Arc

ARC

Two Recent Advances in Decentralized Networks Design

Adi Seredinschi
Principal Product Manager
Circle

My Journey

2019

Research in BFT Consensus

2022

ComeBFT is born

2024

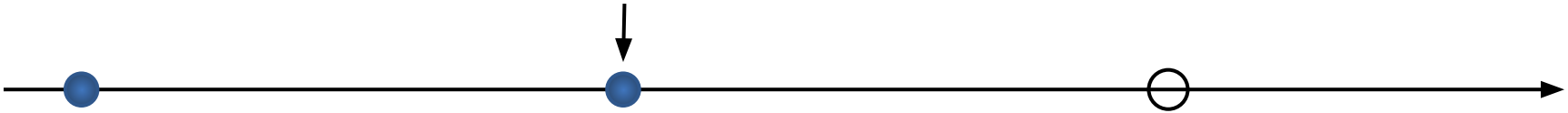
Malachite is born

2025 August

Joined Circle via Malachite acquisition

Arc Public Testnet is here

https://arc.network



SEPTEMBER

Private Testnet

OCTOBER

Arc Public Testnet went live

2026

Mainnet

Note: Dates are subject to change

Join us at Circle!

- Circle is a public 🇺🇸 company (IPO Q2 ‘25)
- Arc is a flagship platform, besides USDC and EURC stablecoins
- Significant portion of our team are EPFL alumni

careers.circle.com → “intern”

Two Recent Advances

in Decentralized Networks Design

{1} {System Design}

Predictable Costs & Settlement

{2} {Protocol Engineering}

Multi-Proposer

Two Recent Advances

in Decentralized Networks Design

{1} {System Design}

Predictable Costs & Settlement

From First Principles

Predictable costs & settlement

1. Predictable fees
2. Deterministic settlement
3. Predictable latency

Stable fees

Importance

Reduce volatility

Mechanism

USDC as Gas
+ others also

Deterministic Settlement (1/2)

Malachite consensus engine

- Implements Tendermint
- The most battle-tested BFT consensus protocol
- Proven in production via CometBFT since 2019
- Well-studied in literature

Tendermint

CometBFT lessons → Malachite design

- Modular design, especially at p2p level
- Rust for type safety & performance

CometBFT

Deterministic Settlement (2/2)

Tendermint Characteristics

- Well-known trade-offs vs. other BFT consensus protocols
- Scalability O(100) validators; up to tens of 1000s
- Latency > Throughput
- Can evolve in both Throughput and Latency dimensions

Measurements ~August 2025

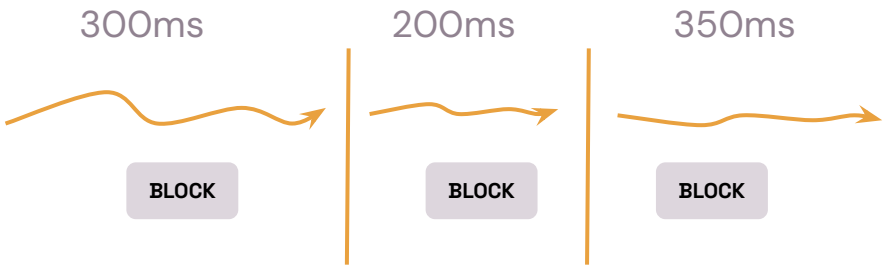
- ~330ms block time
- 3'000tps (->100'000 tps+ in the future)
- In a 20-node geo-distributed network

Why "Deterministic?"

