Emmy$^+$— Tezos' consensus algorithm

Eugen Zălinescu

Nomadic Labs internal presentations

28-11-2019

A consensus protocol for blockchains

- Properties
  - safety: ensure agreement between all nodes on a single chain
    - finality: when can a block be considered final?
      immediate/deterministic or probabilistic finality
  - liveness: the chain is not stuck
  - fairness: number of honest blocks proportional with number of honest nodes

- Type of actors
  - honest users
  - Byzantine attackers

A consensus protocol for blockchains

- Properties
  - safety: ensure agreement between all nodes on a single chain
    - finality: when can a block be considered final?
      immediate/deterministic or probabilistic finality
  - liveness: the chain is not stuck
  - fairness: number of honest blocks proportional with number of honest nodes
  - the optimal baker strategy is to follow the rules
- Type of actors
  - honest users
  - Byzantine attackers
  - rational agents

Tezos: a self-amending protocol

- Tezos blockchain = an economic protocol plugged in a generic shell
  - The shell asks the protocol the *fitness* of each chain and chooses the one with the highest fitness.
  - The shell asks the protocol whether blocks and operations are valid.
- Consensus properties ensured by the fitness and chain validity rules.
  - e.g. Bitcoin ensures probabilistic finality with:
    fitness = accumulated difficulty
    validity = valid PoW $\rightarrow$ on average, 10 minutes between blocks

Tezos: a Proof-of-Stake system

- Block producers are chosen at random in proportion with their stake.
  - This is realized through an infinite list of priorities per level.
  - In each cycle n, a random seed is derived deterministically, on-chain, using commit&reveal.

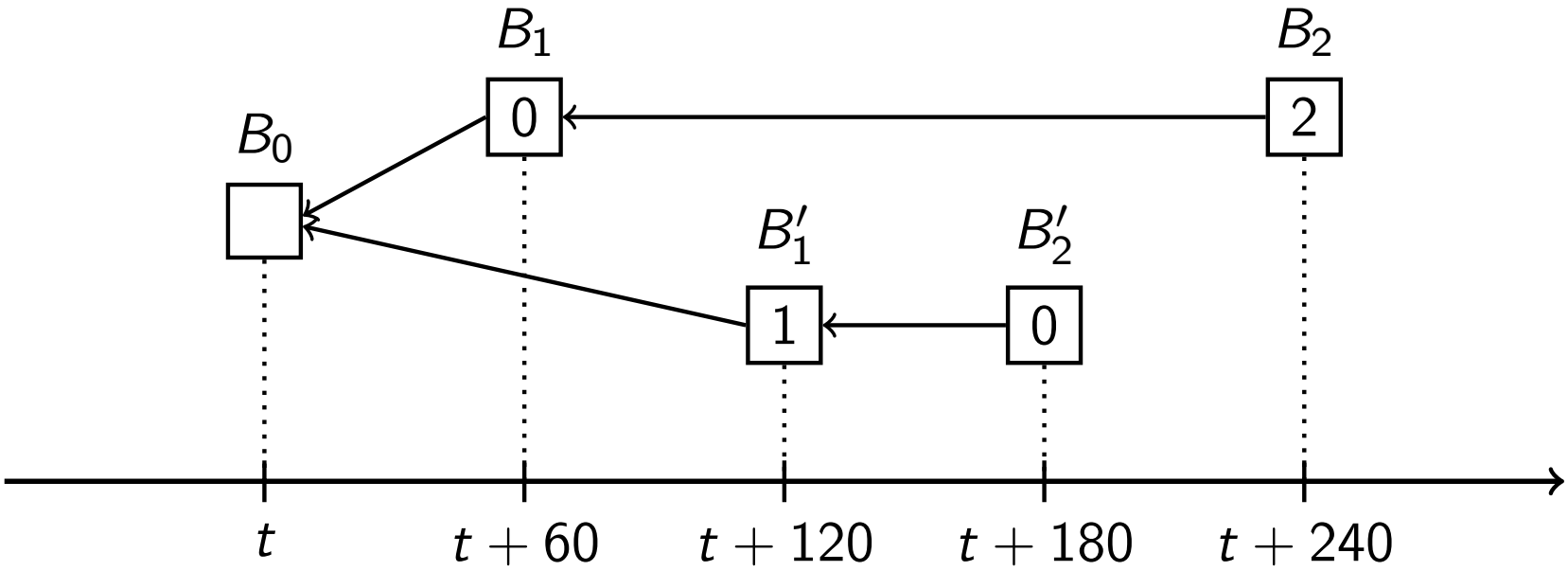
- The (incomplete and approximate) rules:
  - fitness = chain length
  - validity = minimal time between blocks, depending on block priority:
    $$\mathit{delay}(p) = 60 \cdot (p + 1)$$
- These already ensure probabilistic finality against Byzantine attackers
  - in the short run there can be forks:
    - assume the attacker has priority 0 for levels $\ell + 1, \ldots, \ell + k$
    - she proposes the chain $B_{\ell+1} \ldots B_{\ell+k}$ to some nodes
    - she proposes the chain $B'_{\ell+1} \ldots B'_{\ell+k}$ to some other nodes
  - in the long run, the honest chain is the faster chain

