Fairgate

BATTLE For Bitcoin

Sergio Demian Lerner | CTO, Fairgate Labs

SEPT 2025

Agenda

1. DROCA
2. BATTLE Theory
3. BATTLE For Bitcoin
   a. Phase 1
   b. Phase 2
4. Summary

DROCA: Dispute Resolution of Concurrent Assertions

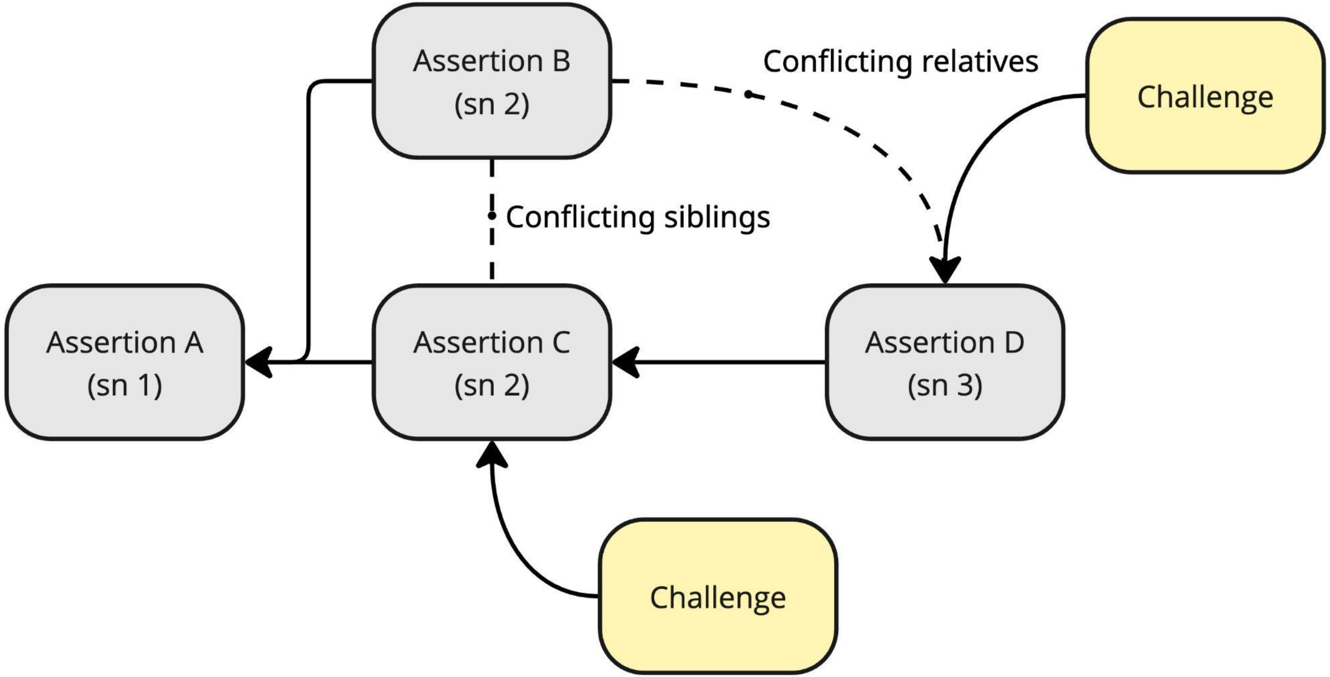
DROCA

- Two roles: Asserters and Challengers
- Asserters claim certain assertions are true
- Challengers disprove those claims
- There can be child assertions (used by rollups)

- Asserters can claim conflicting statements:
    - Alice: There is a withdrawal of 10 BTC to Carol pending with sequence number W
    - Bob: There is a withdrawal of 5 BTC to Dave pending with sequence number W

- The correct assertion must be selected and executed

Example


Assertion B
(sn 2)
Conflicting relatives
Challenge
Conflicting siblings
Assertion A
(sn 1)
Assertion C
(sn 2)
Assertion D
(sn 3)
Challenge

Federated vs BitVM vs Validating Bridges

Cost of Participation

Participation in DROCA consumes three resource classes:

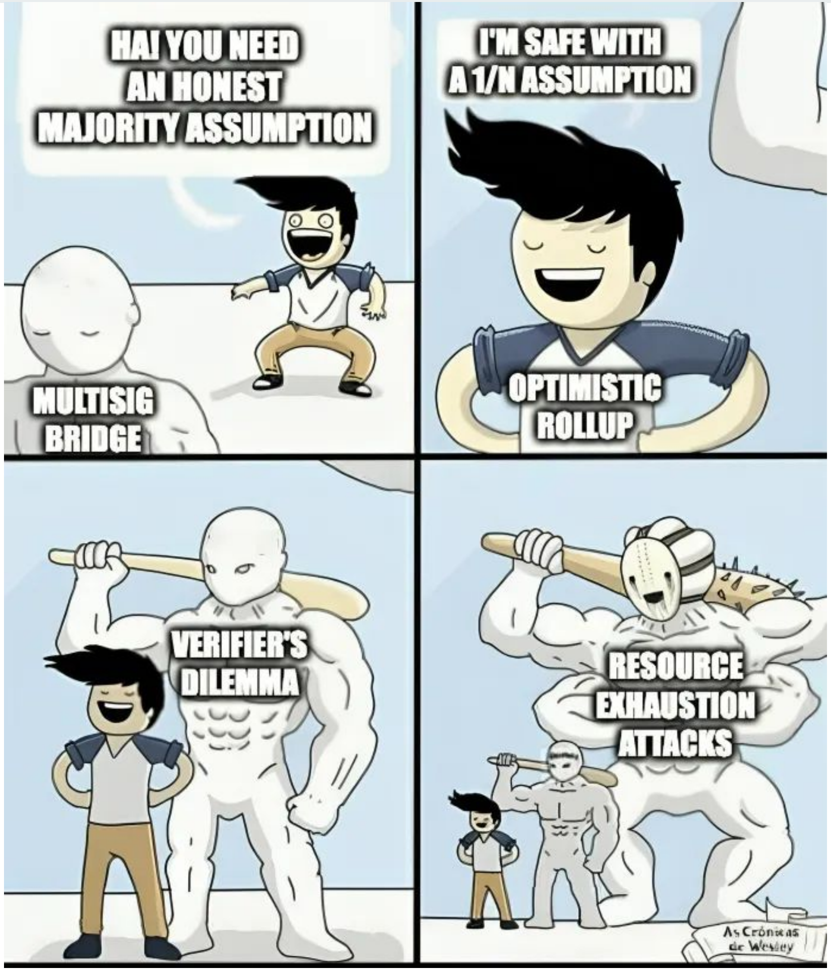
1. staking—capital posted as security bonds, as specified by the protocol;
2. gas—L1 currency to pay inclusion fees for assertions and dispute moves;
3. computation—off-chain compute (and bandwidth) incurred by participating parties.