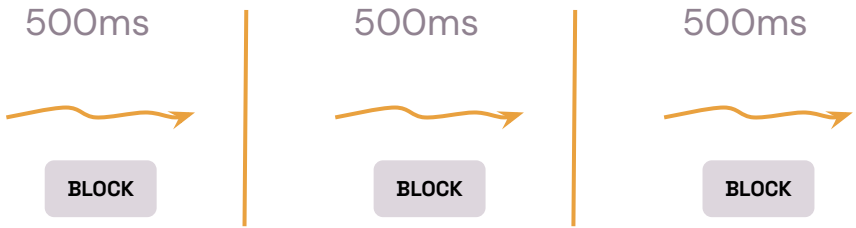
- Known validator set (replicas)
- Prioritizes Safety > Liveness
- Avoids reorgs ("eventual consistency")
- Institutions don't want to deal with poorly defined properties

Predictable Latency

Via Stable Block Times



- Follow the speed of the geo-distributed network
- Natural variations due to block proposer placement & latencies



- “Throttling” algorithm
- Wait at end of block production
- In practice, ~99.99% of block finalize in ~500ms

https://testnet.arcscan.app/

From First Principles

Predictable costs & settlement

✓ 1. Predictable fees
✓ 2. Deterministic settlement
✓ 3. Predictable latency

Bonus, two other system design choices:

4. Opt-in Privacy
5. Permissioned validator set

Johnny Depp in Pirates of the Caribbean

Permissioned validator set

- Institutional-grade
- Professional
- Independent in their judgement
- Wide geographic reach
- Wide jurisdictional reach
- Compliance focused

