mas.s62
lecture 22
Alternate consensus mechanisms

2018-05-02

Tadge Dryja

today

alternate consensus:

- unique node lists
- proof of stake
- variants: delegated
- proof of space
- directed acyclic graphs
- proof of idle

disclaimer

I'm OK with proof of work

I get why people don't like it

I'll try to explain other methods in a neutral way

But many have trade-offs & I'm most familiar with PoW

UNL

Ripple / Stellar

Account based

Transactions have sender / receiver

in stellar case, minimum balance

no work, but nodes sign transactions

UNL

to sync, verify signed blocks

but whose signatures?

Assuming majority honest is tricky with sybil attacks

problem akin to CAs

Unique Node List

UNL

wait for majority of nodes in UNL to sign; if they've signed accept

Needs 90% overlap in UNL to prevent divergence (according to Ripple)

Newer work to reduce to 60%

Who provides UNL?

UNL

fast / no work, but known identities

all coins exist at outset & held by ripple or stellar

Proof of Stake

popular alternative to proof of work

instead of proving work, have coin holders sign blocks

given a genesis block with initial distribution, chain choice can be deterministic (most stake)

stake grinding

signer is determined by pubkey nearest prev blockhash

keep signing / changing your block until you're assured multiple block

devolves into proof of work

(NXT rfc6979)

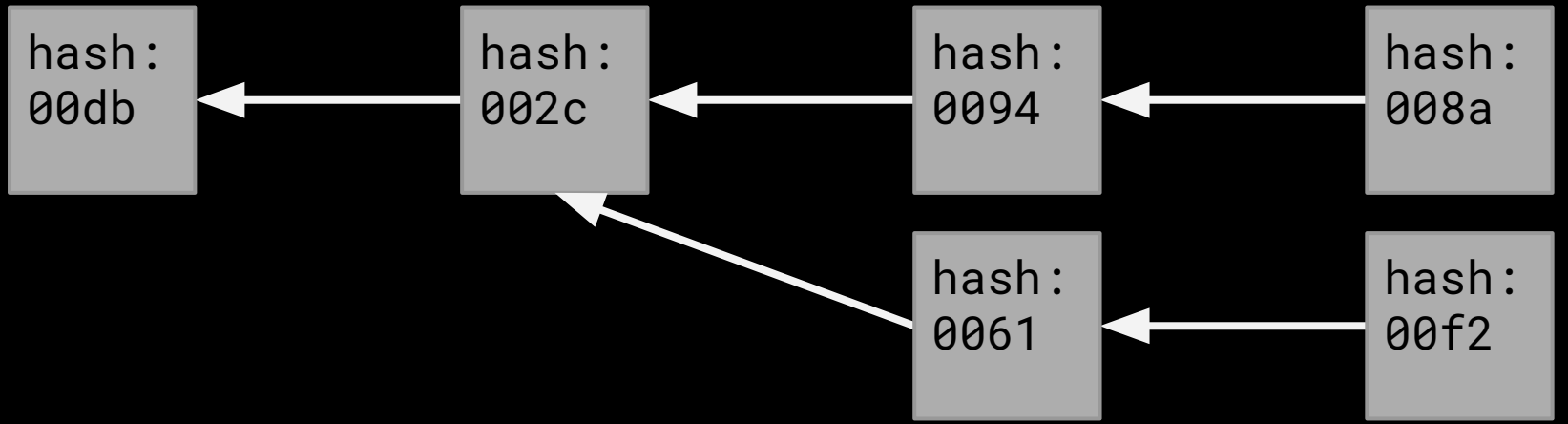
deterministic PoS

If signer influence can be removed, there's another issue

"nothing at stake"

