the mistake. Government in Paxos came to a halt.

Democracy needs a constitution

Q: Consensus that a democratic decision is valid — How?

A: With a constitution defining a valid democratic decision

Q: Democratically amending the constitution itself — How?

A: A difficult question…which we try to answer here

Constitutional Consensus principles

1. Vision: A consensus protocol to be used by grassroots democratic communities, grassroots cooperatives
2. Executed by *volitional* agents = people with smartphones → participants = users
3. Supports nascent communities → *quiescent*, efficient also at low transaction volume (Morpheus Consensus)
4. Supports constitutional *amendments* → Epochs, one per constitution

Part 3: Constitutional consensus for democratic governance

1. Digital democracy, Paxos, and Consensus
2. **Constitutional consensus**
3. Digital democratic governance

The model

- Set of agents Π
  - Each has a unique key-pair
  - Correct agents follow the protocol
  - Others are *faulty* or *Byzantine*
- Eventual synchrony
  - Bounded message delay δ after GST

The constitution

- Rules for consensus decisions
  - In our case: our protocol, 3 amendable parameters
- Rules for amending the constitution
  - Later

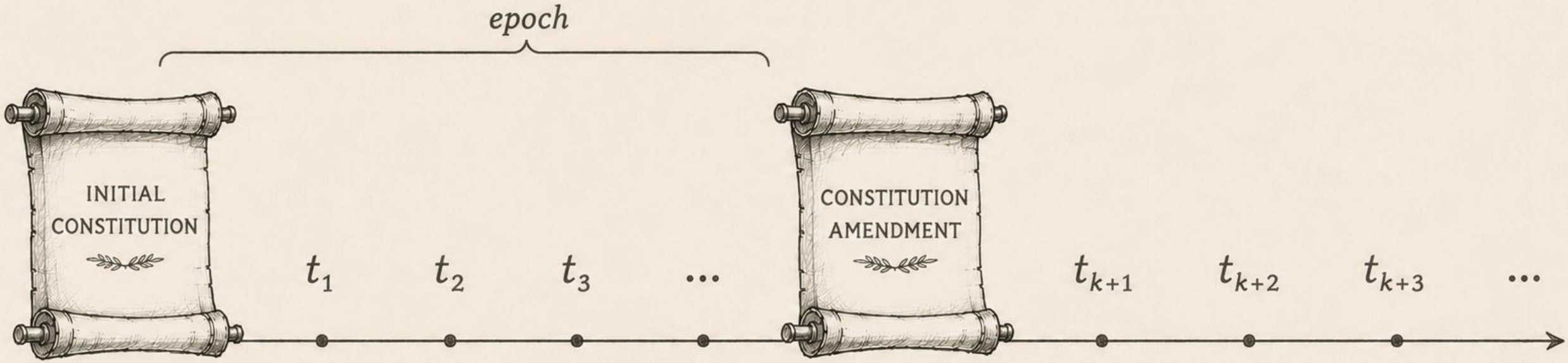
Amendable constitution parameters

- $P \subseteq \Pi$ – set of participants
- $\frac{1}{2} \leq \sigma < 1$ – super-majority threshold
  - Capturing Byzantines and sybils
- Δ – estimated latency bound after GST
  - Among correct participants

Constitution safety and liveness

- A constitution (P, σ, Δ) is *safe* if
  - P is the set of agents running the protocol;
  - there is a correct σ-supermajority in P , and every σ-supermajority in P includes a correct majority.
- The constitution is *live* if
  - #of faulty participants $f < \frac{1}{3}n$, and
  - $\delta \leq \Delta$

Constitutional consensus epochs

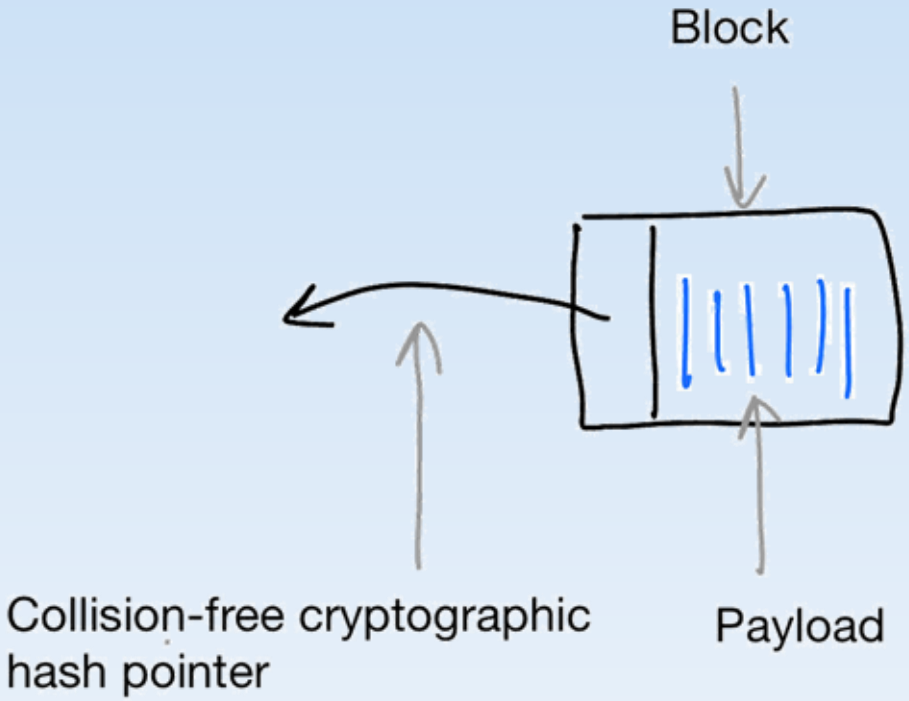


Every agent *p* sees a subsequence consisting of epochs whose amendments include *p.*

Single epoch protocol

- Invoked with a given safe and live constitution
- Orders transactions
- Ends upon ordering of a valid constitution amendment
- Based on a *blocklace* data structure
  - Generalization of blockchain

A Blockchain Block

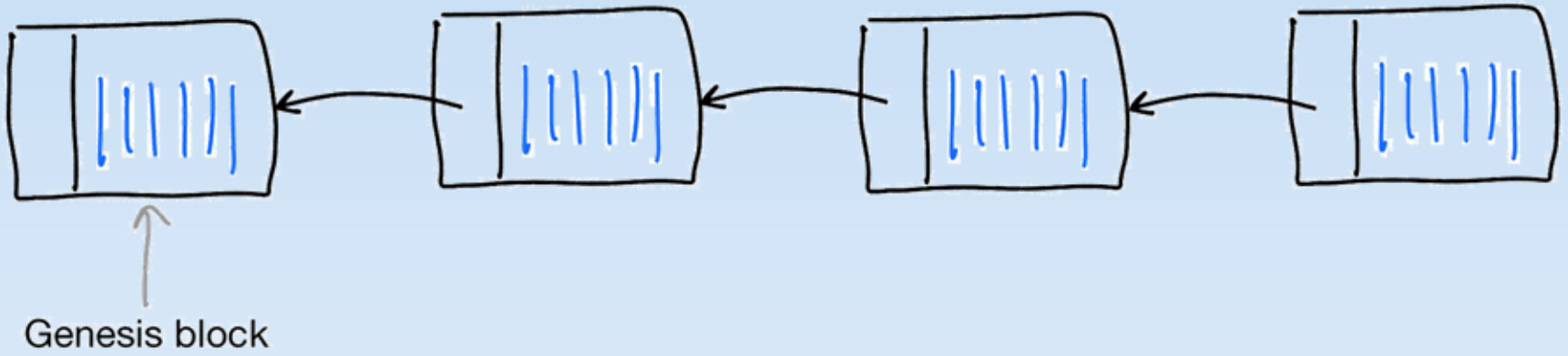


Hash pointer: the hash value $h(x)$ of another block x.

Collision-free: $x \neq y \rightarrow h(x) \neq h(y)$.

Cryptographic: Cannot compute x given $h(x)$; hence no cycles.