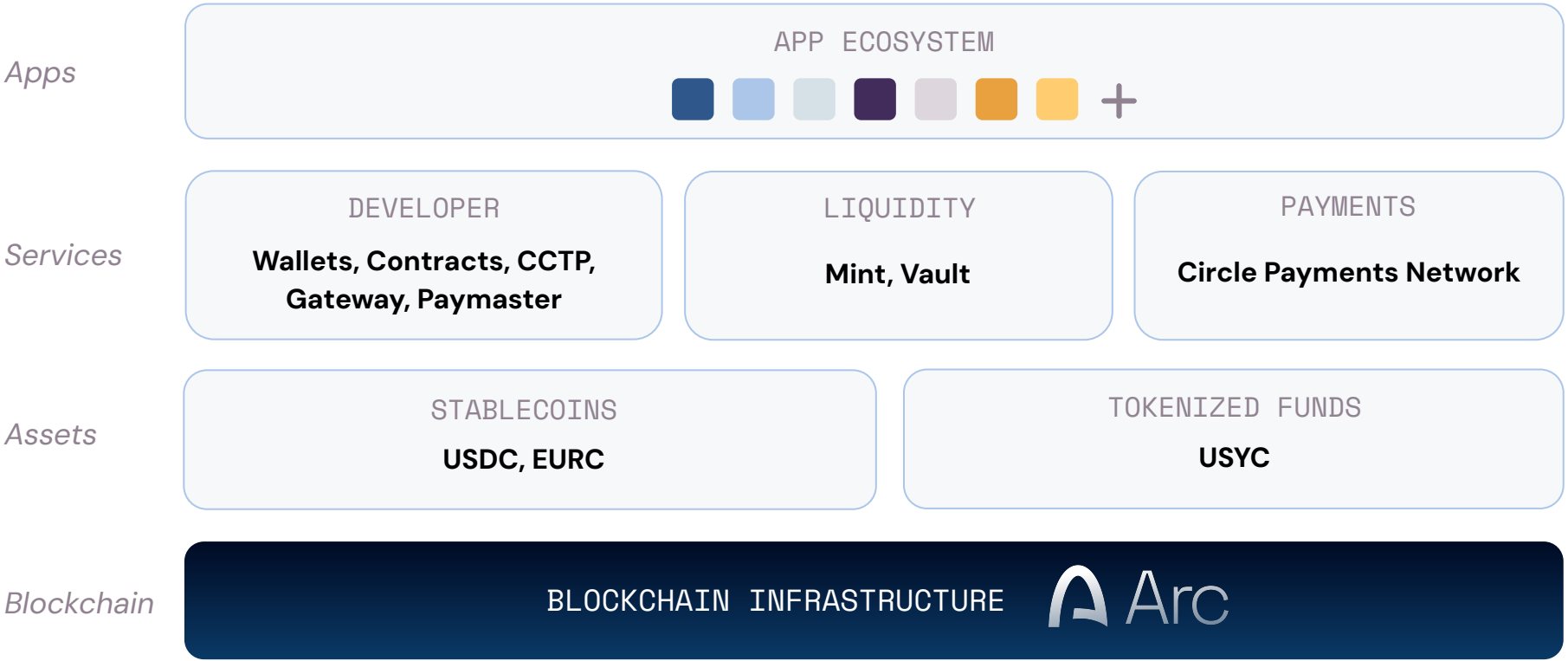
Predictable Costs & Settlement

Why is this important?

Ferdinand Magellan (1519–22) portrait
Encyclopædia Britannica, Inc.

Voyages of Ferdinand Magellan (1519–22) and Francis Drake (1577–80) across the Atlantic Ocean and around the globe.
Encyclopædia Britannica, Inc.

Arc is the foundational layer of Circle's full-stack platform[1]



1. Please see slide 22 for important product disclosure

