F3: Filecoin Fast Finality

Dante Cullari

CEO - Konvergence Inc.

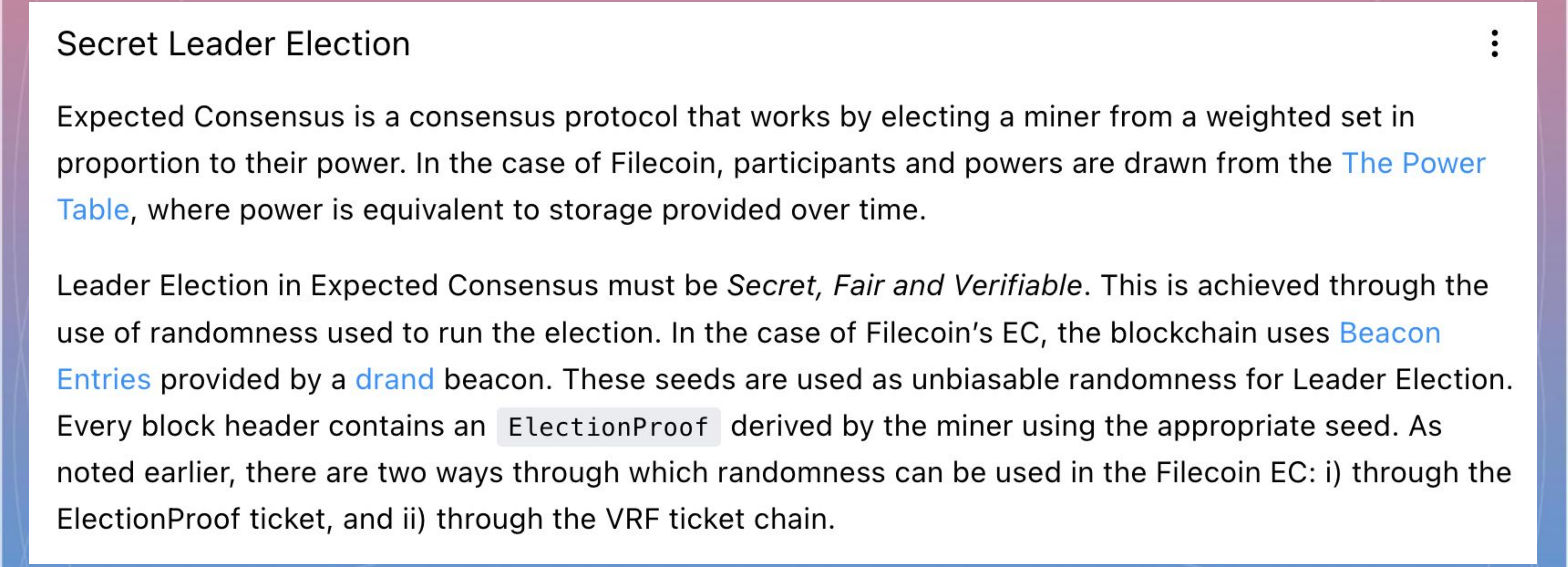
Web3 Architect, Full Stack Developer,
UI/UX Designer, Web Researcher