A Blockchain

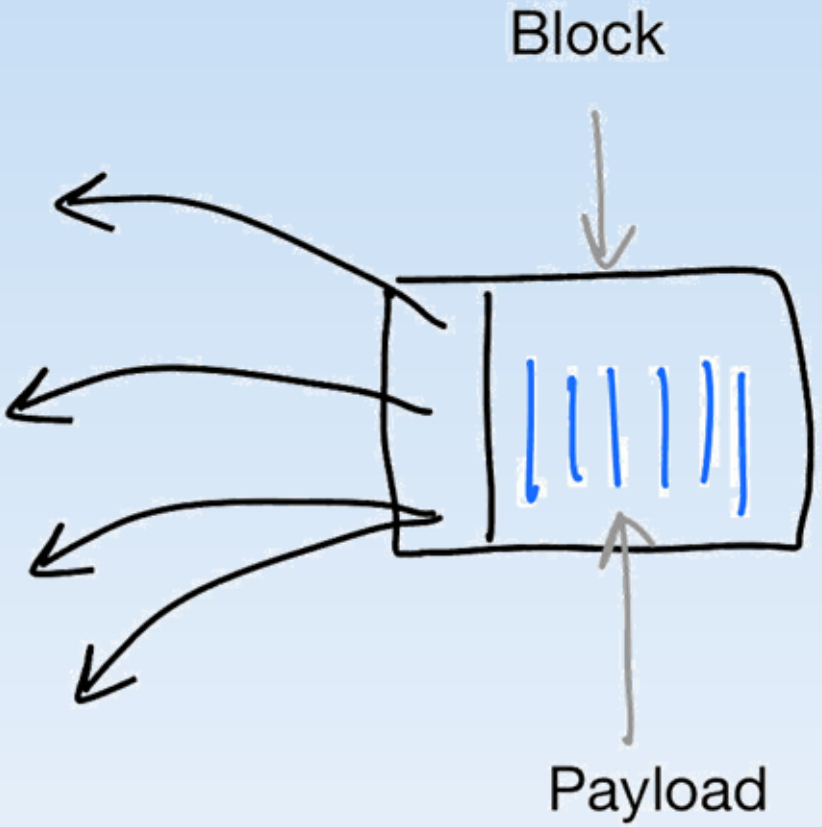


Tamper-proof: payload or pointer cannot be changed without being detected

Non-repudiable: Signed block or payload cannot be repudiated by signatory

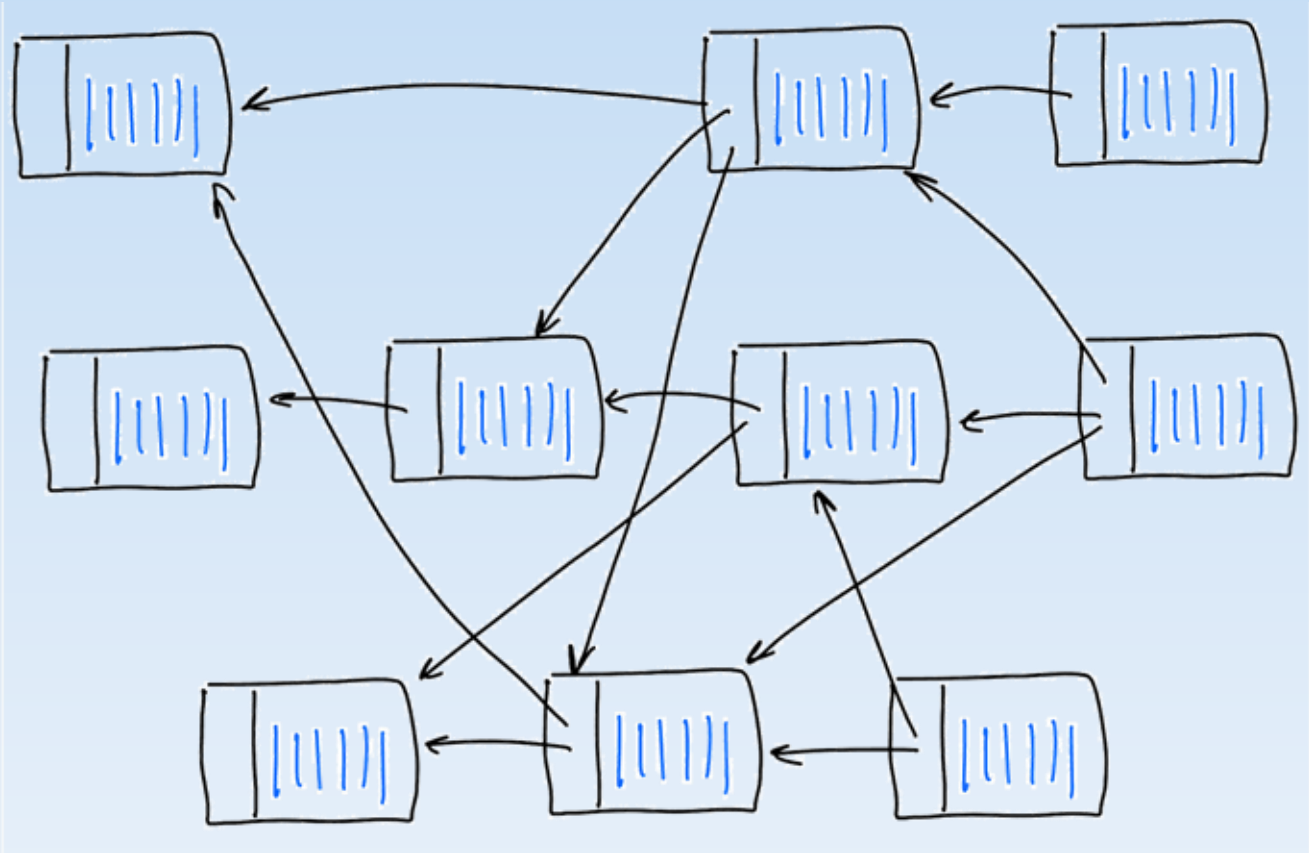
Totally-ordered

A Blocklace Block



hash pointers

A Blocklace

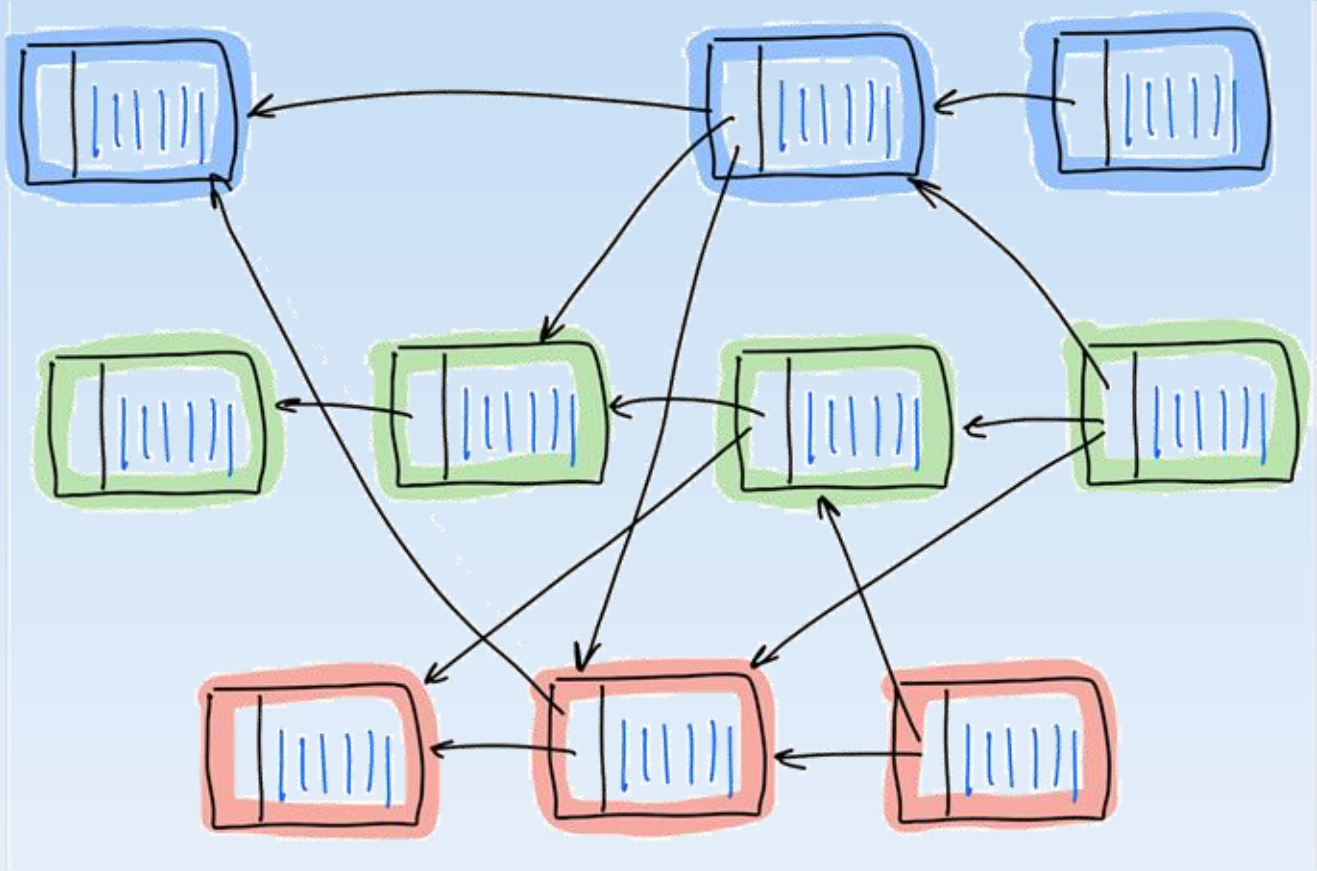


Tamper-proof

Non-repudiable - signed

~~**Totally**~~ **Partially-ordered** – induces a Directed Acyclic Graph (DAG)