Two Recent Advances

in Decentralized Networks Design

{2} {Protocol Engineering}

Multi-Proposer

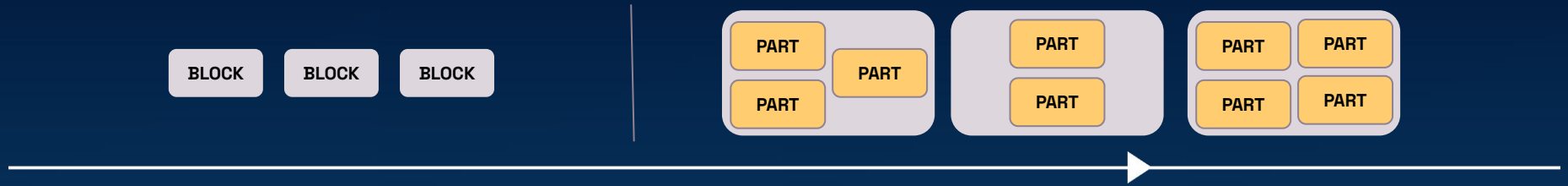
Multi-Proposer

Motivation

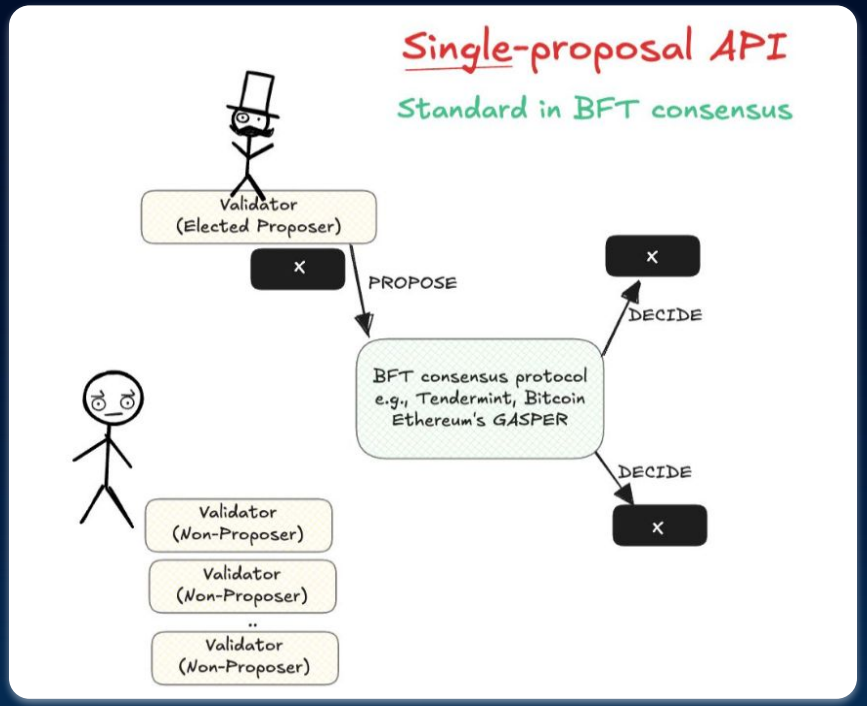
- *How to enable block construction out of multiple proposals?*
- Prompted by anti-censorship motivation
- Avoid rabbit holes with risky new designs
  - Use Tendermint as a black box
  - Build on top of a solid foundation