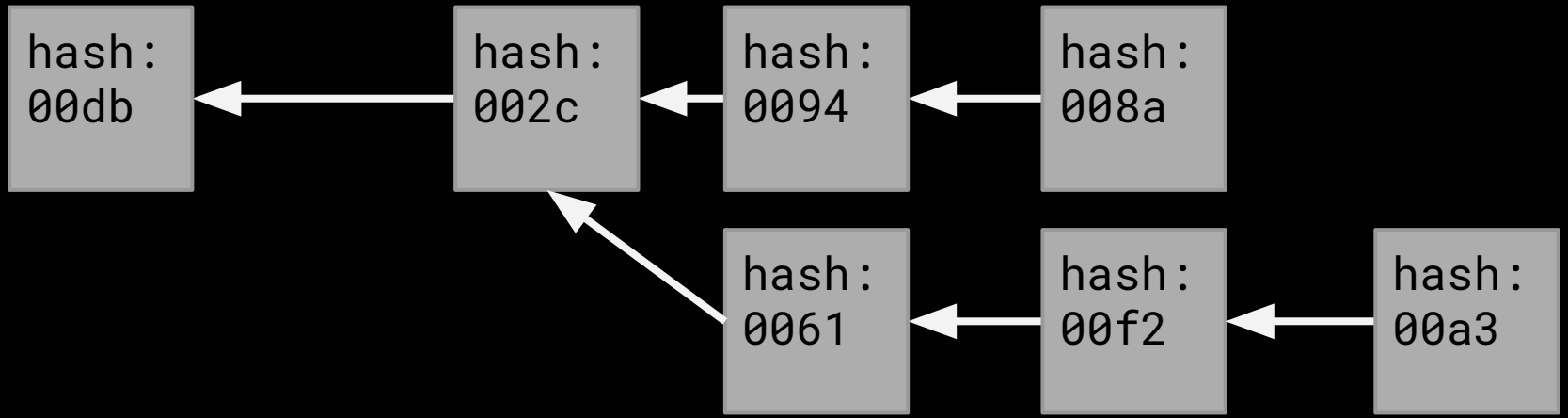
PoW splits

this happens



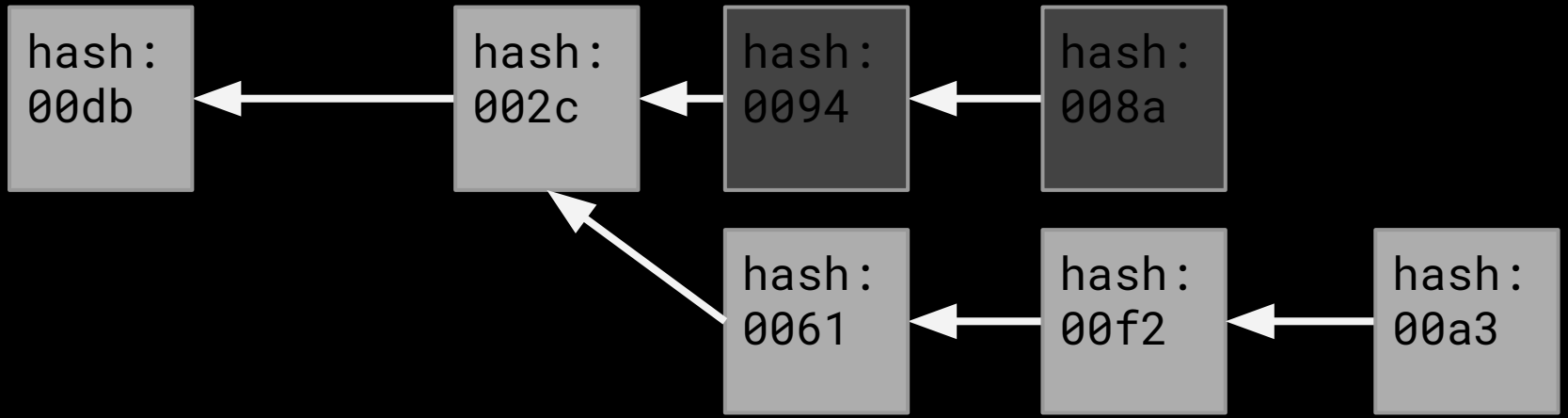
PoW splits

but then this happens



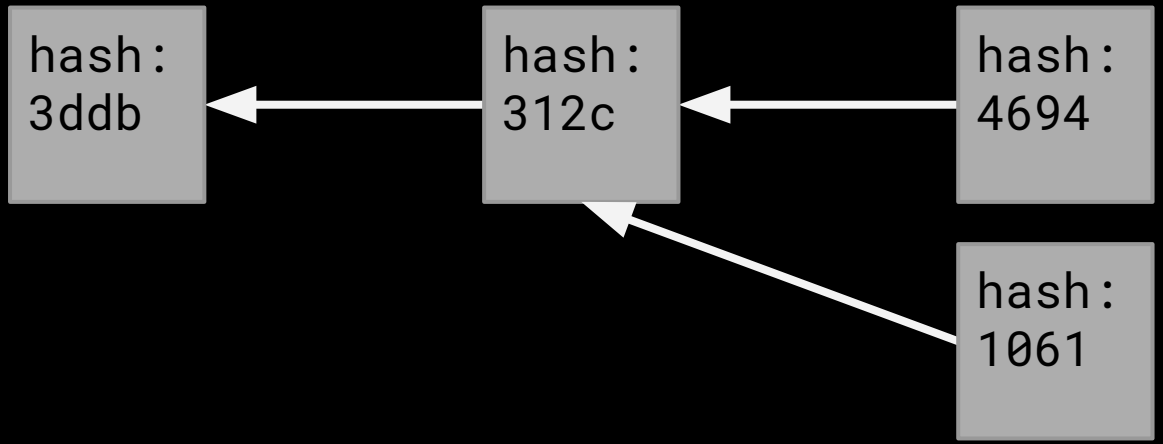