A Blocklace

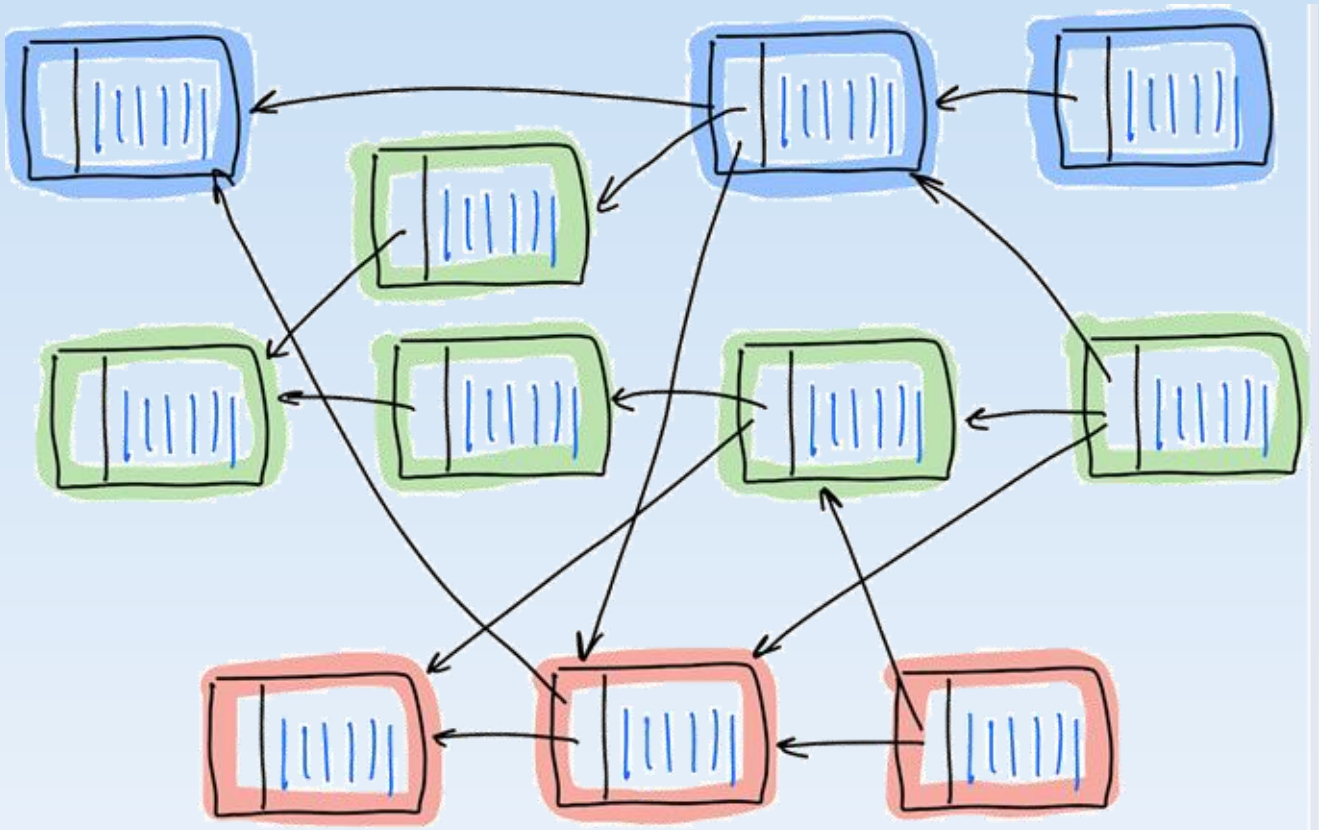


Tamper-proof

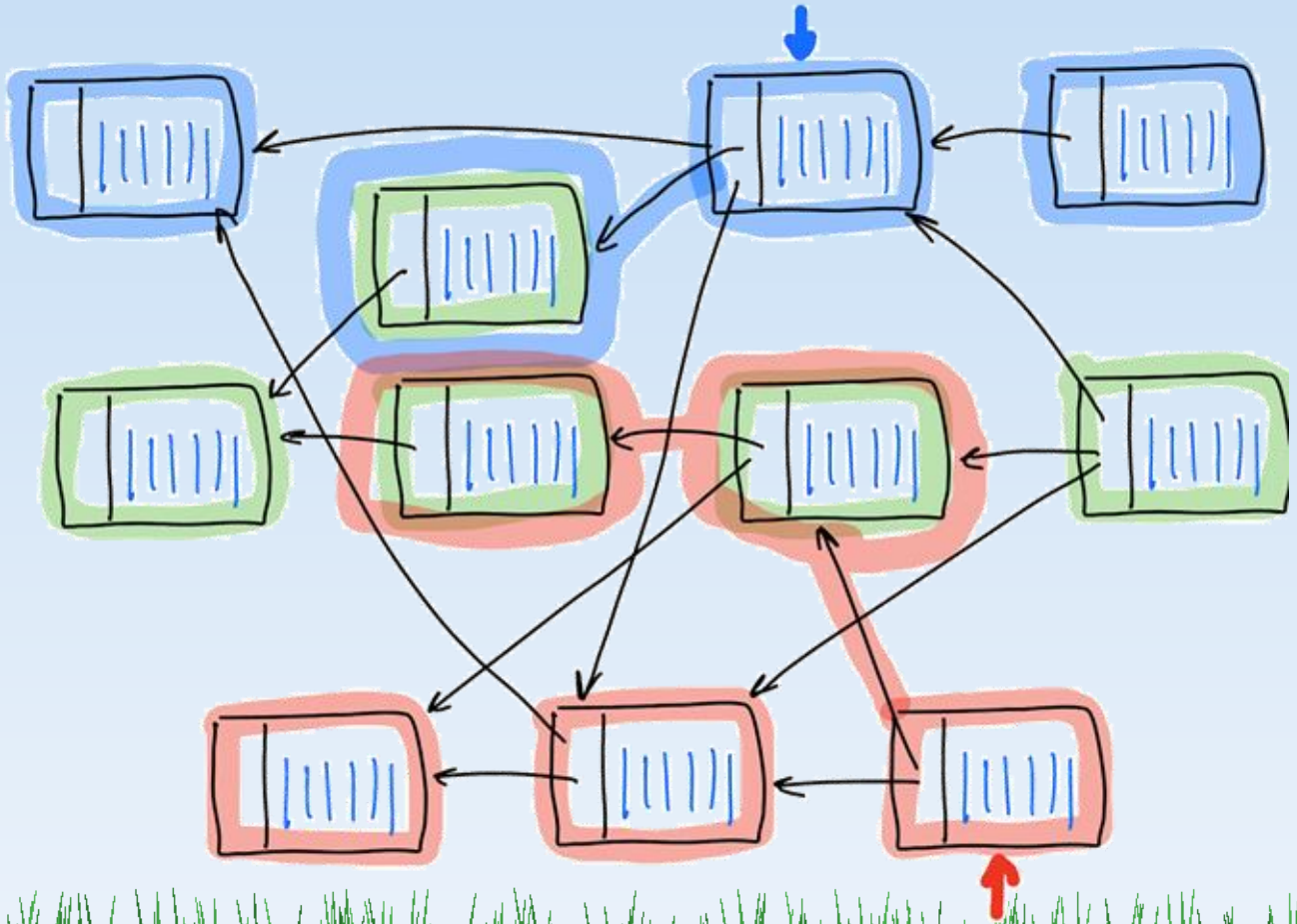
Non-repudiable - signed

~~**Totally**~~ **Partially-ordered** – induces a Directed Acyclic Graph (DAG)

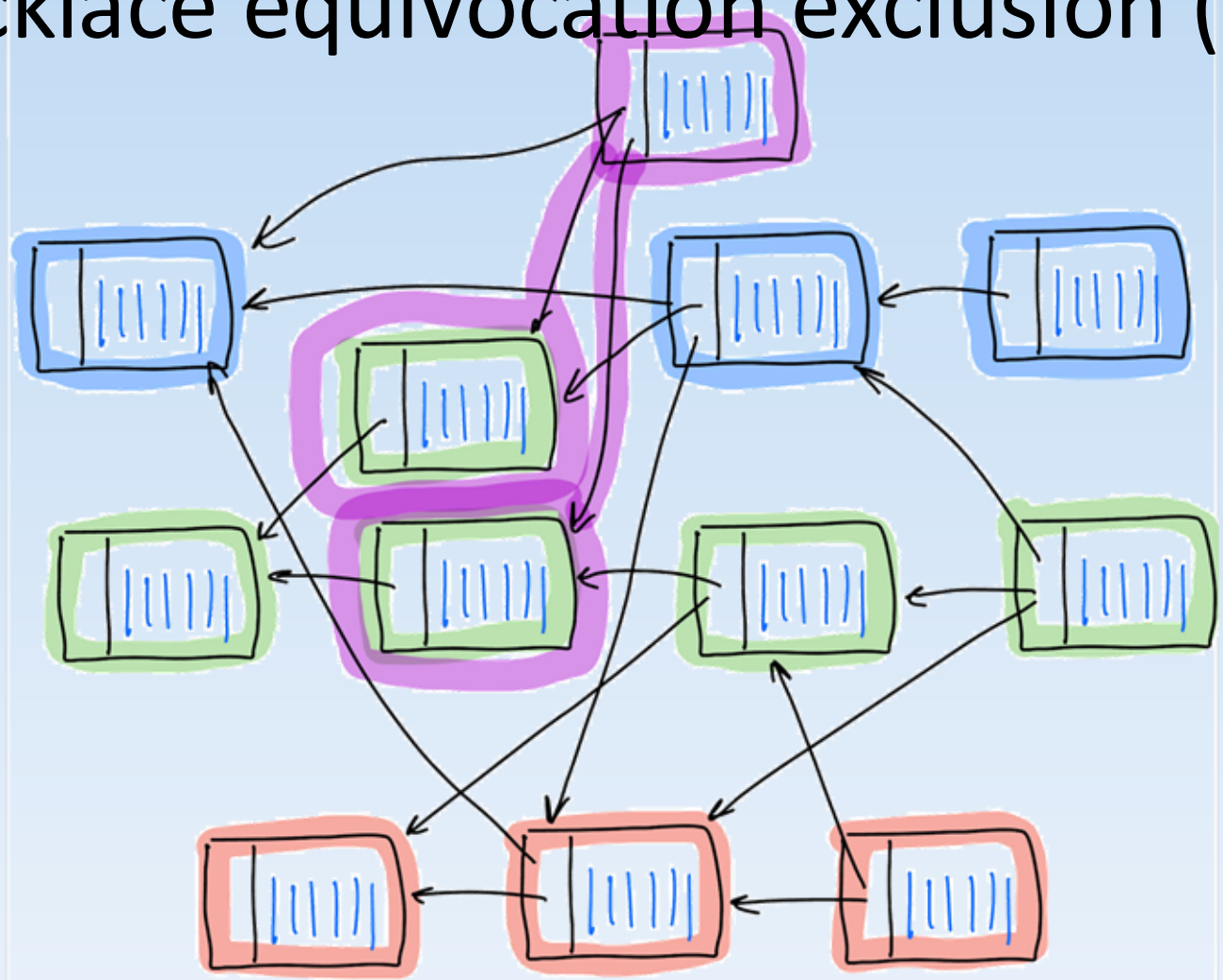
Blocklace equivocation exclusion (Cordial Miners)