dante@raincloud.earth
https://raincloud.earth

Konvergence

Cloud Forest

Current Model: Expected Consensus



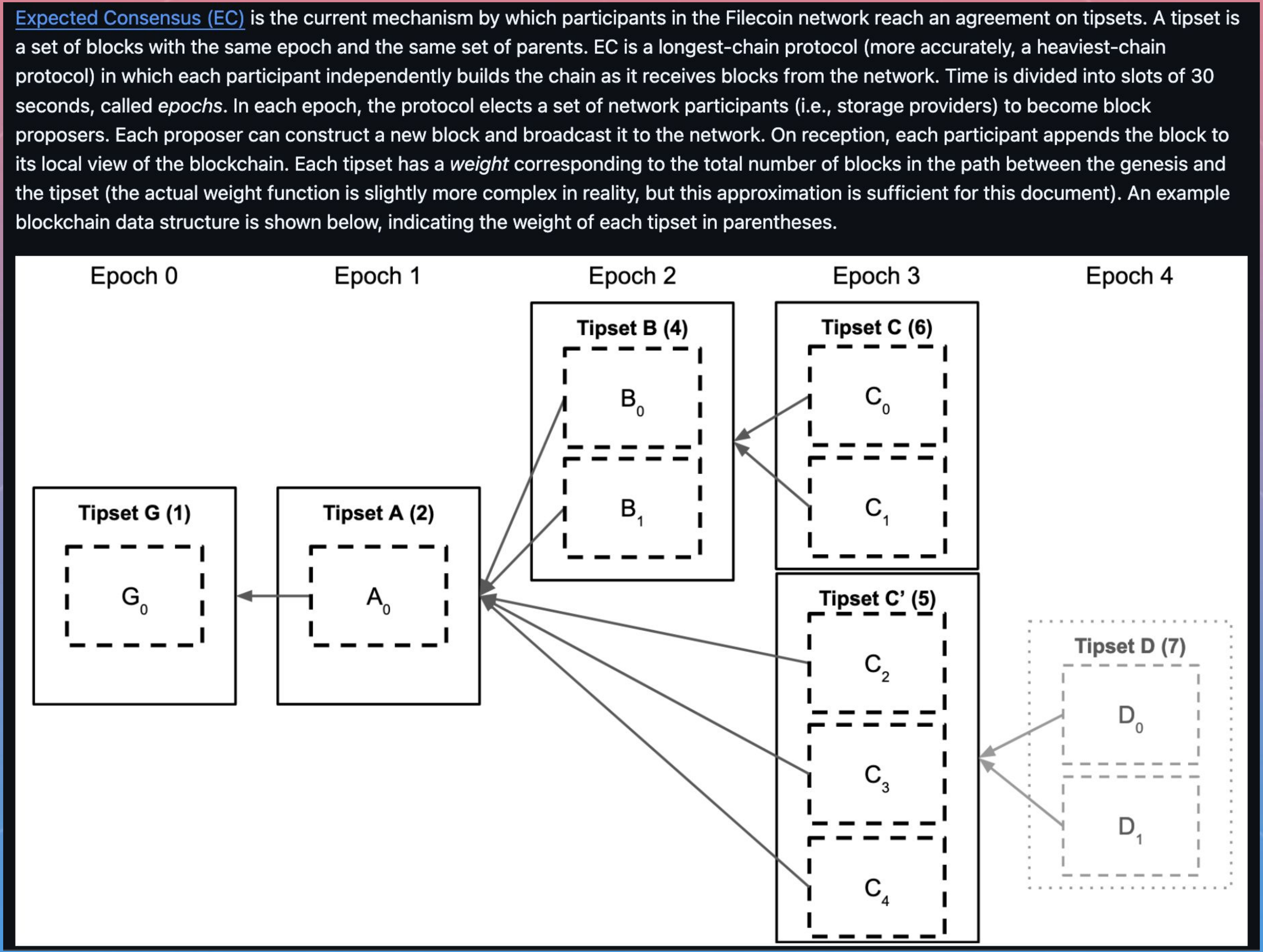
Secret Leader Election

Expected Consensus is a consensus protocol that works by electing a miner from a weighted set in proportion to their power. In the case of Filecoin, participants and powers are drawn from the The Power Table, where power is equivalent to storage provided over time.

Leader Election in Expected Consensus must be *Secret, Fair and Verifiable*. This is achieved through the use of randomness used to run the election. In the case of Filecoin's EC, the blockchain uses Beacon Entries provided by a drand beacon. These seeds are used as unbiasable randomness for Leader Election. Every block header contains an `ElectionProof` derived by the miner using the appropriate seed. As noted earlier, there are two ways through which randomness can be used in the Filecoin EC: i) through the ElectionProof ticket, and ii) through the VRF ticket chain.