Existing DROCA Protocols

1. Optimism
2. Arbitrum Classic
3. PRT
4. BoLD
5. Dave
6. BATTLE

Verifier’s Dilemma in Optimistic Protocols

- Optimistic protocols assume validity by default.
- Fraud is caught only if someone challenges.
- Verifiers must re-check state to find fraud.
- Re-checking costs time and money.
- Each verifier hopes someone else will do it.
- In equilibrium, nobody checks consistently.
- Attackers can slip in invalid assertions unchallenged.
- If verifiers do check, they’re rarely rewarded.
- If they don’t, system safety degrades.
- That tension is the Verifier’s Dilemma.

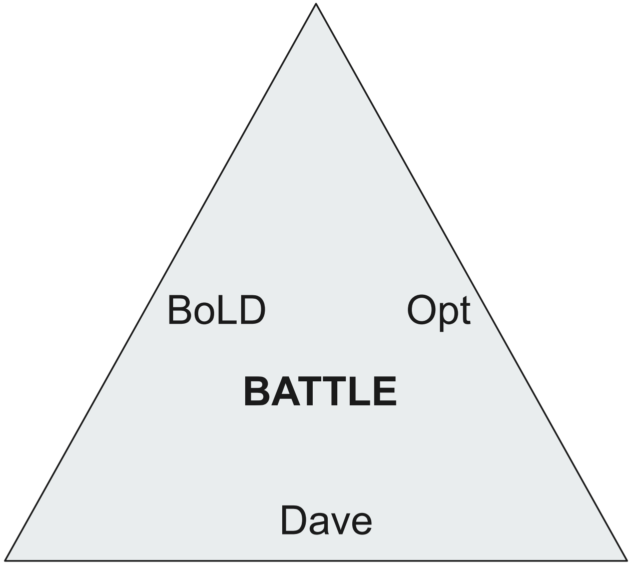

HA! YOU NEED AN HONEST MAJORITY ASSUMPTION
MULTISIG BRIDGE
I'M SAFE WITH A 1/N ASSUMPTION
OPTIMISTIC ROLLUP
VERIFIER'S DILEMMA
RESOURCE EXHAUSTION ATTACKS

Fraud Proof Trilemma

- Fraud-proof systems try to balance **efficiency**, **soundness**, and **liveness**.
- **Efficiency**: Disputes should resolve with low on-chain cost (logarithmic or constant, not linear).
- **Soundness**: Invalid assertions must always be rejected if at least one honest challenger exists.
- **Liveness**: Honest challengers must be able to complete disputes without being blocked or griefed.
- The trilemma: you can strongly guarantee only **two** of the three at once.
- E.g., making disputes highly efficient may weaken liveness; prioritizing liveness may raise costs; maximizing soundness may require heavy on-chain verification.

Fraud Proof Trilemma

Promptness or Liveness

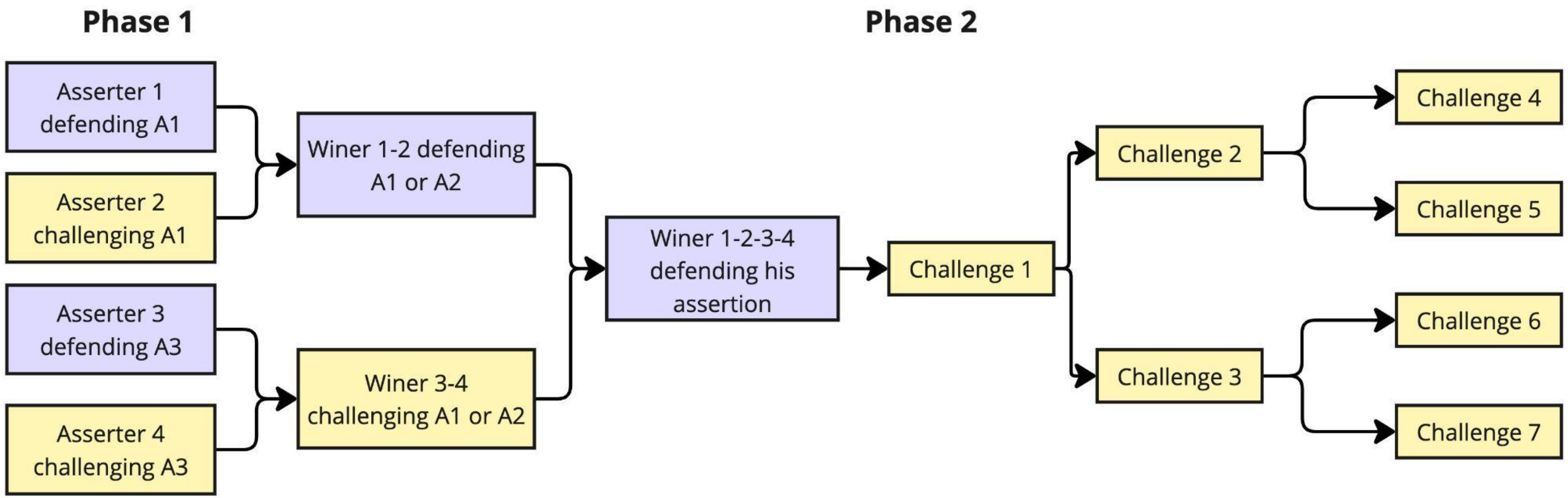


Safety / Soundness

Efficiency / Decentralization

BATTLE

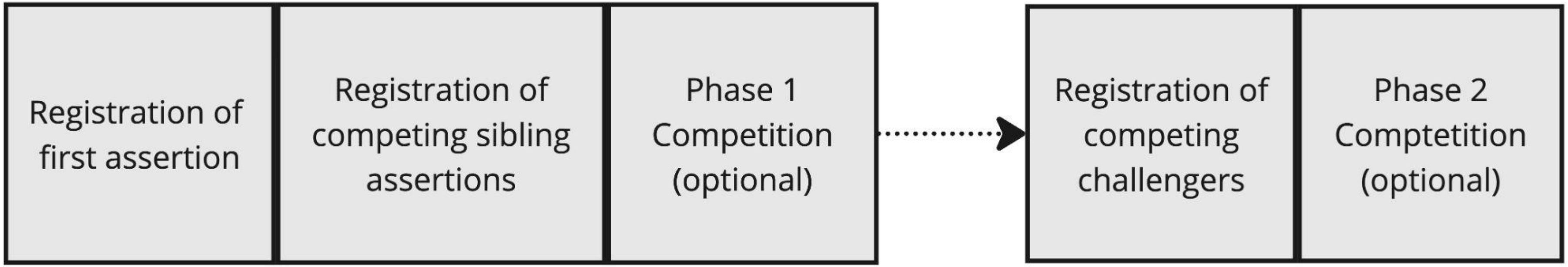
Protocol Phases



Conflicting assertions compete.