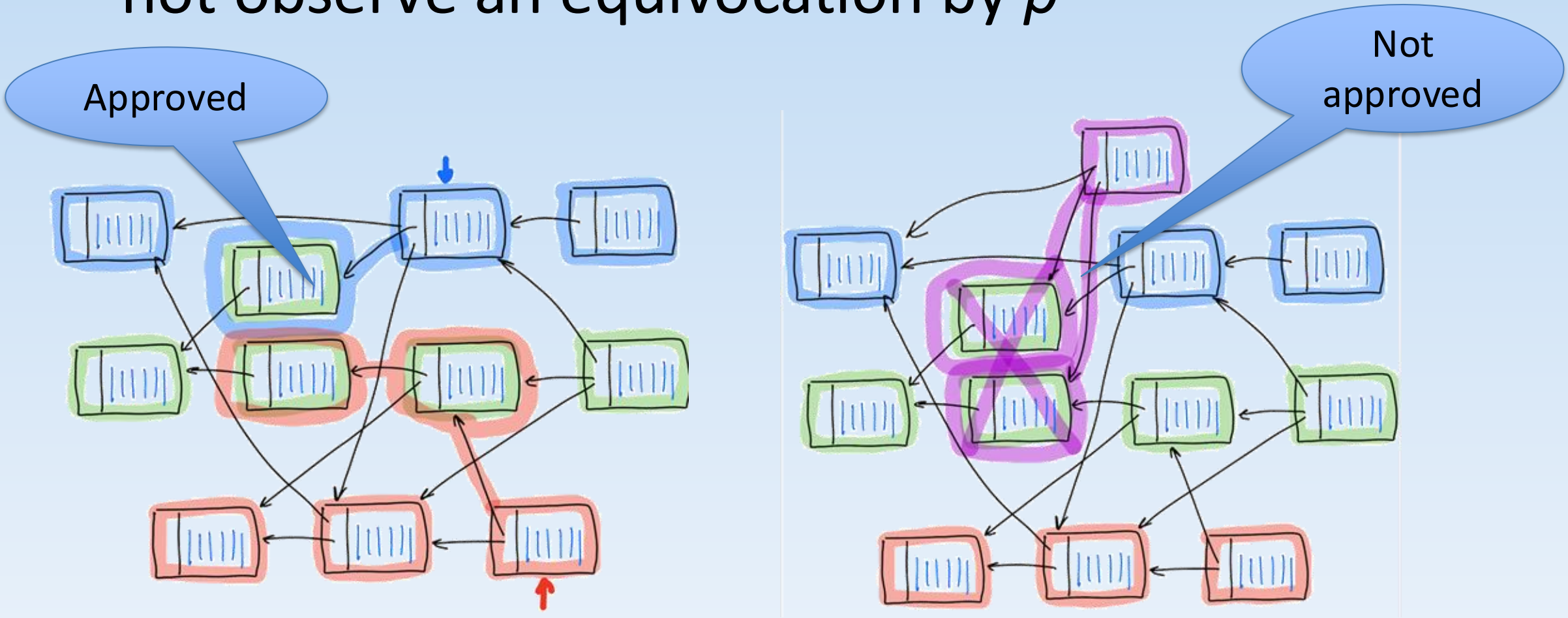
Blocklace equivocation exclusion (Cordial Miners)



Blocklace equivocation exclusion (Cordial Miners)