Incentives

- Rational actors model is more realistic.
- Incentives and slashing are needed:
  - incentives to indirectly punish non-participation
  - slashing to prevent double spending and nothing-at-stake problems

Incentives

- Rational actors model is more realistic.
- Incentives and slashing are needed:
  - incentives to indirectly punish non-participation
  - slashing to prevent double spending and nothing-at-stake problems
- However, rewards can also lead to "selfish baking"



Endorsements

- An endorsement is a signature on a block.
  - included in the block at the next level
- Endorsing rights are given similarly to baking rights.
  - 32 endorsers are picked independently at random.
- Role
  - reduce selfish baking
  - improve finality
  - encourage participation of smaller delegates

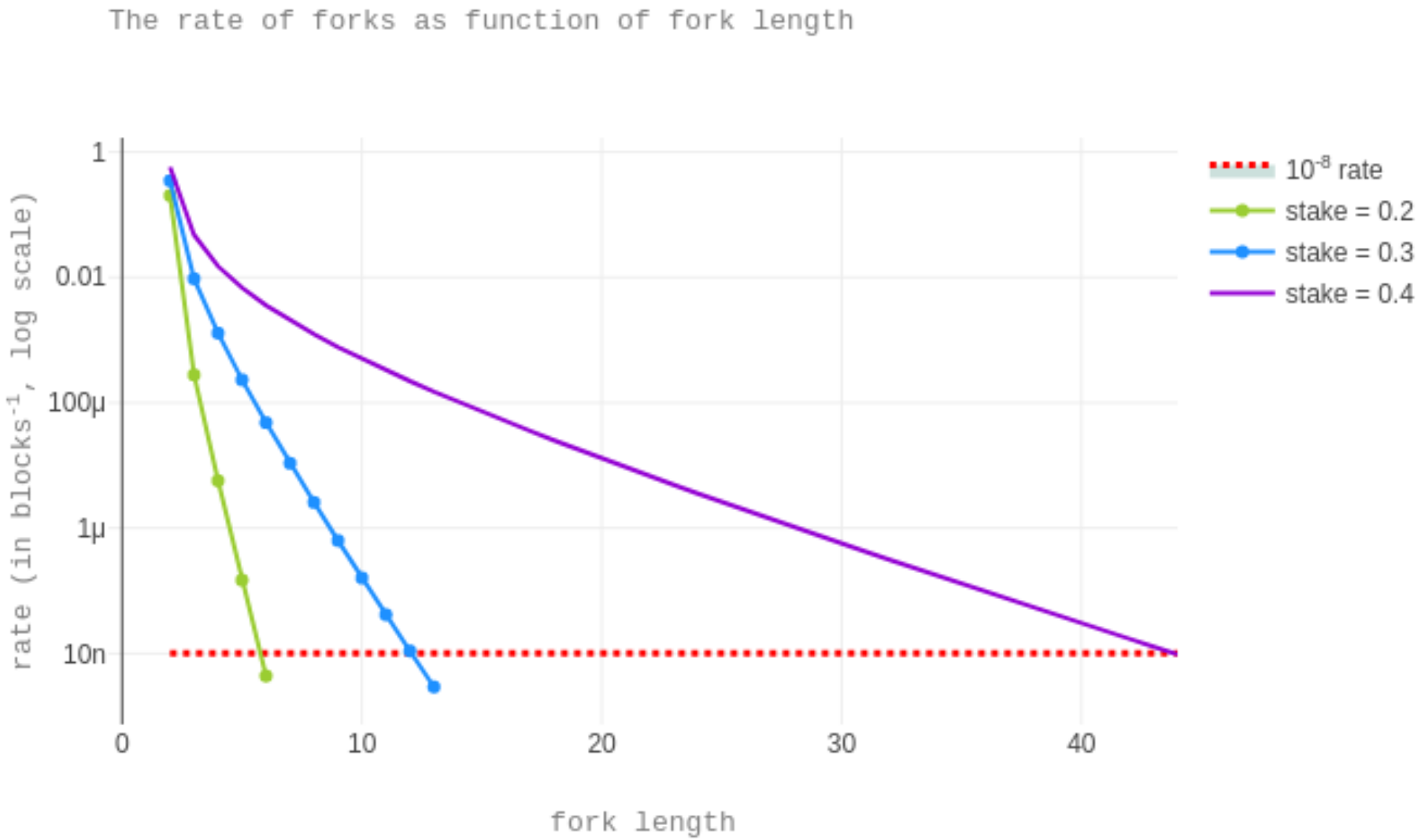
Emmy

- Endorsements count towards the fitness.
- unclear optimal strategy for bakers: tension between
  - send block right away, but fitness might be too small
  - wait for more endorsements
- whether the chain is "healthy" split into two aspects:
  - fitness
  - block delay/priority
- hard to analyze
- selfish baking not negligible