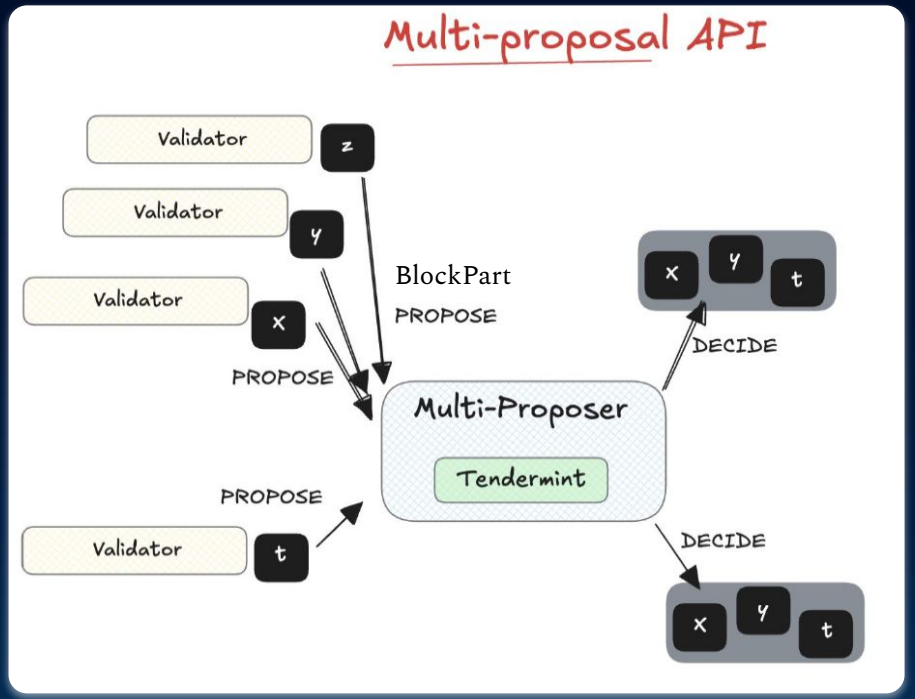
Intuition

- Allow *all* validators to propose
- Proposals happen at *any* time
  (not only when a validator is the proposer)
- Each proposal represents a BlockPart
  (not the full block itself as it used to be)
- Blocks are created out of *BlockParts*