A block *approves* a *p*-block if it does not observe an equivocation by *p*

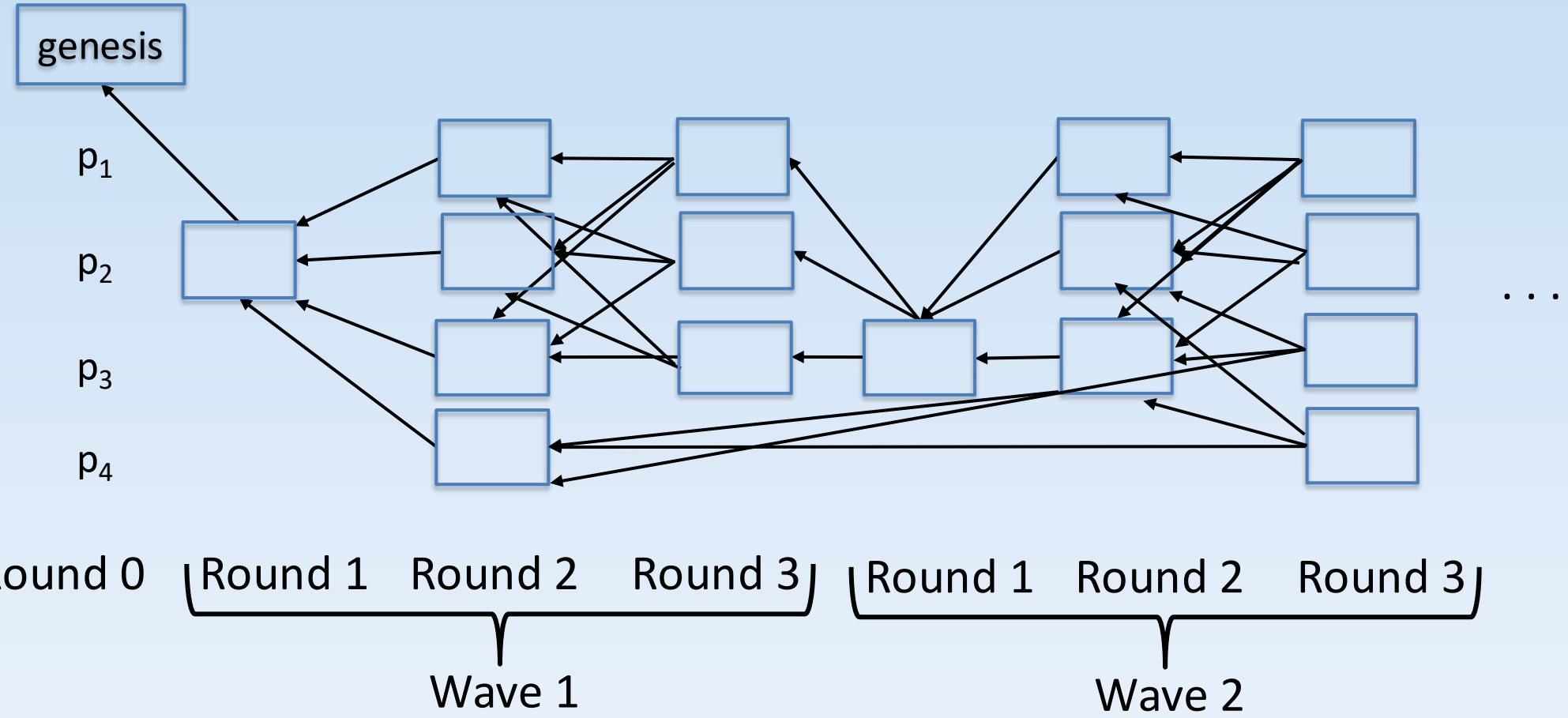


Blocklace eventual consistency

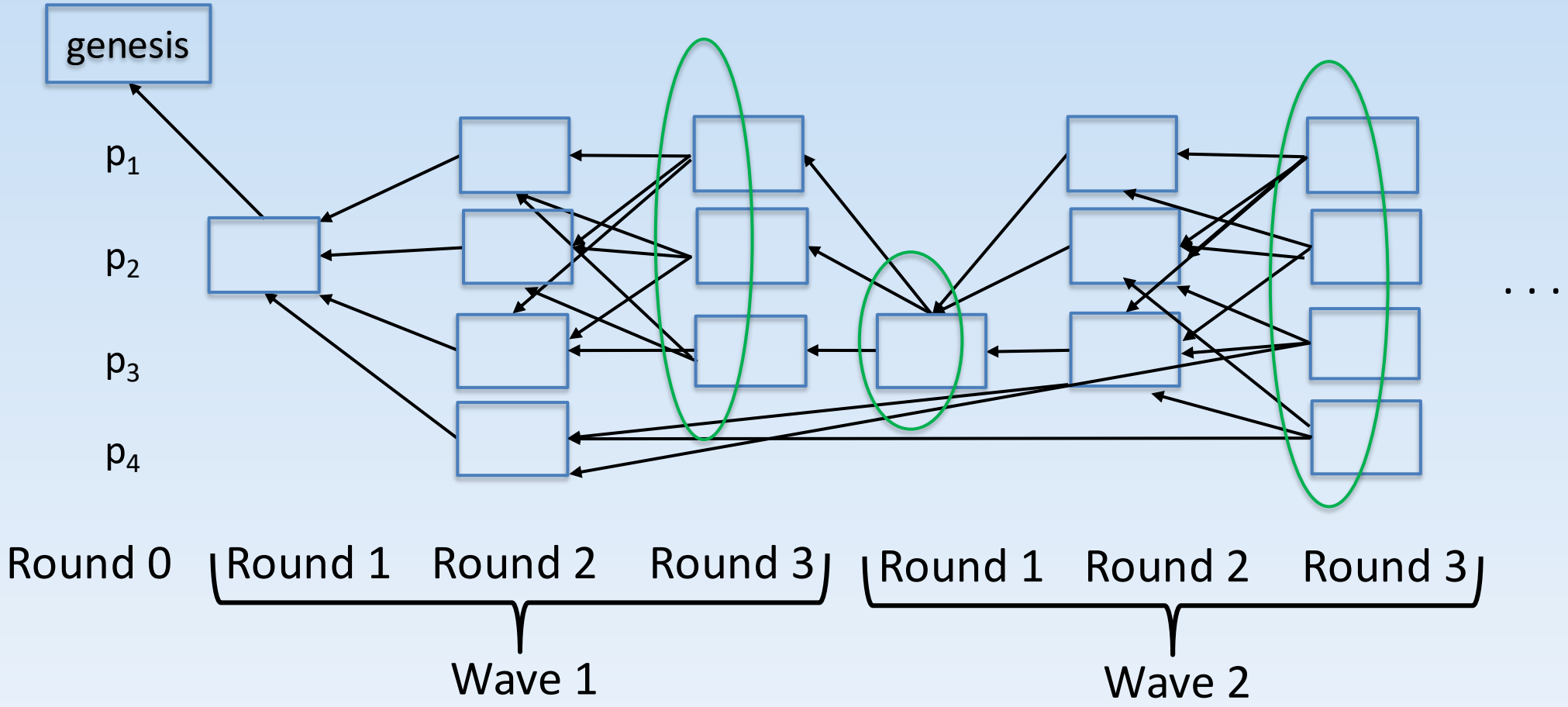
- The blocklace may be revealed to different agents in different orders
- An agent that receives a block pointing to a block it does not have, requests the missing block

∴ Eventually all agents observe a DAG including all the blocks generated by correct agents

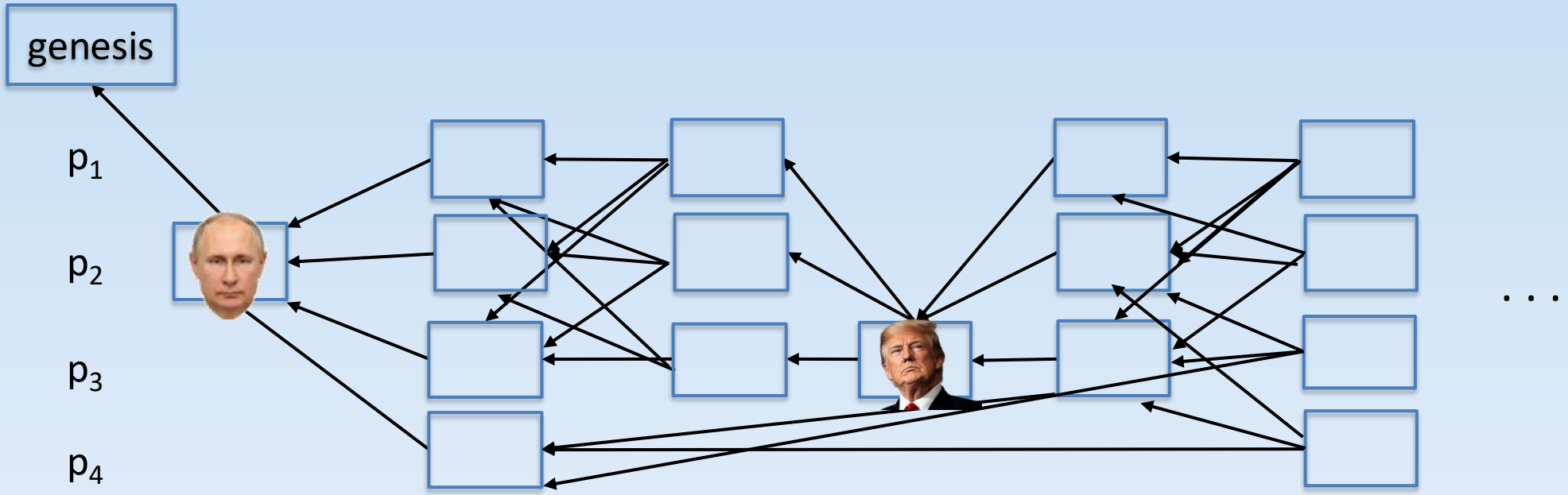
Constitutional Consensus
blocklace waves and rounds



