

PROOFS OF SPACE AND TIME

REMOVING WASTE BY BRAM COHEN

CRYPTOCURRENCIES REQUIRE WASTE

- It's impossible to make a secure distributed database, but there's a loophole
- Proofs of work can secure a database, but they require waste
- Mining rewards will be pursued with resources until the value of the resources roughly equals the rewards

THE LOOPHOLE IN THE LOOPHOLE

- If there's already an existing resource with sunk cost whose value is greater rate than the value of the mining rewards
- And which it costs no additional resources to mine
- Then mining returns will go to $(\text{mining rewards}) / (\text{total world value of depreciation})$
- So buying resources to mine would lose money

THE SOLUTION: PROOFS OF SPACE

- There are massive amounts of unused online storage in the world
- Requires no additional power to mine
- No potential for ASICs
- The available miners are highly decentralized
- But the devil is in the details

STATE OF THE ART: SPACEMINT

- Gets mauled by re-mining since genesis. If the mining rate now is much higher than historically, then a small minority miner today can make a complete blockchain with greater weight than the 'real' one
- Rewards are highly variable, so there's some incentive to mine orphans

AN IMPROVEMENT: PROOFS OF SPACE AND TIME

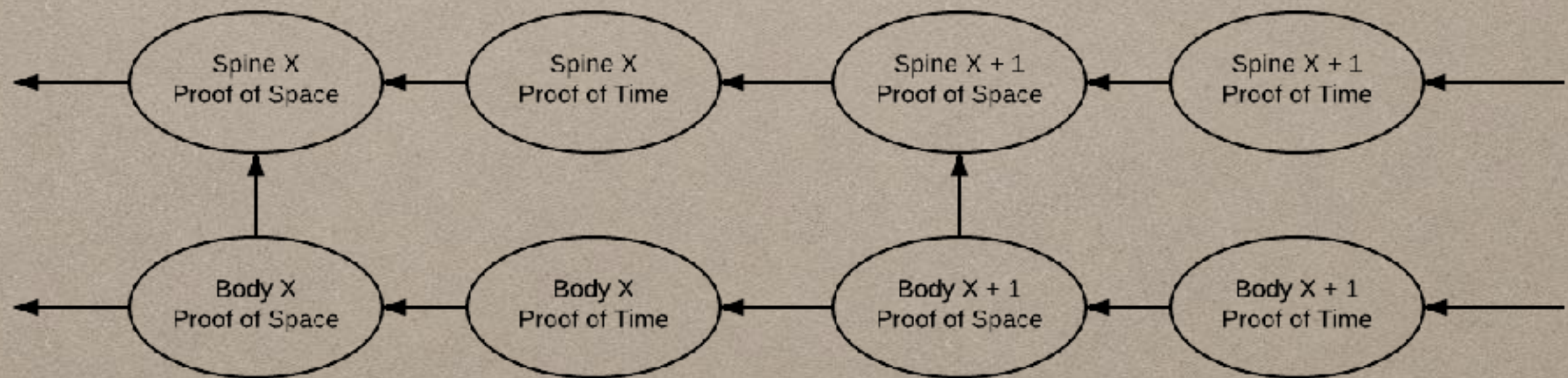
- Alternate proofs of space and proof of time and require that the product of the two meet the work threshold
- No re-mining since genesis because an attacker won't be able to extend the weight of their alternative chain faster than the real one gets extended
- Rewards are fixed amount so little incentive to mine orphans

PROOFS OF SPACE AND TIME (CONTINUED)

- Proofs of space are screamed out and no direct reward for time - people do it to keep everyone else honest
- Time distribution exactly mimics Bitcoin's
- Has $\frac{1}{3}$ attacks instead of $\frac{1}{2}$ attacks, can be slightly improved by using sum quality of last two proofs of space
- Proofs of time must be completely canonical

BLOCKCHAIN STRUCTURE

- Spine has just challenges, responses, and very quantized work difficulty adjustments
- Body also includes transactions and timestamps



PROOF OF TIME: MODULAR ROOTS

- In group of order 2^k , square $k-1$ times to find a square root
- Beautifully simple and robust with good constant factor, but times are linearish on proof size
- If proof sizes could be improved to even be the square root size we'd be in business
- Please help!

PROOF OF TIME: WITNESS SEGREGATION

- Only the challenge response needs to be canonical, the witness can be malleable
- Snarks proofs of repeated hashing are small and quick to verify
- But the ratio of time to make the snarks proof and get the value is way too high
- Please help!

PROOF OF TIME: REPEATED HASHING

- Adding in checkpoints makes verification in parallel possible
- Hashing all previous checkpoints makes spot checking highly effective
- Trivial fraud proofs - just point out which position is wrong
- Works, but needs fraud proofs, and yuck

PROOF OF SPACE: ELEGANT BUT BUSTED

- Store hashes of public keys in sorted order (simplifying, you'd really use salt)
- When a challenge comes in, look up the closest public key and use that as a response
- Beautiful and simple, but Hellman's Time/Memory Trade-Offs kill it

PROOF OF SPACE: FIXED ELEGANT APPROACH

- Almost as elegant as the simple approach
- Uses loophole in Hellman tradeoffs: Requires whole data set be calculated up front (loophole in loophole in loophole)
- First iteration works great, might be enough
- Later iterations need improvement. Please help!

PROOF OF SPACE: PEBBLING

- Malleability problems, resulting in:
- Requires on-chain registration