Single- vs. Multi-Proposer API

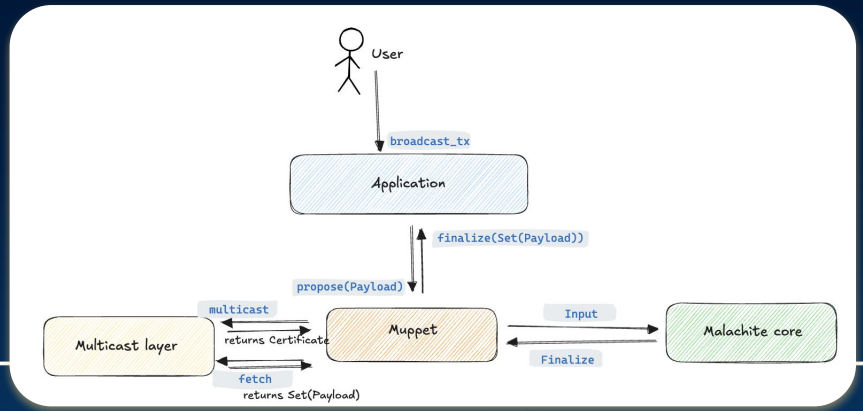




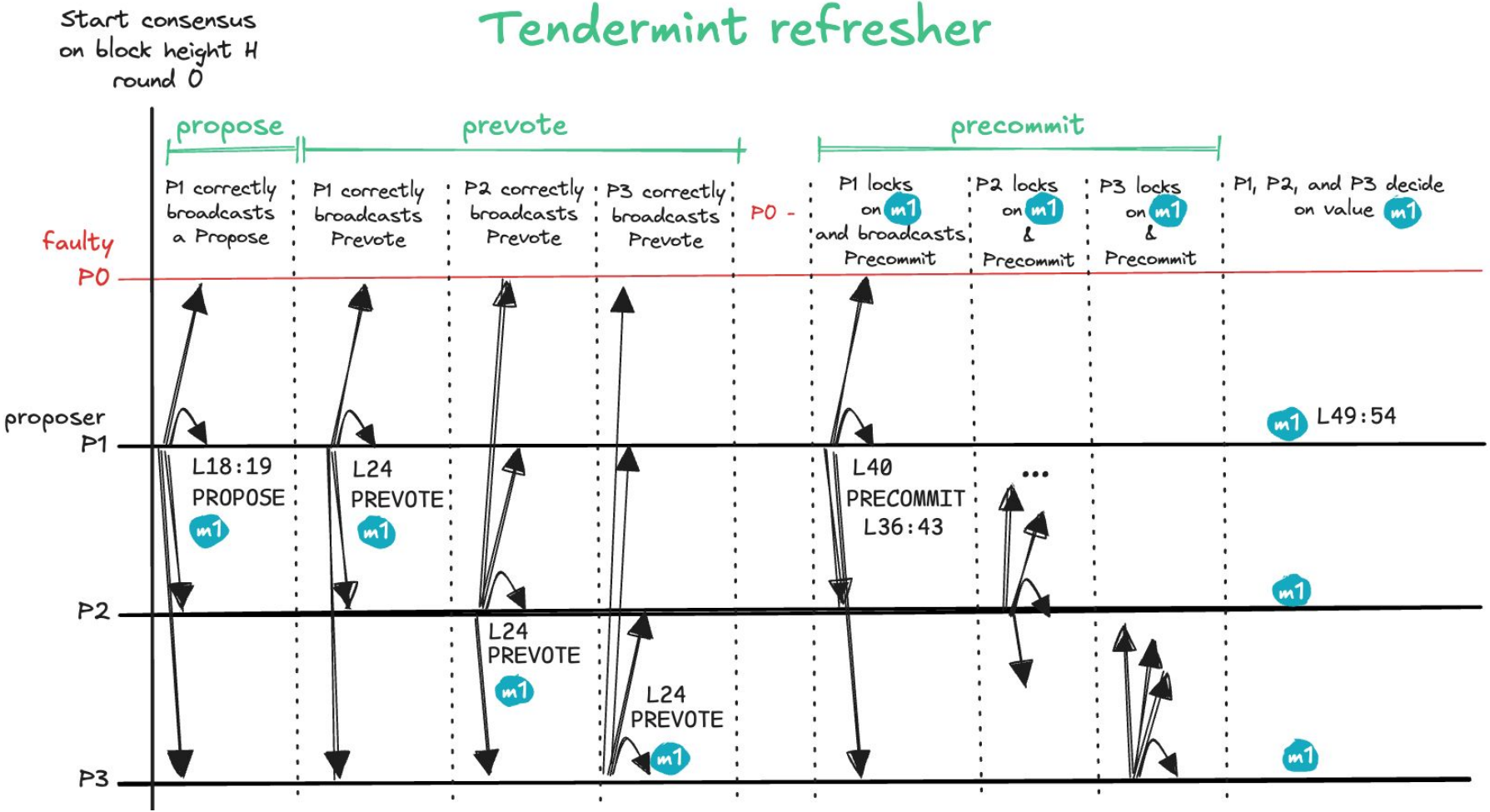
Multi-Proposer

Technical approach

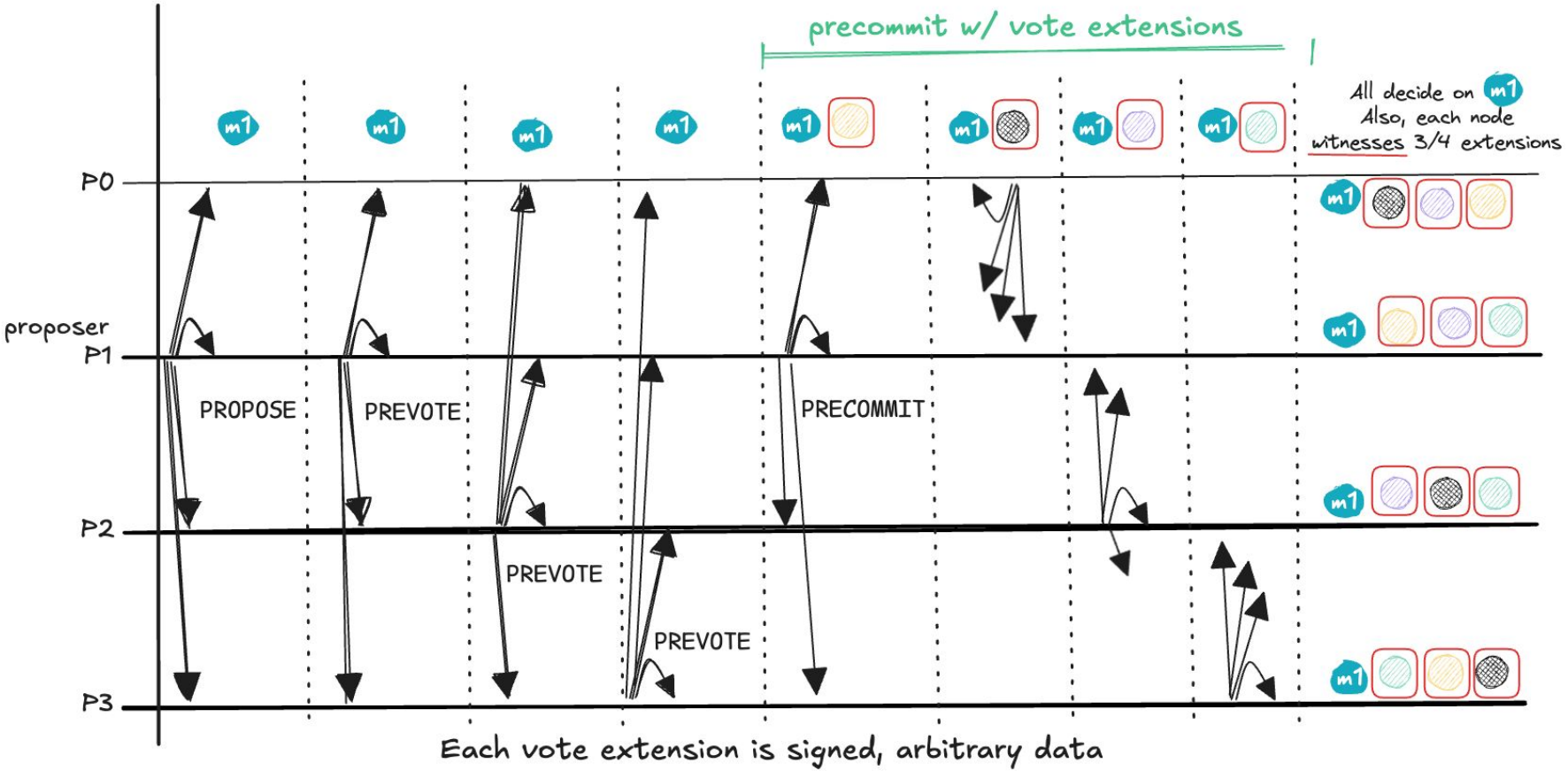
- Leverage Vote Extensions (VE) – messages piggybacked on Tendermint Precommits
- Put each BlockPart in a VE
- Precommits are necessary for liveness & safety -> Make VEs “un-ignorable”
- BlockPart dissemination happens off-the-critical path of consensus via a separate secure multicast protocol