https://spec.filecoin.io/algorithms/expected_consensus/

Filecoin Blocks & Tipsets

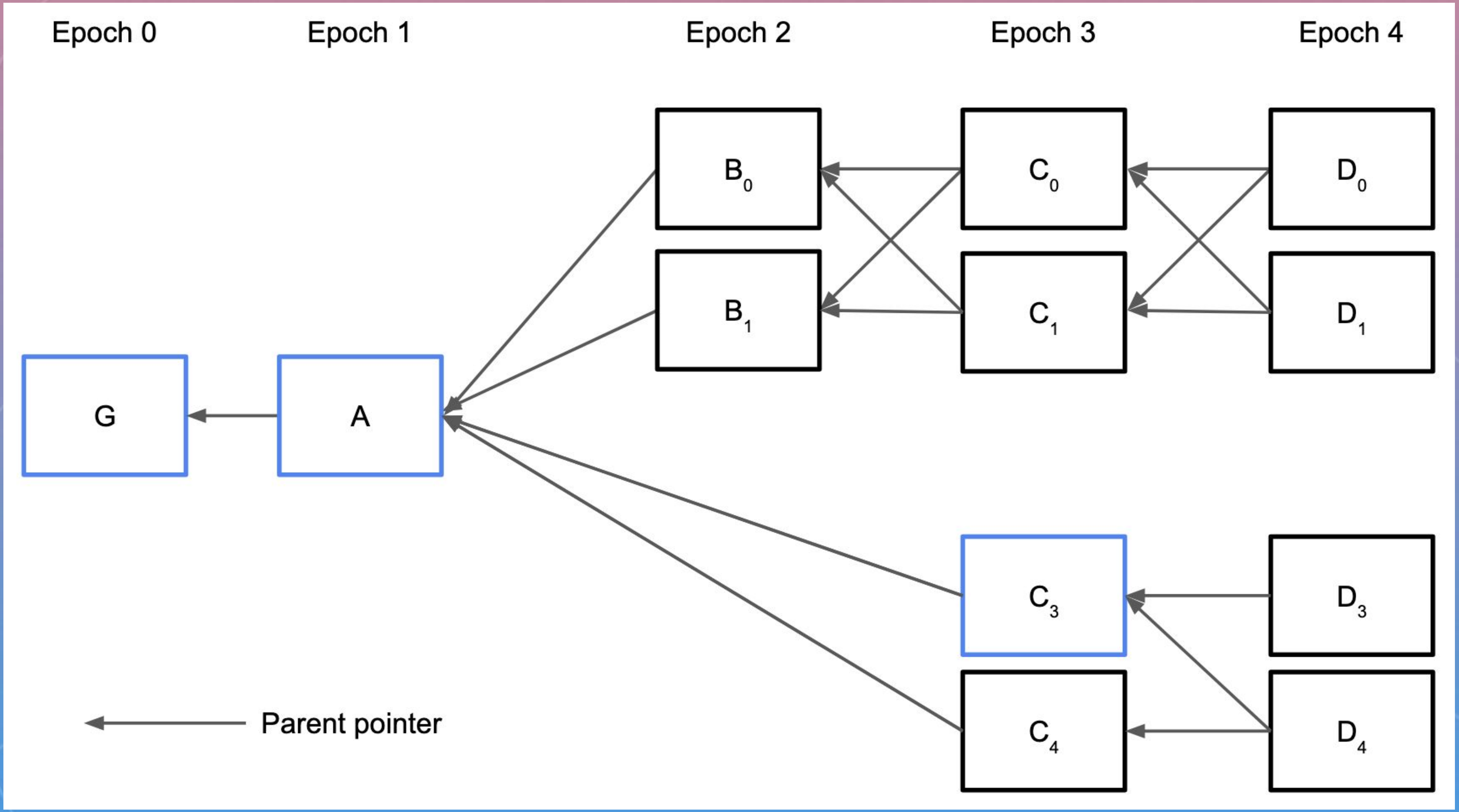


Expected Consensus (EC) is the current mechanism by which participants in the Filecoin network reach an agreement on tipsets. A tipset is a set of blocks with the same epoch and the same set of parents. EC is a longest-chain protocol (more accurately, a heaviest-chain protocol) in which each participant independently builds the chain as it receives blocks from the network. Time is divided into slots of 30 seconds, called *epochs*. In each epoch, the protocol elects a set of network participants (i.e., storage providers) to become block proposers. Each proposer can construct a new block and broadcast it to the network. On reception, each participant appends the block to its local view of the blockchain. Each tipset has a *weight* corresponding to the