Round 1 & 3 blocks point to a supermajority



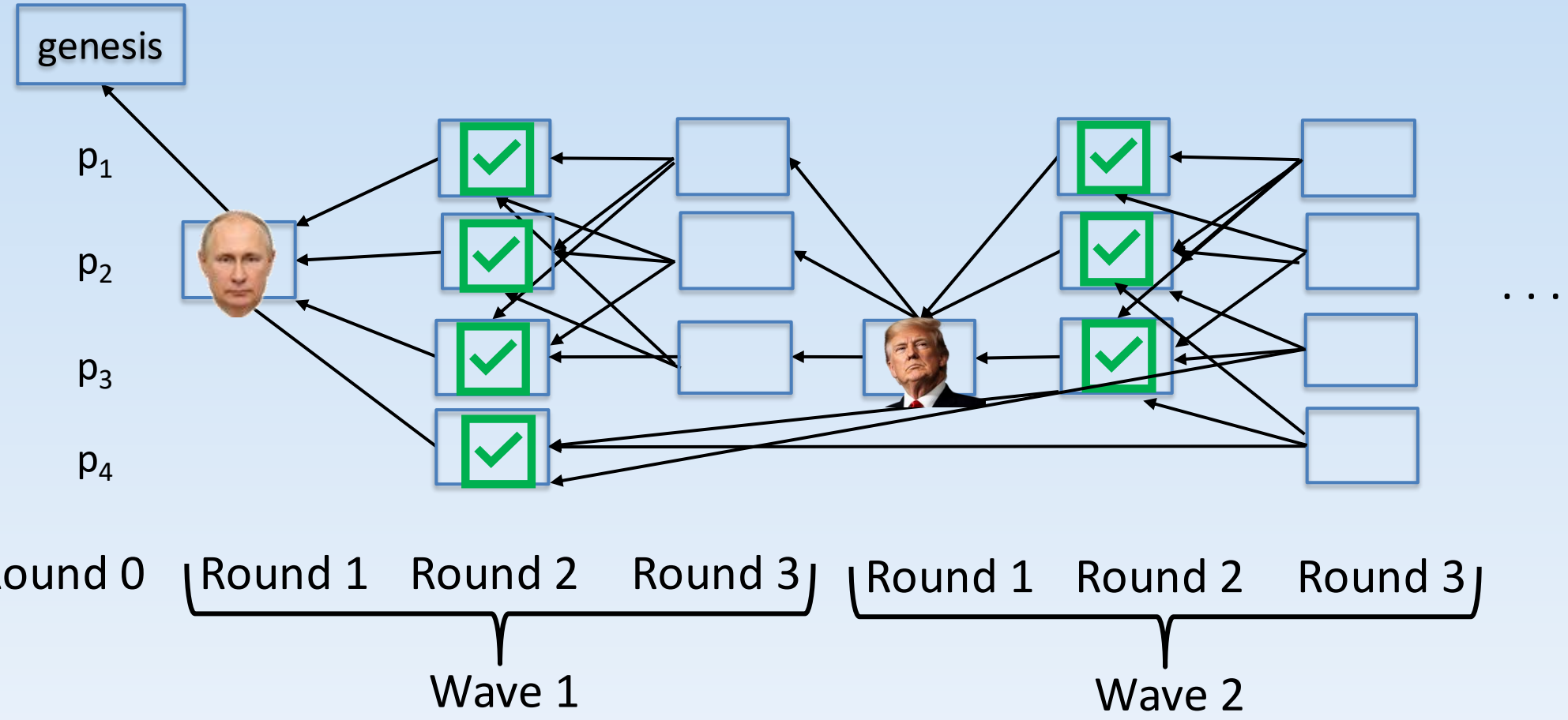
Round 1 is for leaders



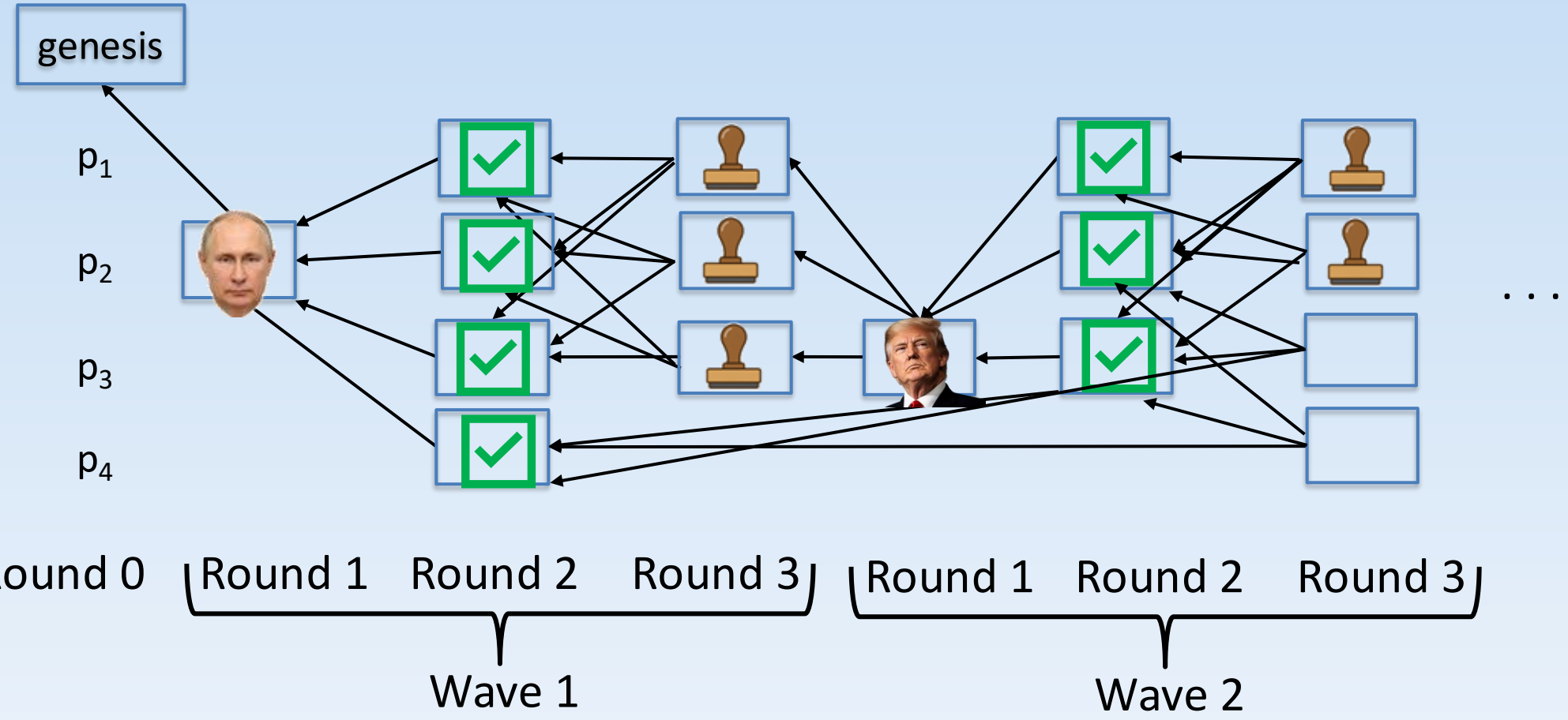
Round 0 | Round 1 | Round 2 | Round 3 | Round 1 | Round 2 | Round 3

Wave 1 | Wave 2

Round 2 is for *endorsing* one leader by approving only its block



Round 3 is for *ratification*
by approving a super-majority of endorsers

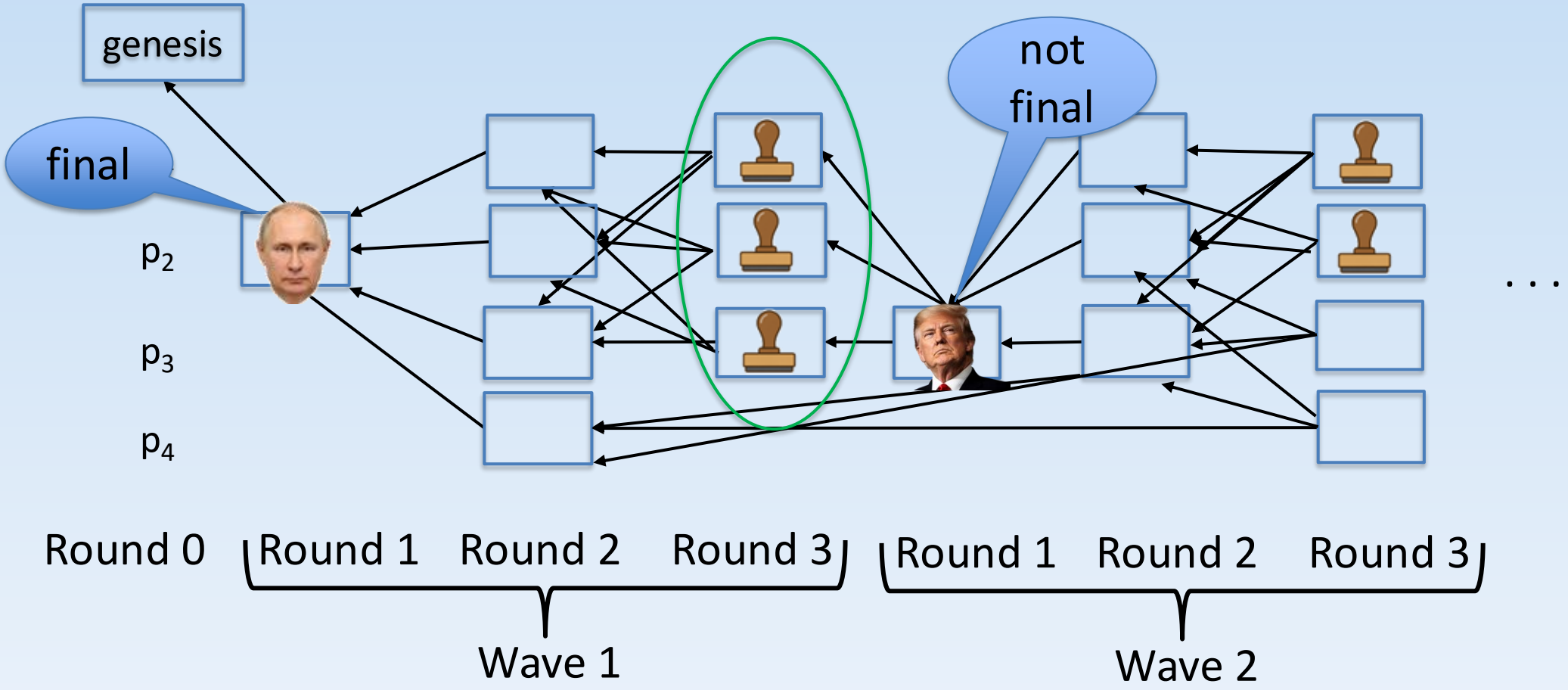


Ratification safety

- A round 2 block endorses at most one round 1 leader block
- Ratification requires a super-majority of endorsements
- Correct agents do not equivocate
- Two super-majorities intersect at at least one correct agent

∴ At most one block is ratified in a wave

A leader ratified by a super-majority is *final*

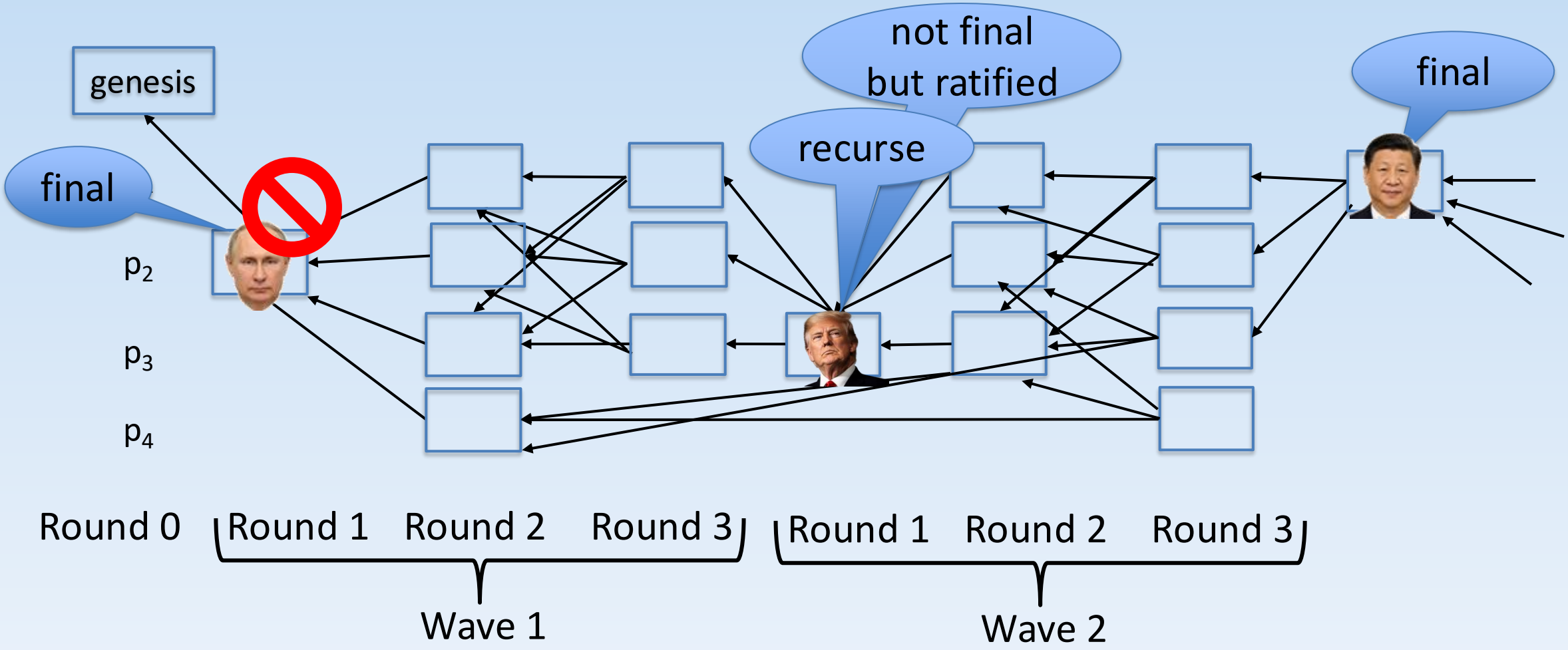


Finalization safety

- A final block b is ratified by a super-majority in round 3
- A round 1 block includes a super-majority of pointers, hence observes that b is ratified