Winning assertion competes with challengers

Protocol Phases



Parameters of a DROCA Protocol

MIN = Minimum Initial Capital

PSB = Persistent Security Bond

OSB =On-Demand Security Bond

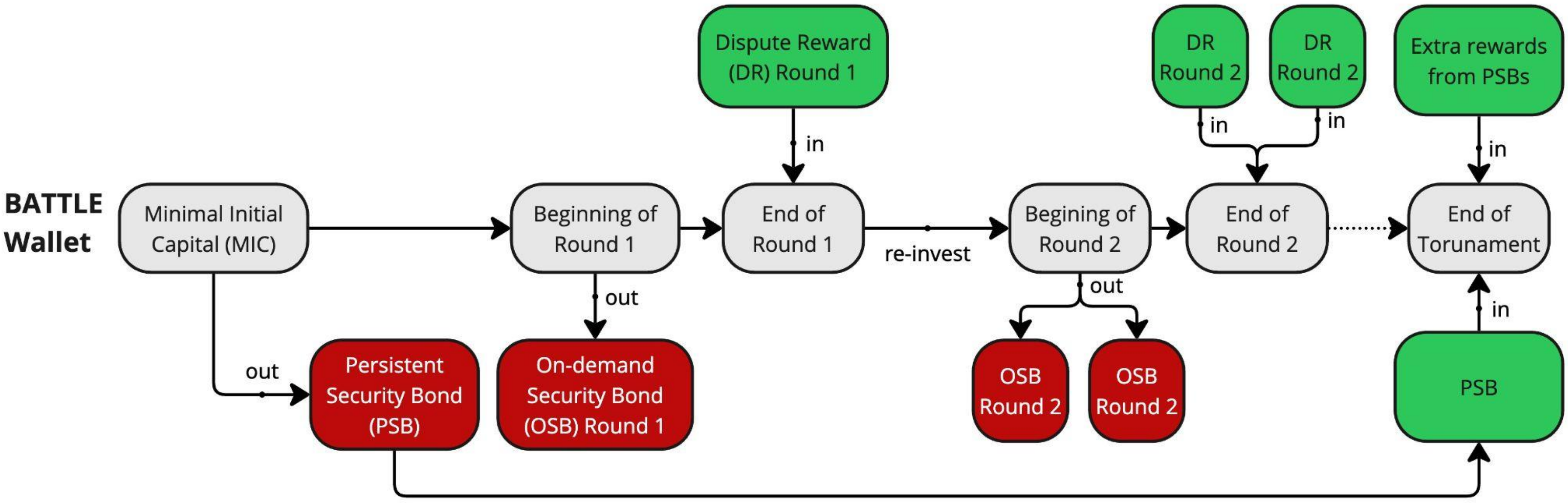
DR = Dispute Reward

DC = Dispute Cost

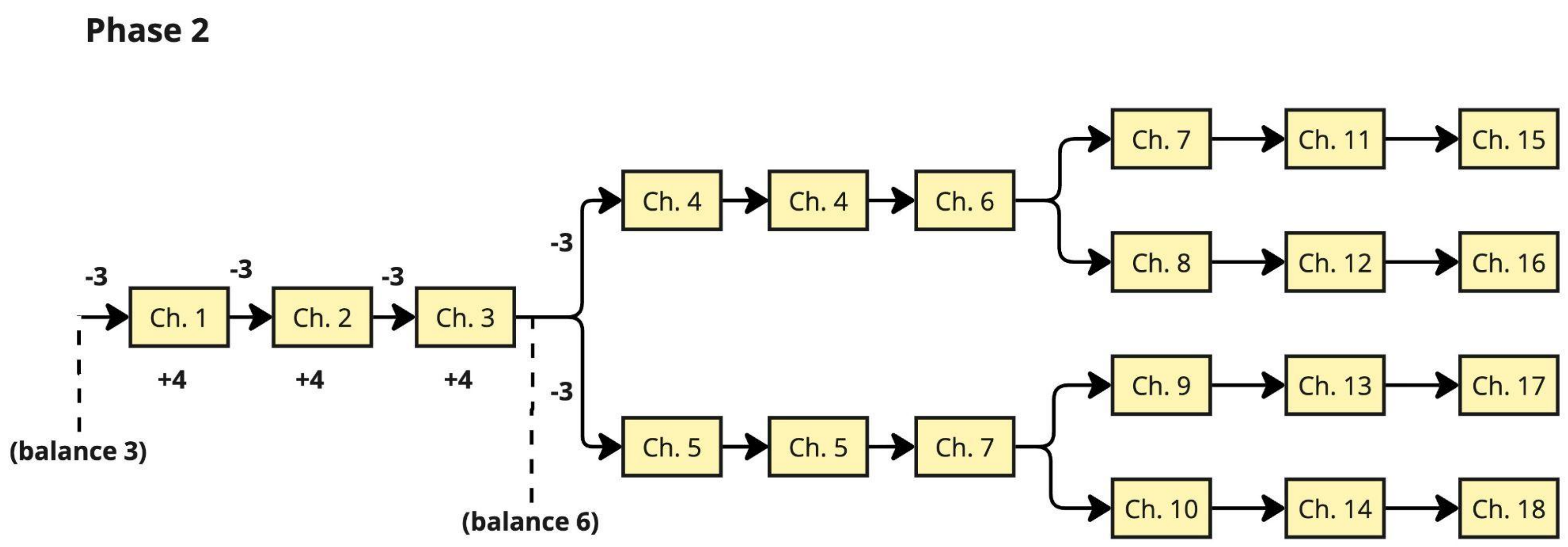
$$DR > DC$$

