Security at Stake?

Christopher Goes

In this presentation

- Nakamoto consensus
- Desiderata: progress, agreement
- Proof-of-stake incentives
- Breaking progress
- Breaking agreement
- Countermeasures
- Future directions
- Informed stakeholder tips
- Further resources

Nakamoto consensus

- Blocks of transactions, in a chain
- Miners/bakers vote on a history
    - PoW: hashpower
    - PoS: signatures
    - Voting must be scarce
    - Also produce blocks (non-essential)
- Fork choice rule
- Probabilistic threshold (*n* confirmations)

Desideratum: Progress

- Blocks continue to be appended
- Meaningfully: also non-censorship
    - One proposer censoring: ok
    - Lots of proposers censoring: not great
    - >=50% (Nakamoto) censoring: terrible

Desideratum: Agreement

- Any two network participants agree on value
    - Otherwise: double-spend!
- Subjective confirmation threshold
    - More difficult to “undo” over time - more work / more signatures

Breaking progress

- Network-layer
    - Partial network control - slow down
- Consensus-layer
    - Selfish mining
        - Hide higher-fitness chain temporarily
        - Reveal once block published
        - Force other baker to waste time, maybe slot
        - Also other direction: build on lower-priority block
            - Maybe ask for a bribe!
    - Nil-voting (threshold BFT)
    - Nakamoto consensus: harder to stop, can slow
- Selective censorship
    - See tx to exchange, censor, front-run
    - Oracles too

Breaking agreement

- Network-layer attacks
  - Total control: eclipse (although ~detectable)
- Consensus-layer attacks
  - Nakamoto consensus: “51%”
  - Then can arbitrary censor, deep fork
  - More stake, deeper possible fork
  - PoS: stake is not scarce!
    - Nothing-at-stake problem
    - Bonding period
  - Opportunistic bribery: cheaper
    - Especially if services use flat threshold
    - Can be automated, hard to punish

Proof-of-stake incentive design

- Carrot and/or stick
    - Lots of design space, all in the state machine
- Incentivize uptime
    - Block reward, endorsement rewards
- Punish any cause of consensus-at-risk
    - Slash a lot for double-signing
- Punish “selfish mining” attack class as possible
    - Endorsement rewards decrease on later-priority blocks
- Some things are hard
    - Punishing censorship not easily possible (yet)
        - Maybe: threshold decryption

Edge cases

- Easy analysis with <<½ stake
  - Consensus attacks not damaging
  - Can incentivize secure setups
- More difficult at threshold
  - No effective double-signing penalty due to censorship
- Intricate incentives hard to get right
  - Want: rewards linear in stake
  - Likely: slightly superlinear
- Bribery
  - Impossible to know off-chain incentives ahead of time
  - Maybe service providers should cost attacks explicitly

Countermeasures

- Detection / mitigation
  - Speed tradeoffs
- Reducing baker power
  - Threshold tx decryption
  - “Social punishment” from delegators
- Encourage attacks
  - Reward for hacking
  - Increase real-world consensus-attack cost
- Hybrid consensus
  - Different attack surfaces
- Fork threat
  - Certain attack class = only option
  - Dependent on off-chain social consensus

Possible future directions

- PoS derivatives
    - Tokenized bonds, index funds
    - “Bet” on baker, endorser performance
        - Consensus participants can influence results
    - Derivative market > base market = dangerous
        - Buy some network token
        - Short more than you bought
        - Break consensus!
        - Who will lend?
- Cross-chain consensus
    - Notarization (PoW, PoS)
    - Easier: backup coordination mechanism

Informed stakeholder tips

- PoS is very experimental
  - Promise vs PoW: quiescent, less centralized, faster
  - Way more design space
  - Not stress-tested yet: may totally break!
- Understand network roles
  - Delegation = voting, not just rewards
    - More relevant long-term
    - Tragedy-of-the-commons problems
- Multiplayer game
  - Unlike nation-state governance, no finite resource (eqv. land)
  - Fitness selection function on blockchains: governance quality
    - Proposing helpful changes
    - Passing the right proposals
    - Rejecting the wrong proposals

Further resources

- Tezos PoS [Official Gitlab]
  - https://tezos.gitlab.io/tezos/whitedoc/proof_of_stake.html
- Tezos Governance [Jacob Arluck]
  - https://medium.com/tezos/amending-tezos-b77949d97e1e
- How to Write Protocol Upgrades [Cryptium Labs]
  - Coming soon!