∴ A final block is observed as ratified by every correct agent at every subsequent wave

Finalization triggers ordering on the spanned DAG

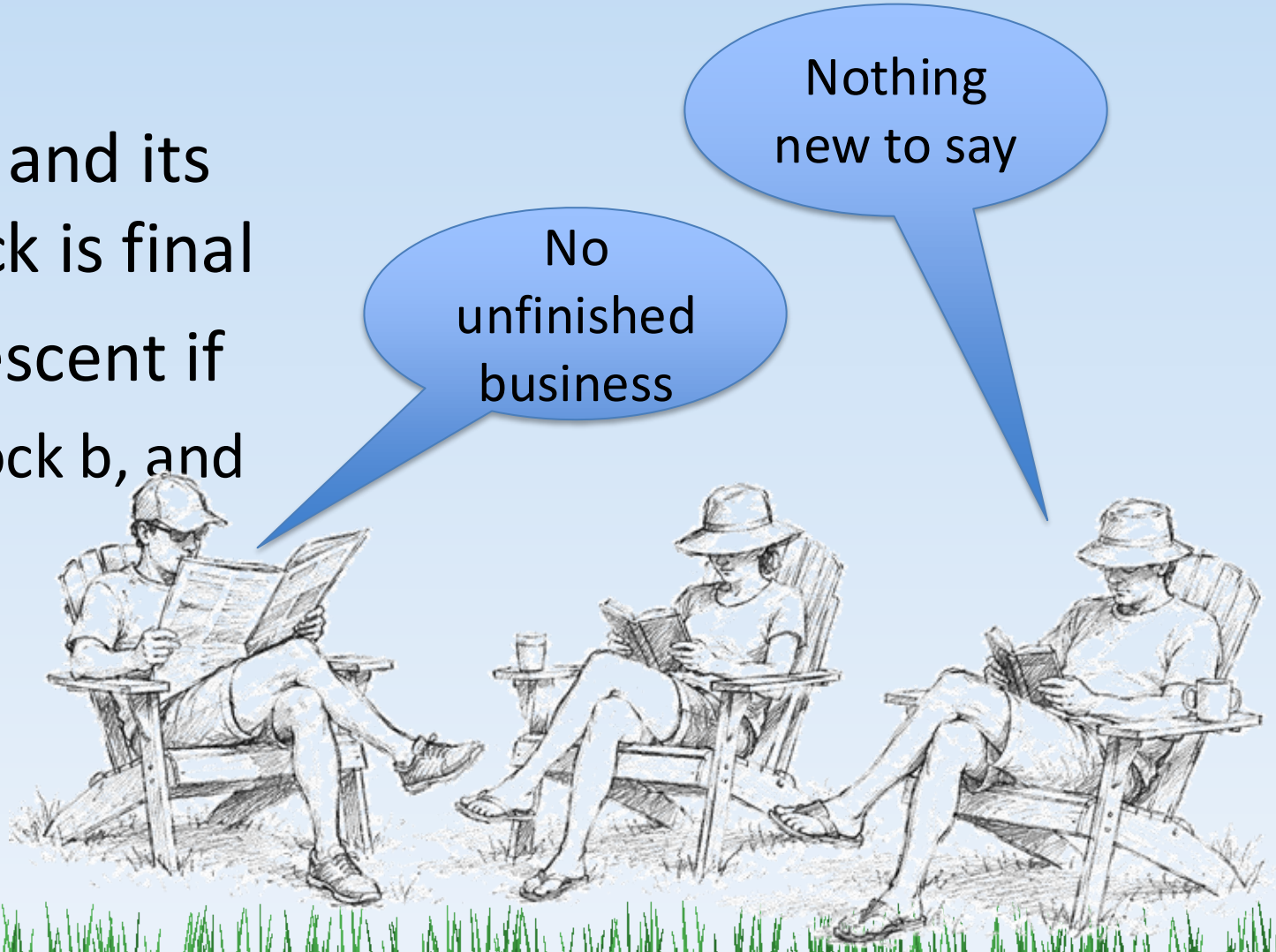


Nascent communities

- An instance of constitutional consensus may be invoked in a small community
  - which might later grow or coalesce with others
- There can be extensive periods with nothing to order
  - Minutes, hours, even days
- The system becomes *quiescent*

Quiescent waves

- The 0th-wave is quiescent and its constitutional genesis block is final
- A subsequent wave is quiescent if
  - it includes a final leader block b, and
  - all the blocks in the wave except b are empty



Low and high throughput (Morpheus)

- After a quiescent wave, the algorithm operates in *low throughput mode*.
  - Generates traffic only when agents have payloads.

- Otherwise, it operates in *high throughput mode*.
  - Generates blocks in all rounds.

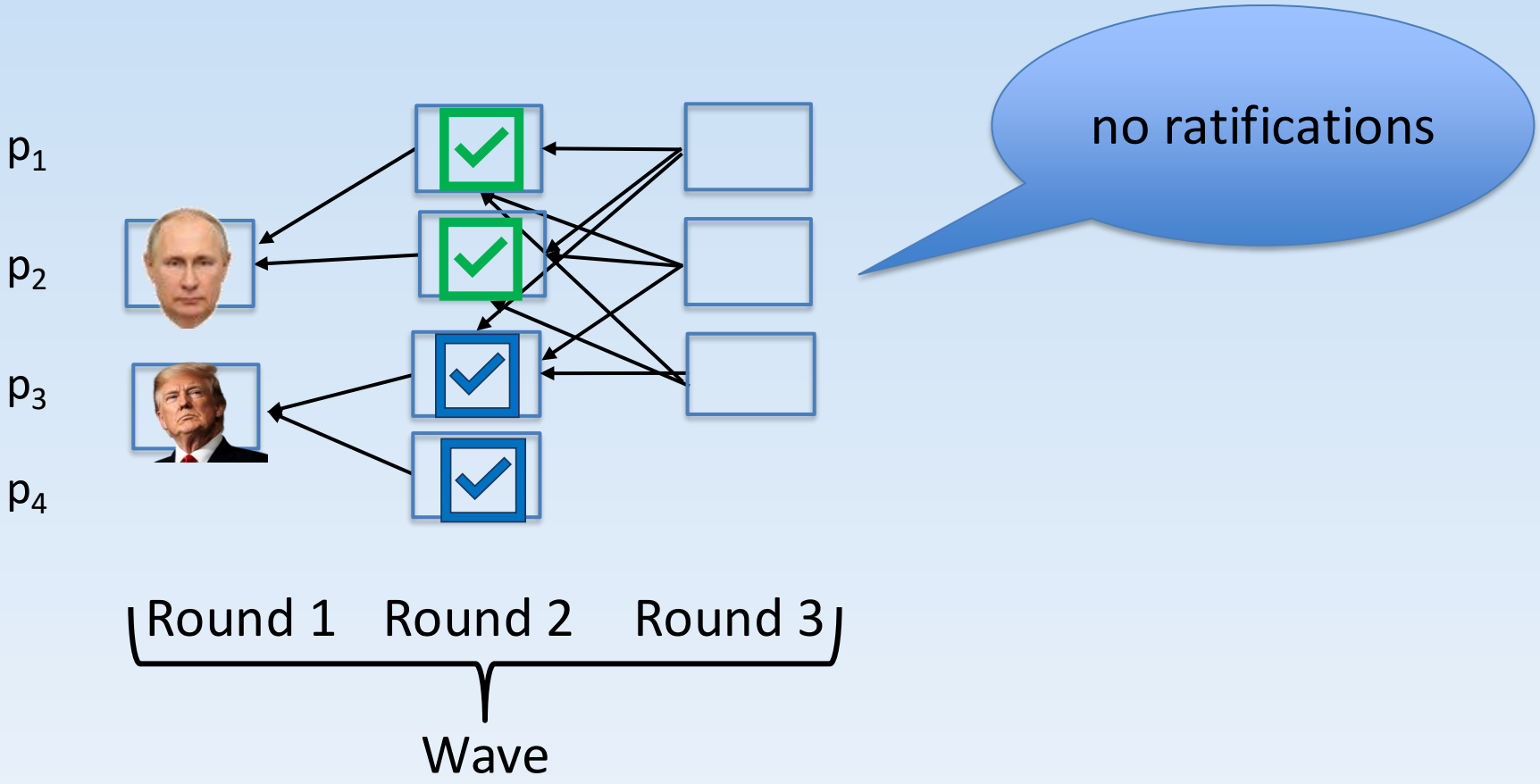
High throughput – formal leaders

- A deterministic and fair *leader* function selects a unique *formal leader* for each wave.
- In the good case, only the formal leader sends a round 1 block.
- In case of timeout, other agents send round 1 blocks.
  - May jeopardize finalization in this wave.
- Round 2 begins after there are blocks from either the formal leader or a supermajority.

Low throughput – spontaneous leaders

- All agents are quiet as long as they have no payloads.
- An agent with payload emerges as a *spontaneous leader.*
- If unique,
  it is endorsed by
  all correct agents.

Multiple leaders can prevent progress



Advanced rounds

- Round 0 is advanced.
- A round 1 is advanced if it includes a leader (either formal or spontaneous) or a super-majority.
- A round 2 or 3 is advanced if it includes a super-majority.