$$DR < OSB + PSB$$

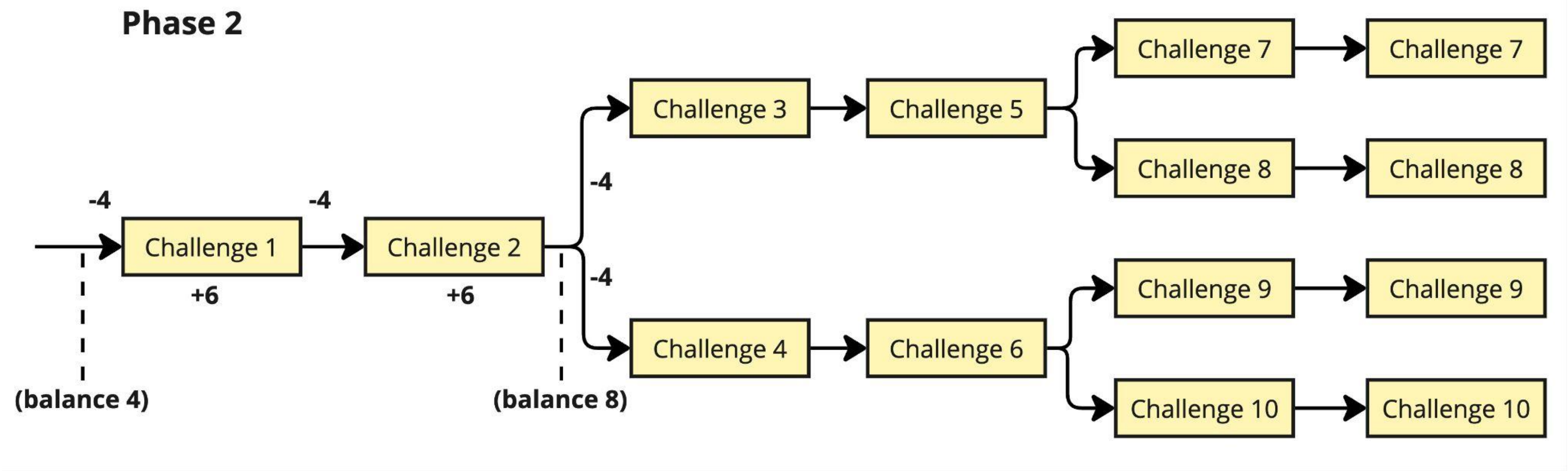
Wallet Updates During Tournament



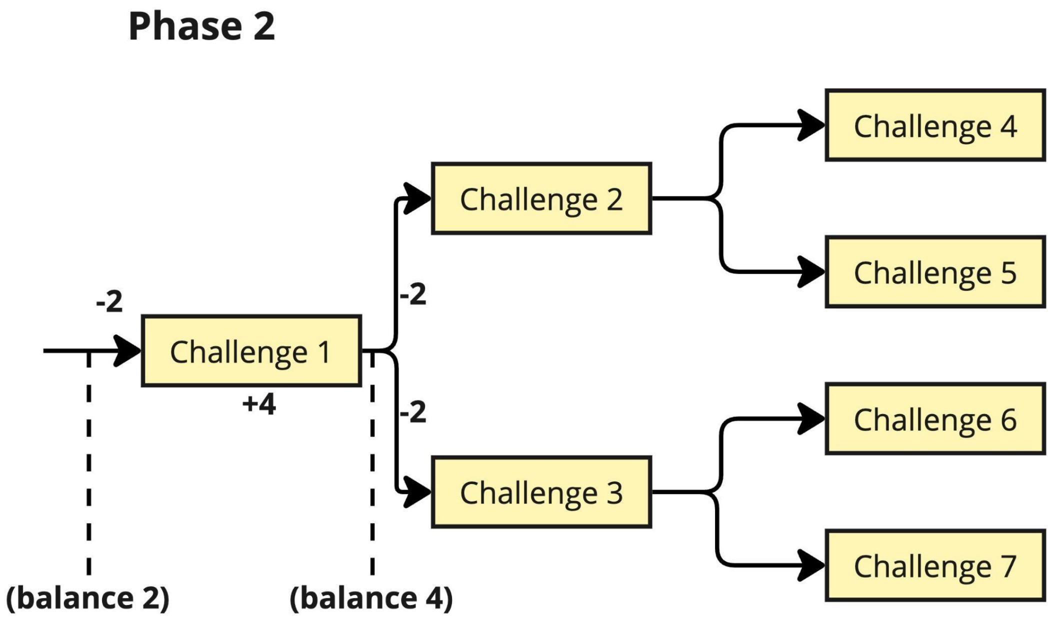
Schedule 1: MIN=3, DC=1, DR=OSB = 2



Schedule 2: MIN=4, DC=1, DR=OSB=3

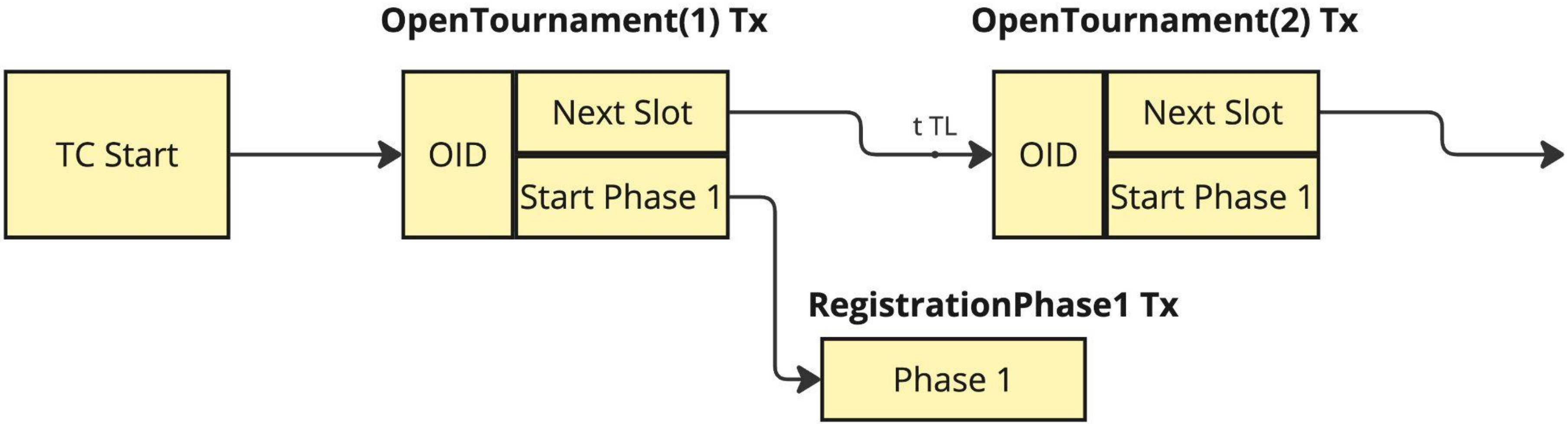


Schedule 3: MIN=2, DC=1, OSB=1, DR=3 (asserter)
MIN=4, DC=1, OSB=3, DR=1 (challenger)