total number of blocks in the path between the genesis and the tipset (the actual weight function is slightly more complex in reality, but this approximation is sufficient for this document). An example blockchain data structure is shown below, indicating the weight of each tipset in parentheses.

More Reading:
https://github.com/filecoin-project/FIPs/blob/master/FIPS/fip-0086.md#GossiPBFT-Consensus

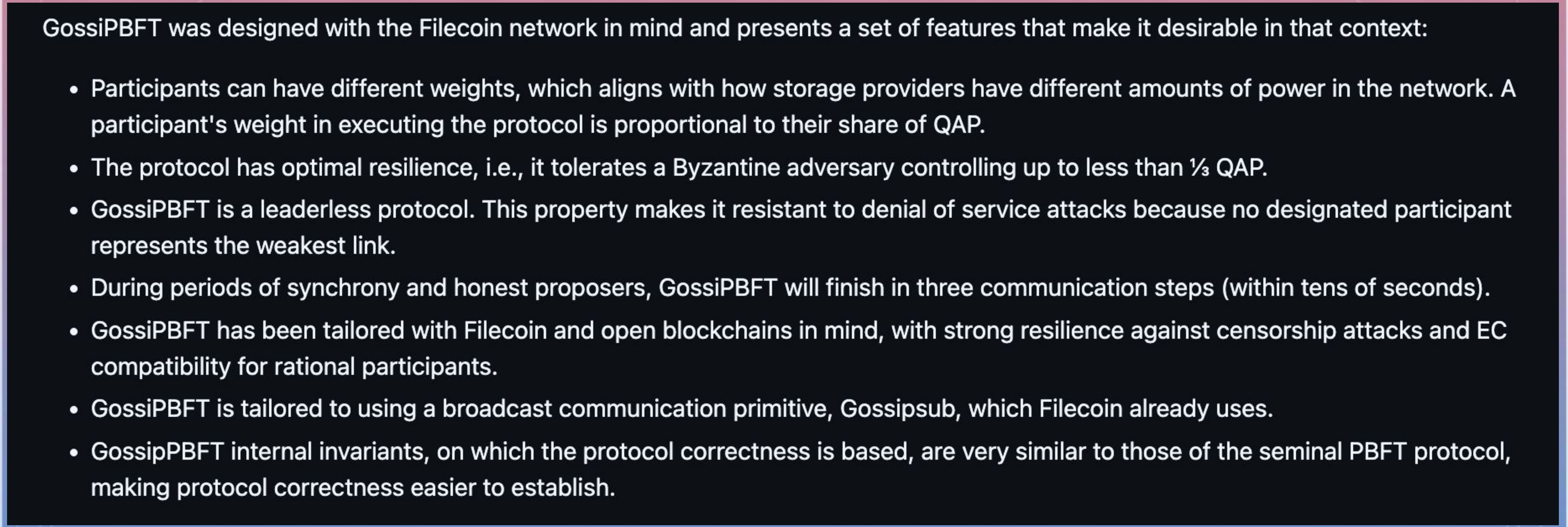
F3: GosiPBFT Consensus

GossiPBFT is a Byzantine fault-tolerant consensus protocol that is resilient-optimal, i.e., it tolerates up to less than ⅓ QAP being controlled by a Byzantine adversary. The committee for each instance of the protocol is known. Each participant inputs a proposal value, and the protocol outputs one of the input values as the final decision value. Unlike a longest-chain protocol, the output of GossiPBFT is permanent.