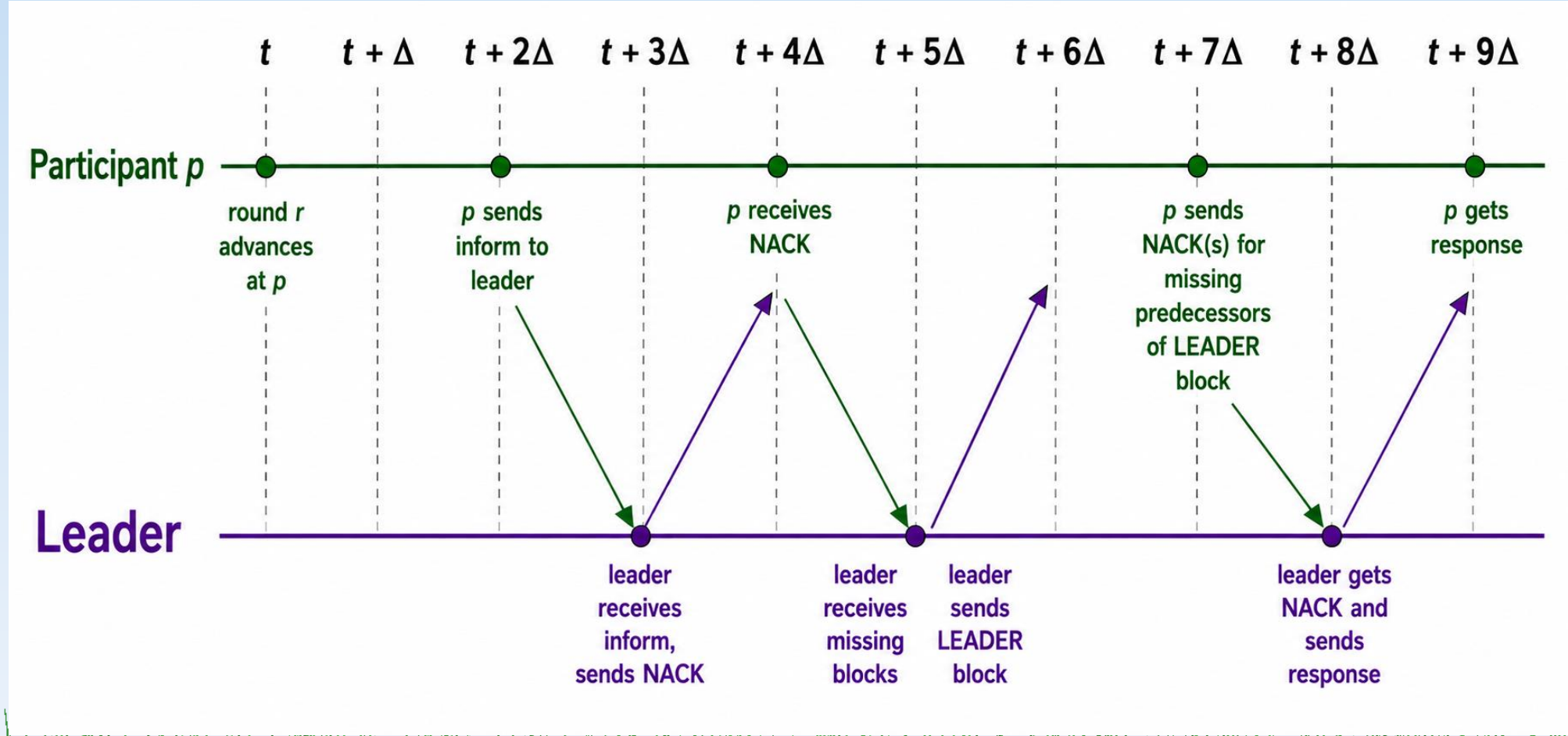
When to send blocks?

- Let r be the maximum advanced round
- Send a round r+1 block:
  - Rounds 2 and 3: immediately
  - Round 1 and quiescent: once I have payload
  - Round 1 and non-quiescent:
    - if I am the formal leader or
    - the round has been advanced for 9Δ
- Send backlog (in round r) if I have payload

NACKs, inform-leader, and timeouts

- Missing block (pointed by received block)
  - Wait Δ before sending a NACK
  - No NACKs in the good case (no failures, post-GST)
- Missing formal leader block in non-quiescent state
  - Maybe the leader is correct but doesn't know the 3rd round of the previous wave advanced
  - Wait 2Δ, then send inform-leader block to let it know the round advanced

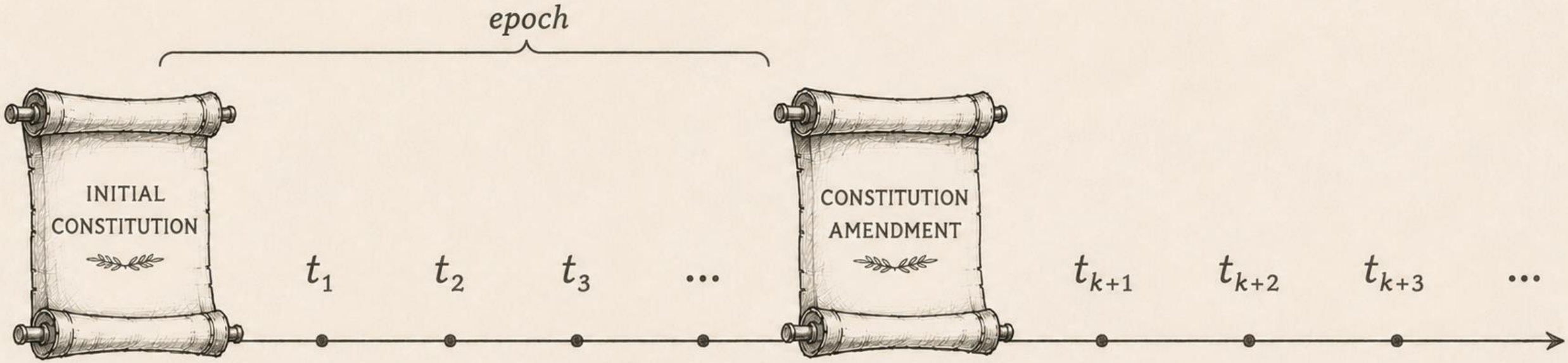
Worst-case delay after GST



Part 3: Constitutional consensus for democratic governance

1. Digital democracy, Paxos, and Consensus
2. Constitutional consensus
3. **Digital democratic governance**

Constitutional consensus democratic governance



1. Rules for producing a new *valid* constitution
2. Protocol for transitioning to the next epoch

Democratic governance is based on a constitution

- In general, the initial constitution specifies
  - an initial population,
  - an initial consensus protocol,
  - a rule for amending both, and
  - a rule for amending the constitution itself.
- In our case, amendments affect (P, σ, Δ)
  - P– set of participants
  - $\frac{1}{2} \leq \sigma < 1$ – super-majority threshold (tolerating Byzantines and sybils)
  - Δ – estimated latency bound after GST

Why these three parameters?

- P– members of the digital community should be sovereign to add/remove members
- σ – reflects the level of trust in the community
  - may be higher as new members are added, and lowered as trust in new members is gained.
- Δ – highly sensitive to the composition of P.

Amendments are decided by agents

- Volitional choice, not out-of-the-blue reconfiguration
- Crucial for democratic governance
- Constitution guards against problematic changes
  - Dead sailors
  - Voting to prevent future updates

Amending P to P’

- Requires signatures of
  - A super-majority in P – relinquishing control
  - All of P’ – adding only willing members (no dead sailors)
- The people who sign the amendment
  - Would only vote to add trusted individuals
  - Would only join if they trust a super-majority of the members of P’
  - See literature on sybil resistance admission and governance

Amending σ to σ’ - *h-rule*

- Studied in democratic context (Abramowitz et al.)
  - The only rule that satisfies certain intuitive and self-evident axioms.
- Each agent in P votes for their most-preferred new value of σ
- Then σ’ is
  - the maximal σ’ > σ for which there is a σ’-supermajority among P who voted for a value greater or equal to σ’
    (e.g., to increase to ¾, need a ¾-supermajority in P to vote for at least ¾)
  - or the minimal σ’ for which there is a σ-supermajority among P who voted for a value less than or equal to σ’
  - or σ remains unchanged.

Amending Δ to Δ' - *Suppress Outer-f*

- Shahaf et al. parameter update rule
  - for single-peaked domain with potential Sybil presence
- Each agent votes for its preferred $\Delta_i \in \mathbb{R}^+$
- If the median vote > Δ: discard the maximal f votes, take the median Δ' of the remaining votes.
- If the median vote < Δ: discard the minimal f votes, take the median Δ' of the remaining votes.
- Otherwise, Δ remains unchanged.

Properties of Suppress Outer-f

- If all Sybil agents wish to increase Δ (to slow down the protocol) but the correct agents do not, Δ will not increase;
  - symmetrically for decreasing.
- If all correct agents wish to update Δ to some Δ′, the update succeeds regardless of adversarial votes, provided $f < n/3$

Democratic amendment rules summary

A constitution (P, σ, Δ) is amended democratically to (P′, σ′, Δ′), using the prevailing (P, σ, Δ) as status quo:

1. P → P ′: per-member σ-supermajority among P, plus consent of all new members in P ′ \ P
2. σ → σ′: h-rule for constitutional amendment
3. Δ → Δ′: Suppress Outer-f parameter update rule

Valid constitution amendment decisions

- In a consensus epoch, agents run an *amendment protocol*

Part 3: Constitutional consensus for democratic governance

1. Digital democracy, Paxos, and Consensus
2. Constitutional consensus
3. Digital democratic governance

Questions?