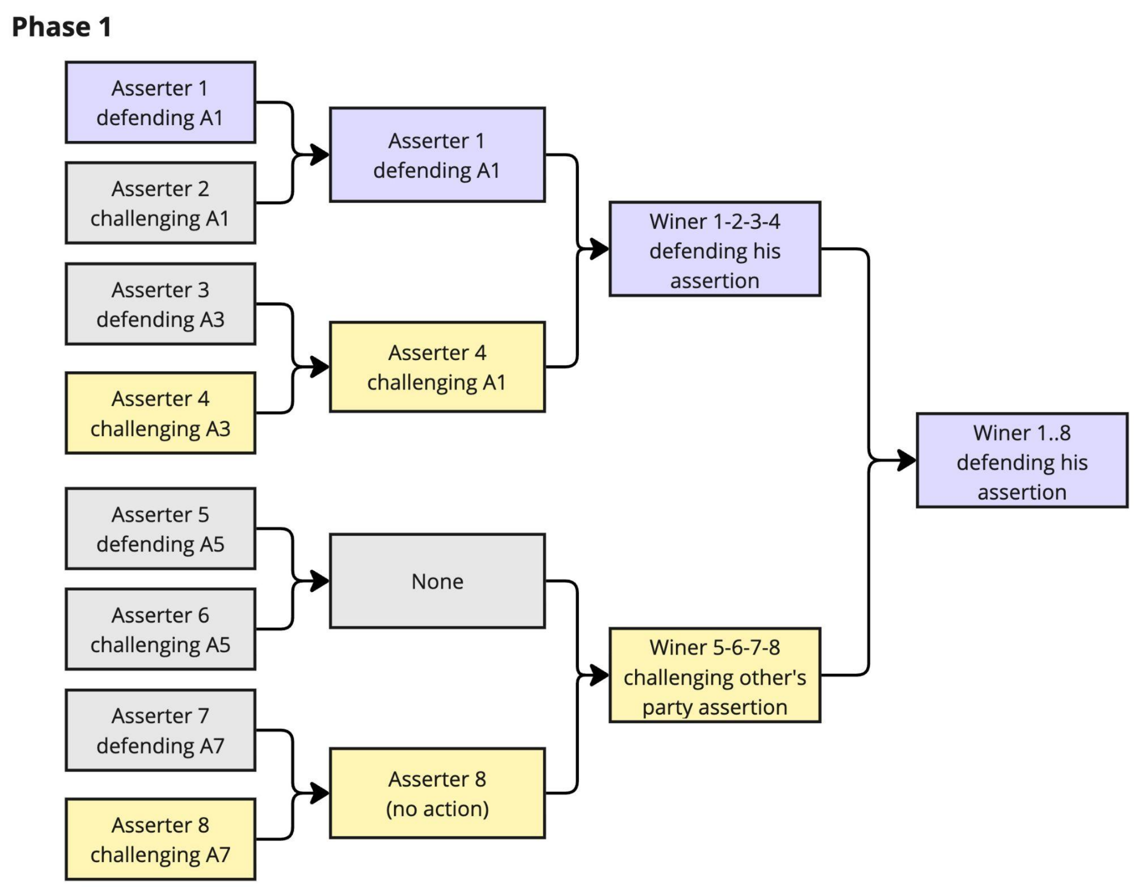
BATTLE For Bitcoin

Tournament Chain

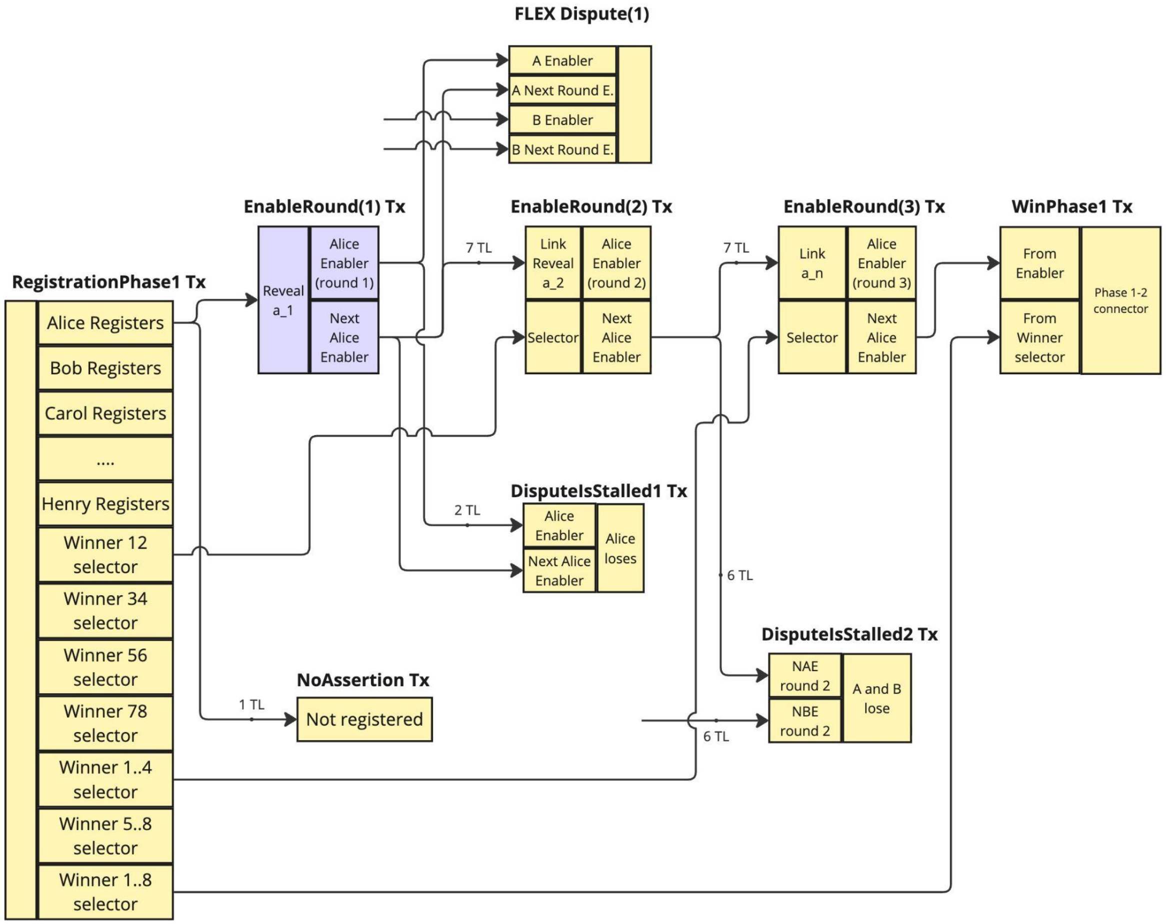


Phase 1 Transaction DAGs

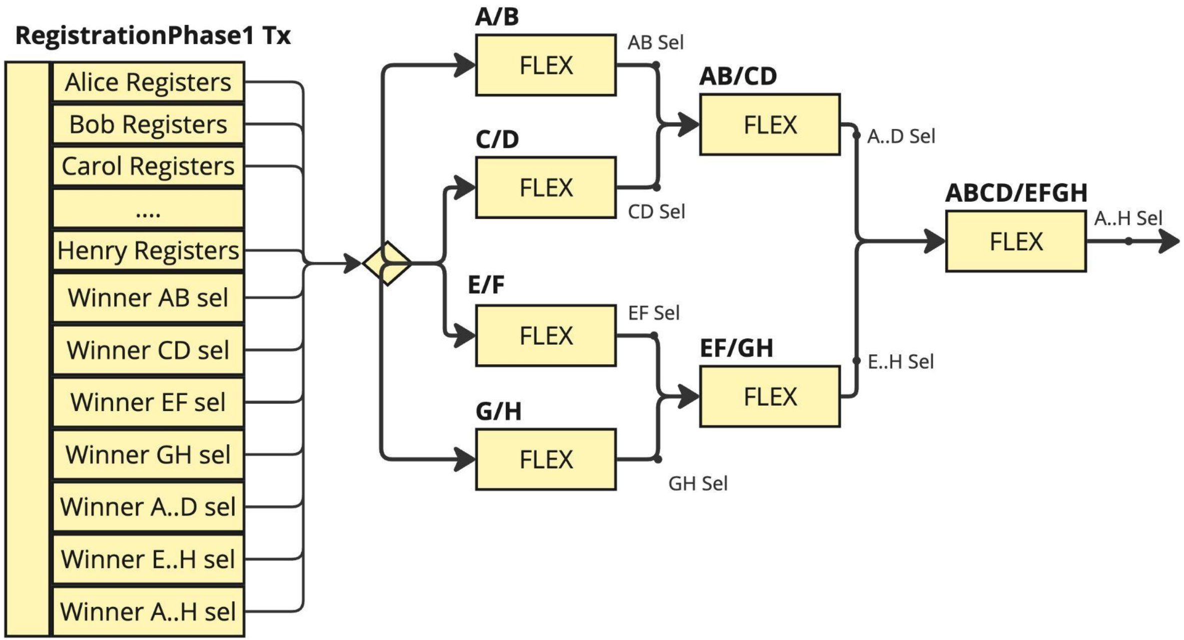
Phase 1 Schedules



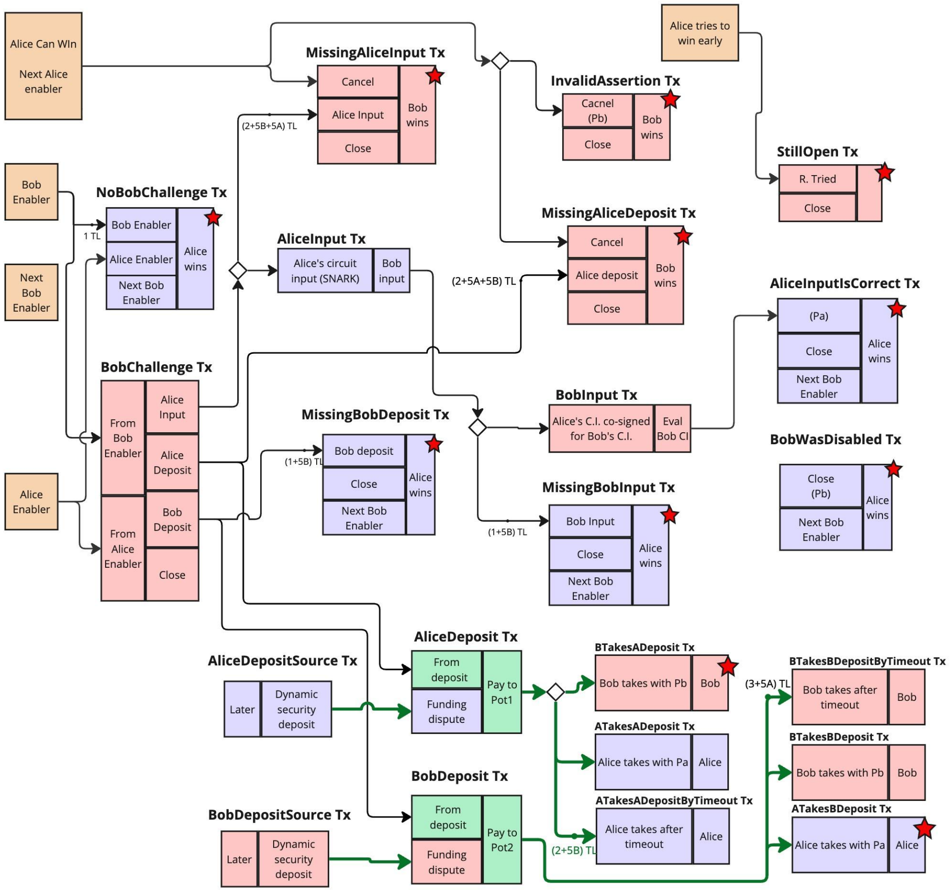
Phase 1 Enablement Chains



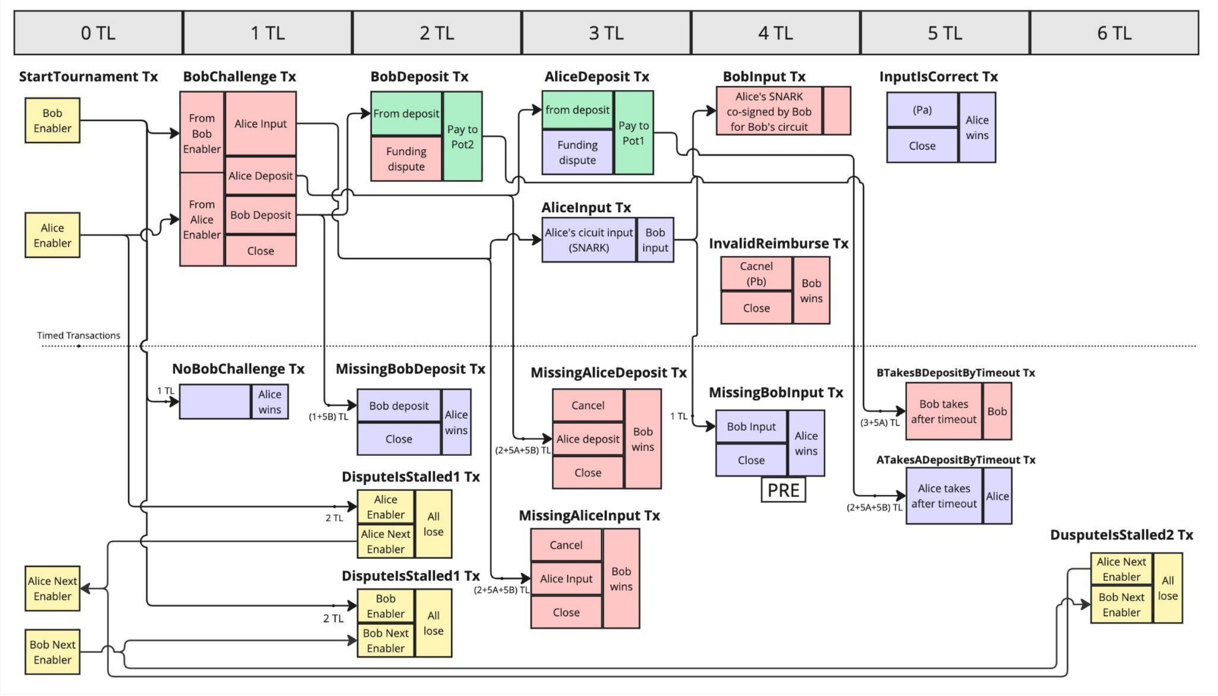
Phase 1


RegistrationPhase1 Tx
Alice Registers
Bob Registers
Carol Registers
....
Henry Registers
Winner AB sel
Winner CD sel
Winner EF sel
Winner GH sel
Winner A..D sel
Winner E..H sel
Winner A..H sel
A/B
FLEX
AB Sel
C/D
FLEX
CD Sel
E/F
FLEX
EF Sel
G/H
FLEX
GH Sel
AB/CD
FLEX
A..D Sel
EF/GH
FLEX
E..H Sel
ABCD/EFGH
FLEX
A..H Sel