Emmy$^+$

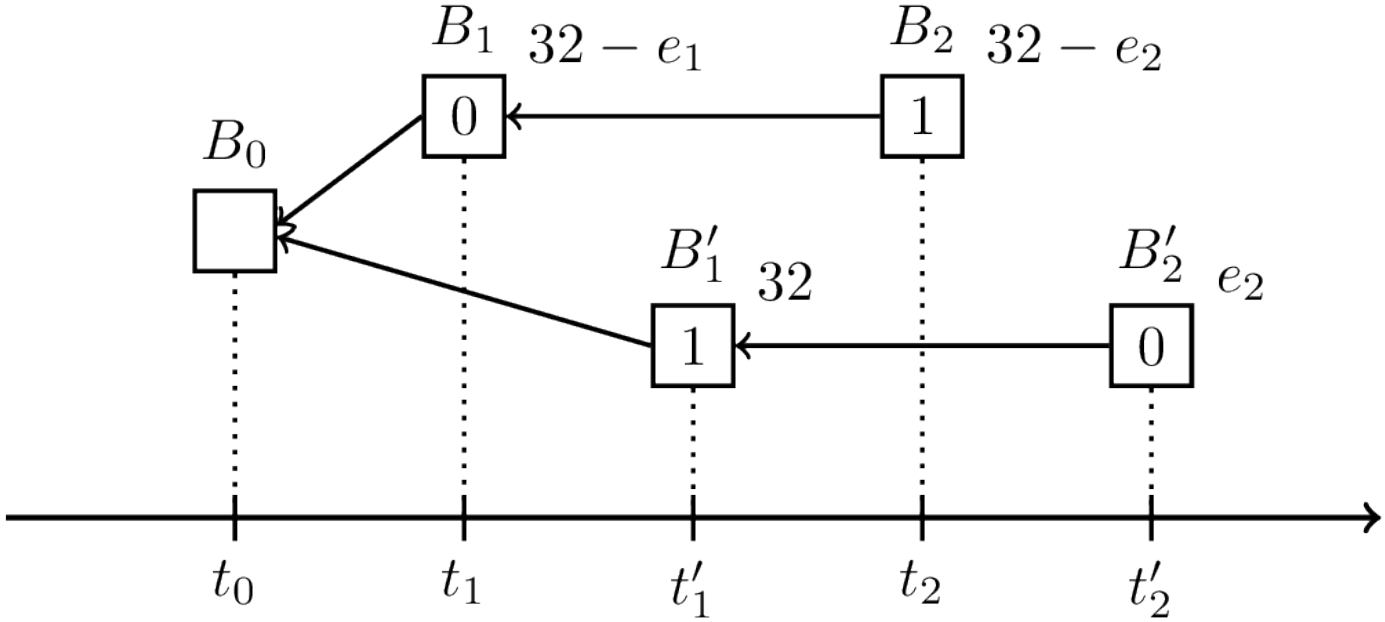
- Give more weight to a chain through timing.
  - fewer endorsements $\rightarrow$ slower chain
    $delay(p, e) = 60 + 40 \cdot p + 8 \cdot \max(0, 24 - e)$
    $delay(p, e) = 60 + dp \cdot p + de \cdot \max(0, ie - e)$
  - a clearer notion of "chain health":
    - the delay of the chain with respect to the "healthiest" chain, where all blocks baked at priority 0 and with all endorsements

Rate of malicious forks



Selfish baking

- The baker's strategy is to withhold his endorsements in order to slow down the honest chain.



- Dishonest baker "steals" block if

$$\mathit{delay}(1, 32) + \mathit{delay}(0, e_2) < \mathit{delay}(0, 32 - e_1) + \mathit{delay}(1, 32 - e_2)$$

That is, $40 < e_1 + 2e_2$.

The dp/de ratio

- It is the ratio dp/de that matters:

$$delay(p, e) > delay(p', e')$$
$$\Leftrightarrow$$
$$\frac{dp}{de} > \frac{\max(0, ie - e') - \max(0, ie - e)}{p - p'}$$

- Assuming dp fixed,
  - a small de gives less weight to endorsements
  - a big de means less endorsements needed to steal a block
- Trade-off value: $dp/de = 5$
- $dp = 40$ (why not?) implies $de = 8$

On the value of *ie*

- The "first" $(32 - ie)$ missing endorsements do not penalize the baker
  - A big value (like $ie = 32$) means less endorsements needed to steal a block
    - Number of endorsements needed to steal a block is $(32 - ie) + dp/de$.
- The higher the *ie*, the more weight we give to the number of endorsements on the chain.
  - higher *ie*, fewer chances for an attacker to build a faster alternative chain

Future work

- improve and extend the current analysis
  - understand better the impact of the design and the constants
  - take inflation into account
- perform simulations

Rate of malicious forks (2)

- Assume transaction included n blocks ago
- In these n observed blocks:
  - 1/4 of endorsements are being missed per level and no skipped priorities