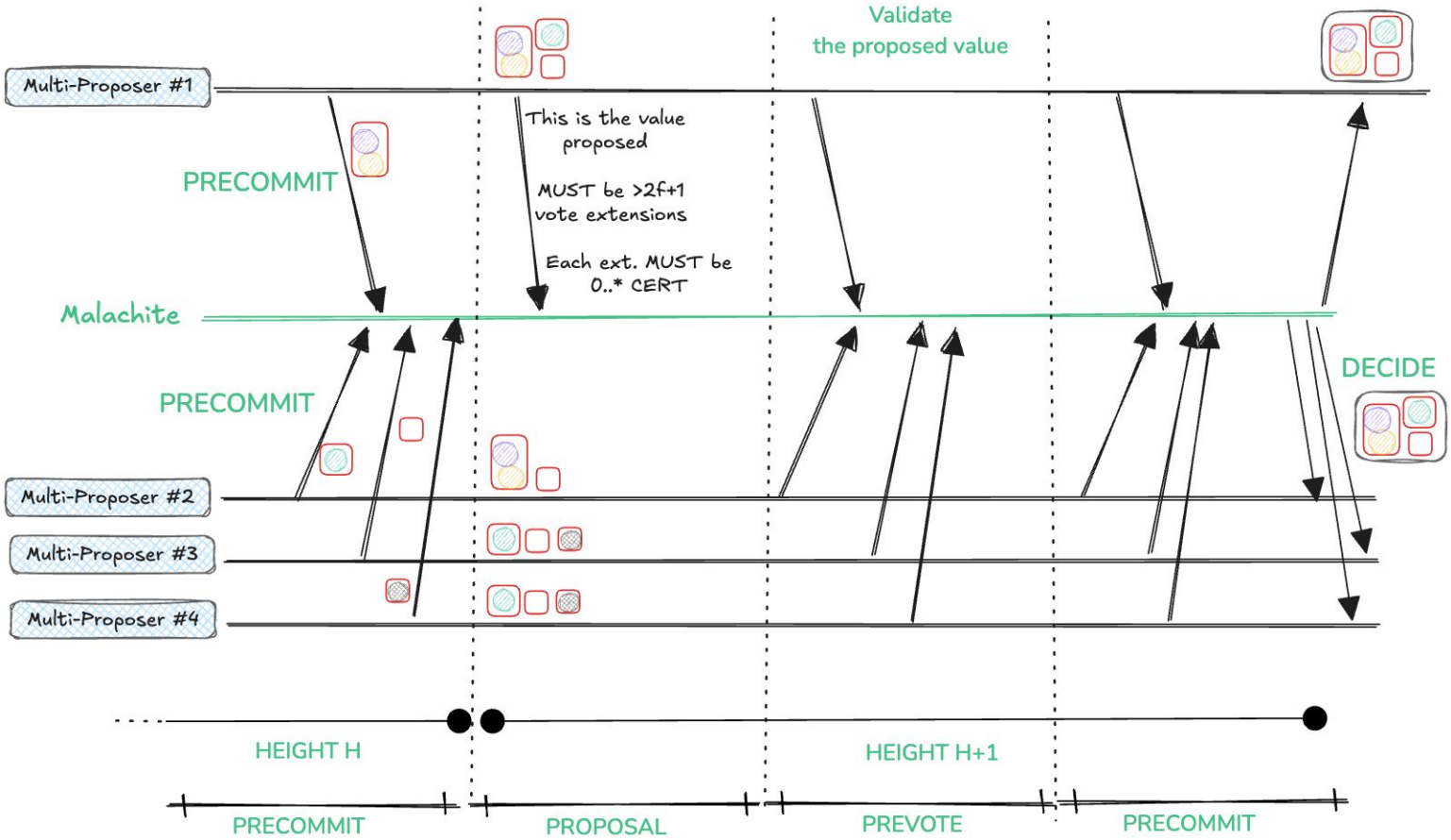
Tendermint refresher



Vote Extensions



Multi-Proposer Design



Join us at Circle!

- Circle is a public 🇺🇸 company (IPO Spring ‘25)
- Arc is a flagship product, besides USDC and EURC stablecoins
- Significant portion of our team are EPFL alumni

careers.circle.com → “intern”

Arc testnet is offered by Circle Technology Services, LLC ("CTS"). CTS is a software provider and does not provide regulated financial or advisory services. You are solely responsible for services you provide to users, including obtaining any necessary licenses or approvals and otherwise complying with applicable laws. Arc has not been reviewed or approved by the New York State Department of Financial Services. The product features described in these materials are for informational purposes only. All product features may be modified, delayed, or cancelled without prior notice, at any time and at the sole discretion of Circle Technology Services, LLC. Nothing herein constitutes a commitment, warranty, guarantee or investment advice.

Circle Mint and money transmission services are provided by Circle Internet Financial, LLC, NMLS # 1201441, and Circle Internet Financial Europe SAS, Electronic Money Institution License No. 17788, when provided in France. A list of Circle's regulatory authorizations can be found at circle.com/legal/licenses. Circle Mint is currently available only to institutions and is not available to individuals.

Circle Wallets, Circle Contracts, and Circle Vault are provided by Circle Technology Services, LLC ("CTS"). CTS is a software provider and does not provide regulated financial or advisory services. You are solely responsible for services you provide to users, including obtaining any necessary licenses or approvals and otherwise complying with applicable laws. For additional details, please see console.circle.com/legal/developer-terms for the Circle Developer terms of service.

Circle Technology Services, LLC (CTS) is the operator of Circle Payments Network (CPN) and offers products and services to financial institutions that participate in CPN to facilitate their CPN access and integration. CPN connects participating financial institutions around the world, with CTS serving as the technology service provider to participating financial institutions. While CTS does not hold funds or manage accounts on behalf of customers, we enable the global ecosystem of participating financial institutions to connect directly with each other, communicate securely, and settle directly with each other. CTS is not a party to transactions between participating financial institutions facilitated by CPN who use CPN to execute transactions at their own risk. Use of CPN is subject to the CPN Rules and the CPN Participation Agreement between CTS and a participating financial institution.

USDC and EURC are issued by regulated affiliates of Circle. A list of Circle's regulatory authorizations can be found at circle.com/legal/licenses.

USYC is a digital asset token. Each USYC token serves as a digital representation of a share of the Hashnote International Short Duration Fund Ltd. (the "Fund"), a Cayman Islands registered mutual fund. The Fund has appointed Circle International Bermuda Limited ("CIBL"), a Bermuda Monetary Authority licensed digital asset business, as its token administrator, responsible for the management of USYC on behalf of the Fund. Shares of the Fund and USYC are only available to non-U.S. Persons, as defined under the Securities Act of 1933, as amended. Additional eligibility restrictions may apply. The information provided herein is solely for educational and informational purposes and should not be construed as an offer to sell or a solicitation of an offer to buy any security, financial instrument, or other product.