More Reading:
https://github.com/filecoin-project/FIPs/blob/master/FIPS/fip-0086.md#GossiPBFT-Consensus

F3 Benefits

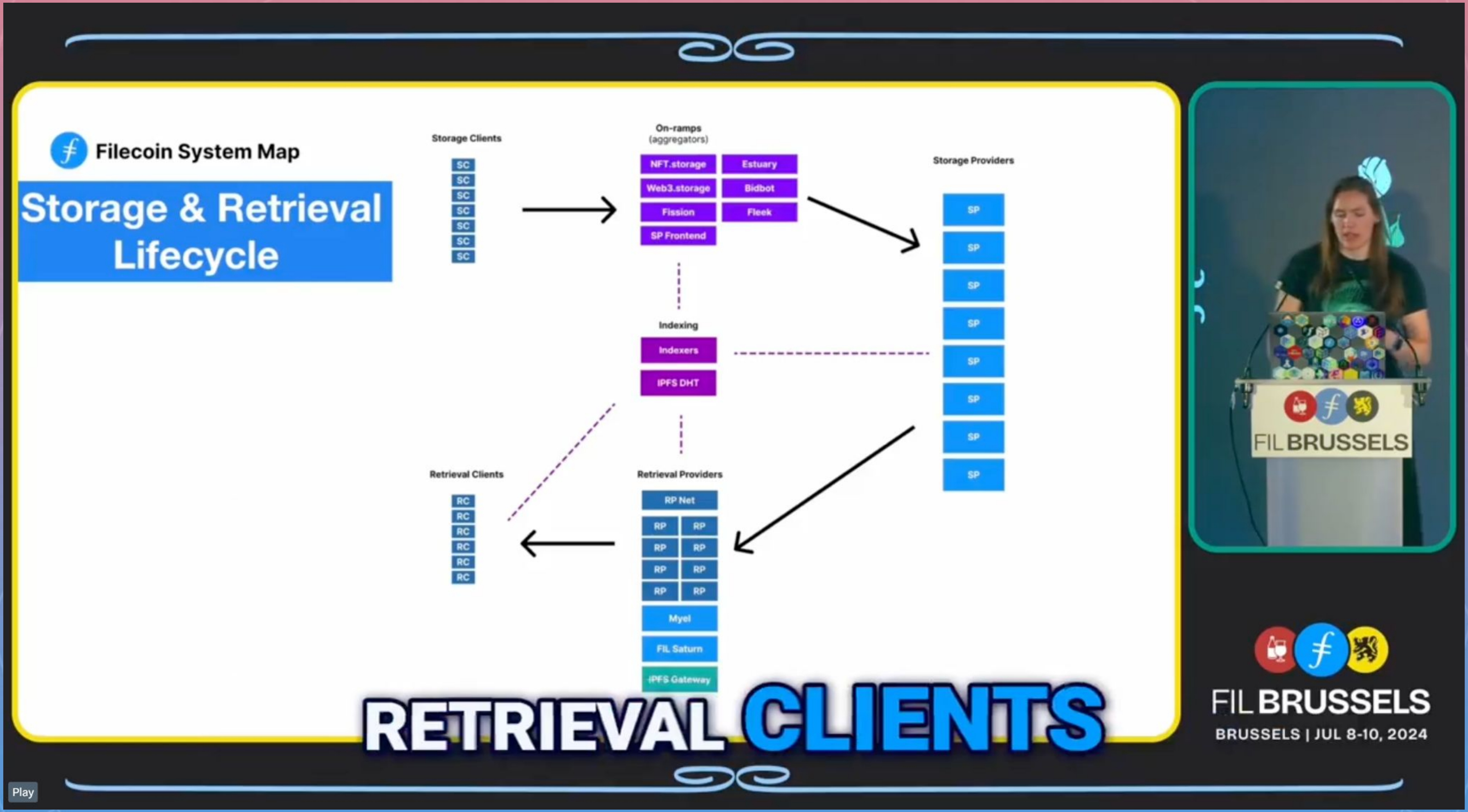


GossiPBFT was designed with the Filecoin network in mind and presents a set of features that make it desirable in that context:

