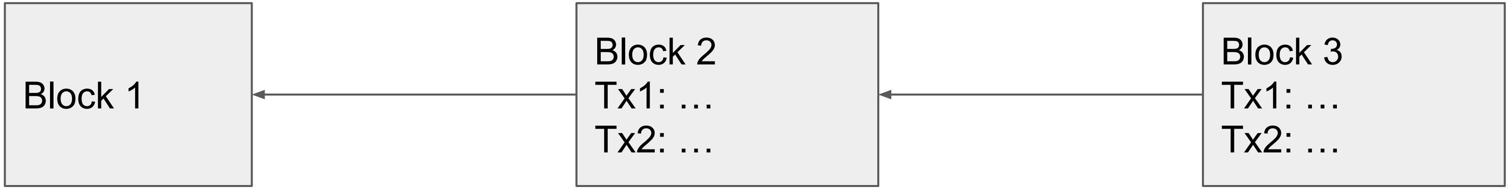
Multi-chain communication with proof of authority

Jessica Taylor
jessica@gigascaling.net

Regular blockchains (Bitcoin, Ethereum)



- “A → B” means “A includes hash code of B”
- Proof-of-work or proof-of-stake (details omitted)
- All full nodes download and verify every transaction

Why multi-chain?

- If there are n users of a chain and each makes k transactions, total work (bandwidth, compute, storage) is $O(kn^2)$
- If the n users are instead evenly distributed across c chains, total work is $O(ck(n/c)^2) = O(kn^2/c)$
- Problem: 51% attacks are easier since each chain is smaller
  - Proof-of-work is out
  - Proof-of-stake may work if stakers don't always sell tokens at market price (compare: publicly traded company)
  - Proof-of-authority as an alternative to proof-of-stake (compare: private company)
- Problem: no cross-chain communication
  - We show a solution using proof-of-authority

Proof of authority (basics)

- Each chain has an authority token (possibly transferable)
- Each new block must be signed by holders of a majority of authority tokens
- These authorities assert that the block is valid and that there aren’t alternative competing blocks
- Overall similar to proof-of-stake
- Differences with proof of stake
  - Sign by majority instead of random sample (more workable for smaller chains)
  - Separate authority token from commerce token

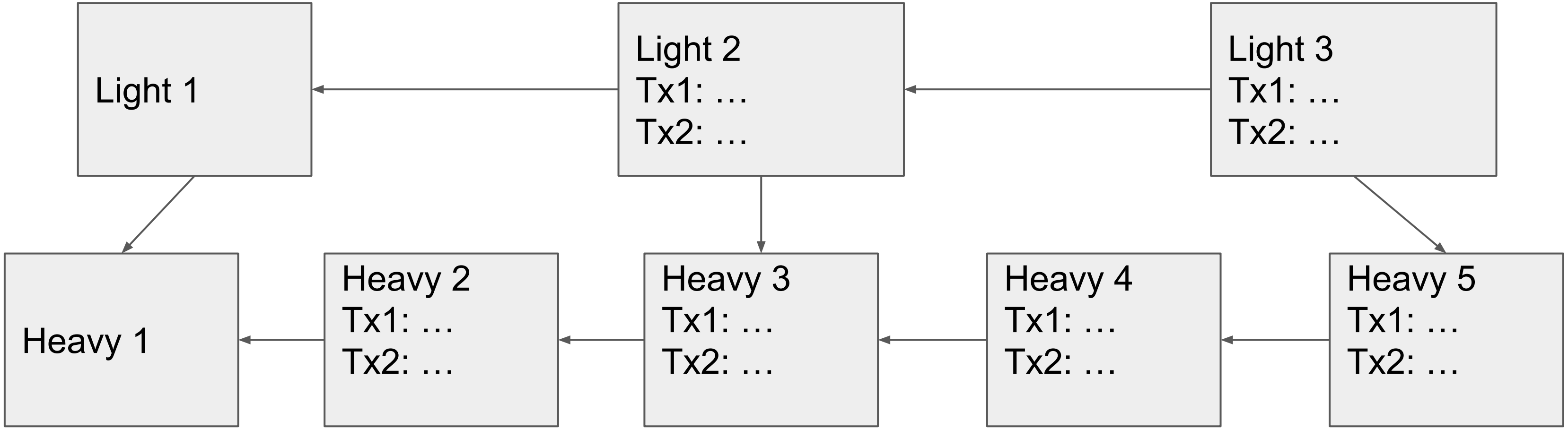
Error handling

- Problem: authority signs invalid block
  - This is easy to prove
  - Slash authority token
- Problem: authority signs multiple blocks
  - Also easy to prove
- Problem: authorities commit to signing different blocks, none has >50%
  - Similar to proof of stake, wait for a new round
- Problem: no majority of authorities signs any new blocks
  - Rare case
  - Outsiders can see lack of progress
- Problem: majority of authorities signs an unavailable block
  - Rare case
  - Authorities can be challenged to reveal blocks
- In last two cases, can restart the chain from the last checkpoint with new authorities

Analogy: corporations

- Corporations A and B don’t keep track of most of each others’ internal operations
- However, they keep track of who the authorities are, e.g. CEO
- They by default trust that statements made by the authorities about the corporation’s activities are true
- They also allow these statements to be disproven by other corporation members (trust but verify)
- Members of A store a “heavy” history of A and a “light” history of B, and vice versa

Light blockchains



- Heavy chain has more frequent blocks
- Light transactions are a subset of heavy transactions
- Heavy block hashes are signed by authorities
- Light blockchain contains enough information to infer authorities
  - New light block whenever authority token allocation changes

Light clients

- A light client only stores the light blockchain
- This has enough information to read the heavy blockchain lazily, as long as authorities are honest
- Dishonest authorities can be challenged *on the light chain*, so light clients keep track of authority challenges

Cross-chain messaging

- Suppose chain A and chain B are communicating
- Every heavy client of A contains a light client for B and vice versa
- On heavy chain A, an assertion is made: light chain B includes block with hash *x*
  - If true, *x* can be used to prove the contents of any B block in *x* or before
  - E.g. prove a certain transaction was made
- Evidence (on heavy chain A): present all unknown light blocks of B up to *x* and beyond
  - Each light block must be valid
- Possible refutations
  - A significantly longer B chain not containing *x*
  - An invalid heavy block corresponding to a light block
  - A heavy block's data (referred to by a light block of B) is unavailable
- Assertions, evidence, and refutations occur on heavy chain A
- Provide a time window for refutations

Applications

- Multi-token system
  - Each token is its own chain
  - Transfers can be proven without having to download the whole chain
- Gaming
  - Each game is its own blockchain
  - Results of a completed game can be proven to others, e.g. a scoreboard
- Forums
  - Each forum is its own blockchain
  - Light users of a forum don’t download the whole history, just enough to display the posts they’re looking at