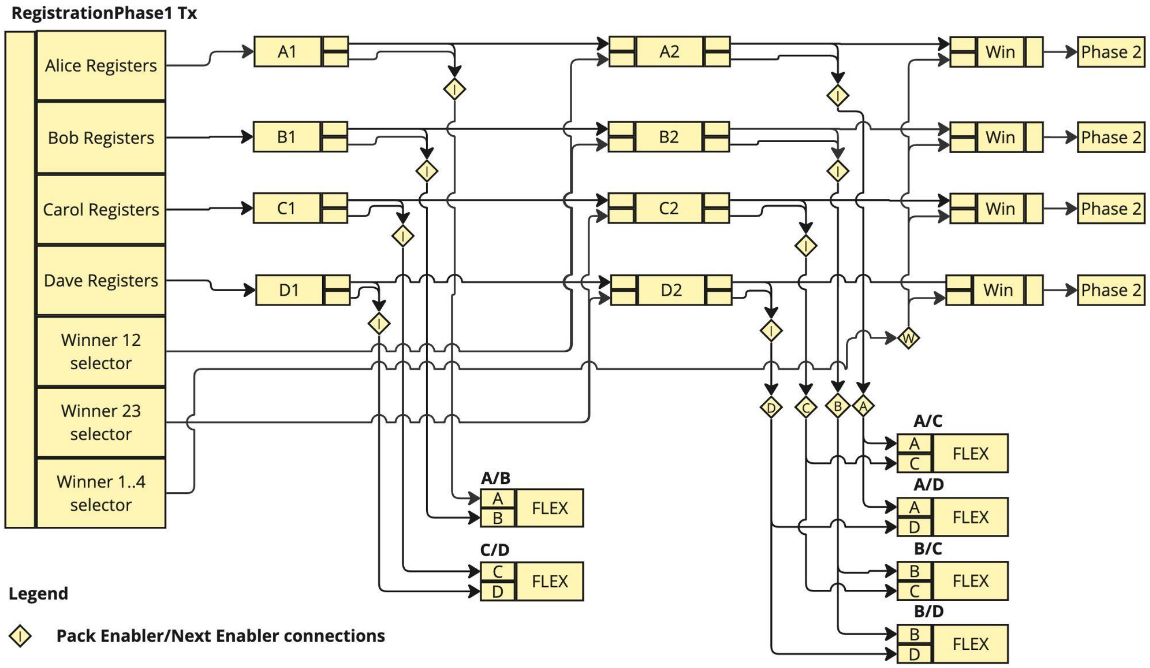
FLEX Component



FLEX Time restrictions

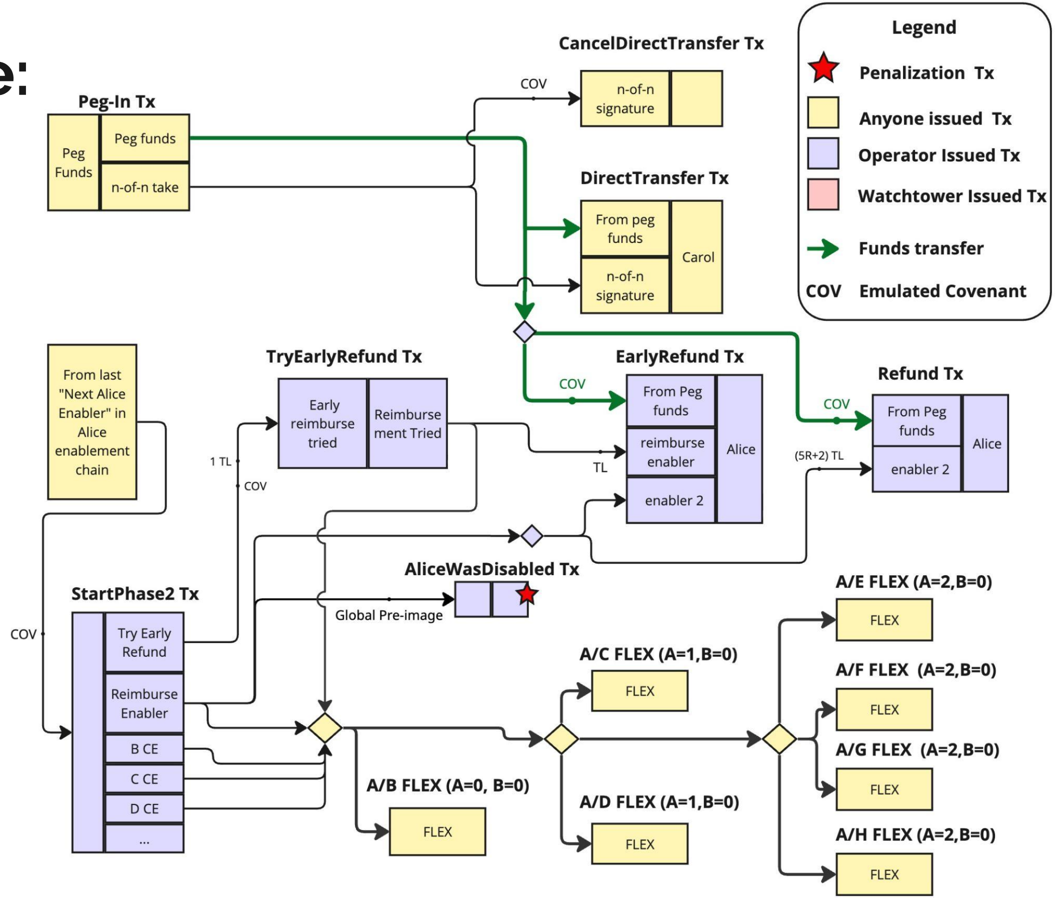


Phase 1 Example: Alice, Bob, Carol, Dave

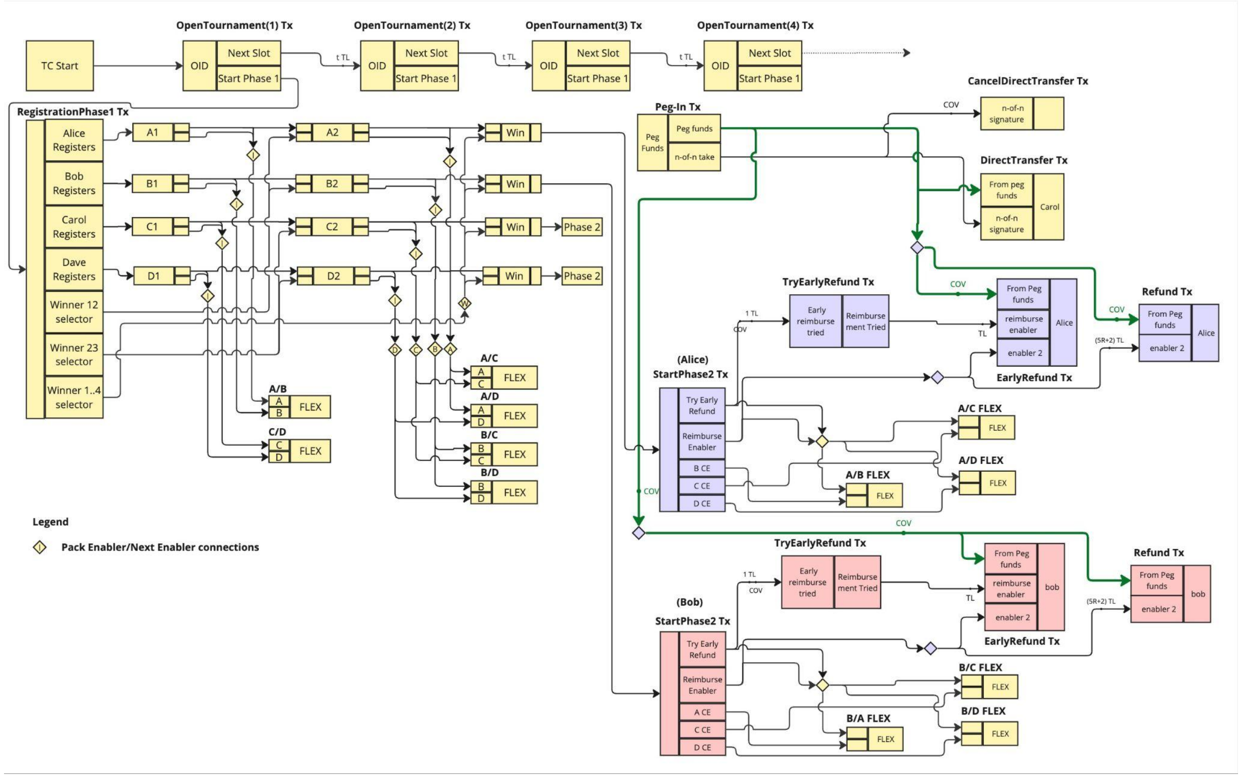


Phase 2 Transaction DAGs

Phase 2 Example: A to H



Combining All Together (2 Phases, 4 parties)



Summary

- **Two-phase tournament** with reward recycling: keeps honest asserter capital constant and resolves C challenges in O(logC) rounds via escalation schedules.
- **Bitcoin-native design**: FLEX/BitVM garbled-circuit disputes, per-move timelocks, on-demand L1 bonds, reusable escrowed rewards, stall handling.
- **Phase 1** uses enabler chains (winner cuts + third-party stall cuts) to yield a single surviving asserter;
- **Phase 2** the remaining challenges it with non-decreasing concurrency.
- **Admission/DoS control**: Tournament Chain rate-limits openings
- **Cost**: pre-signed material is O(N^2) and GC size dominates; per-peg-in DAGs amortize cost; practical near N ≈ 1000 operators.

Thank You!

Fairgate

www.fairgate.io

https://github.com/FairgateLabs

BitVMX

https://bitvmx.org