- Participants can have different weights, which aligns with how storage providers have different amounts of power in the network. A participant's weight in executing the protocol is proportional to their share of QAP.
- The protocol has optimal resilience, i.e., it tolerates a Byzantine adversary controlling up to less than ⅓ QAP.
- GossiPBFT is a leaderless protocol. This property makes it resistant to denial of service attacks because no designated participant represents the weakest link.
- During periods of synchrony and honest proposers, GossiPBFT will finish in three communication steps (within tens of seconds).
- GossiPBFT has been tailored with Filecoin and open blockchains in mind, with strong resilience against censorship attacks and EC compatibility for rational participants.
- GossiPBFT is tailored to using a broadcast communication primitive, Gossipsub, which Filecoin already uses.
- GossipPBFT internal invariants, on which the protocol correctness is based, are very similar to those of the seminal PBFT protocol, making protocol correctness easier to establish.

More Reading:
https://github.com/filecoin-project/FIPs/blob/master/FIPS/fip-0086.md#GossiPBFT-Consensus

Quick Overview



Filecoin System Map

Storage & Retrieval Lifecycle

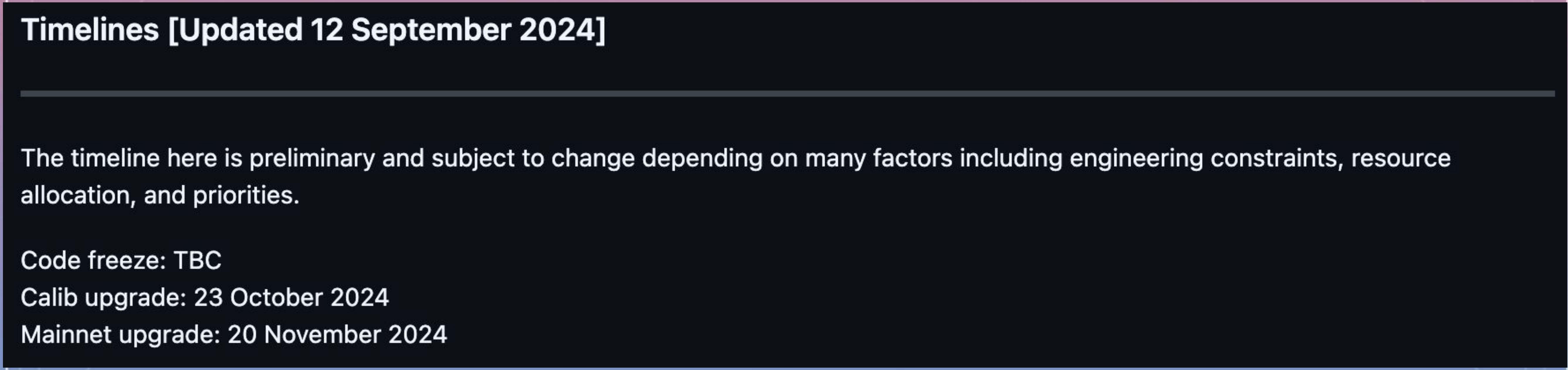
RETRIEVAL CLIENTS

FIL BRUSSELS

BRUSSELS | JUL 8-10, 2024

Video: https://x.com/FilFoundation/status/1816890790327275563

F3 Timeline



Timelines [Updated 12 September 2024]

The timeline here is preliminary and subject to change depending on many factors including engineering constraints, resource allocation, and priorities.

Code freeze: TBC
Calib upgrade: 23 October 2024
Mainnet upgrade: 20 November 2024

Further Reading on F3:
https://filecoin.io/blog/posts/how-f3-is-transforming-the-filecoin-network/

NV24 Update:
https://github.com/filecoin-project/core-devs/discussions/150#discussioncomment-10214831

JOIN FILECOIN DISCORD!

https://discord.cofm/invite/filecoin

Fill out our Survey!

Survey

- Filecoin Orbit Community Program Survey

Thank You

dante@raincloud.earth

https://raincloud.earth

https://twitter.com/KonvergenceInc