PoW splits

then everyone build off the highest block



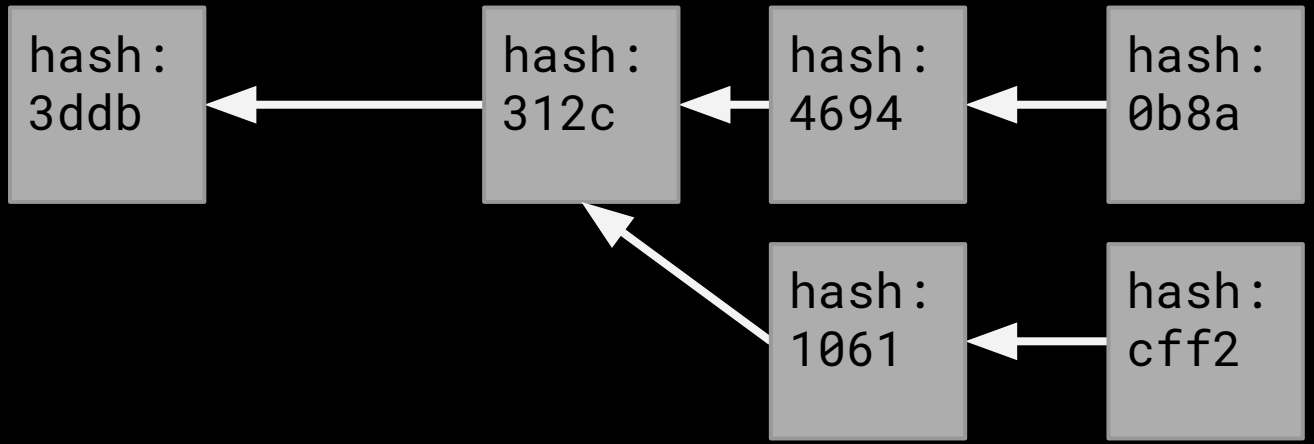
PoS splits

this happens



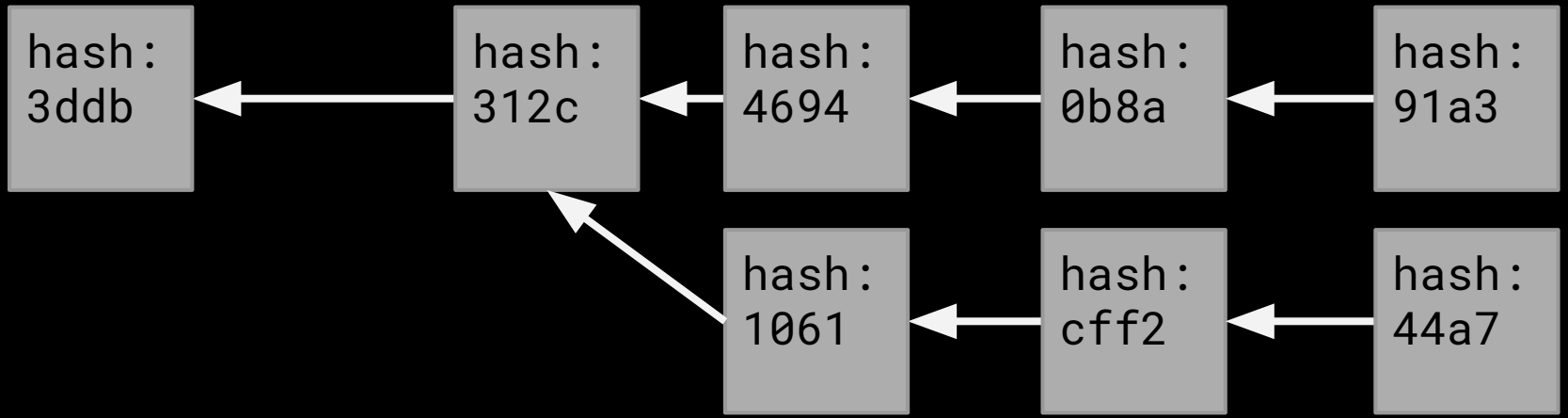
PoS splits

then this happens



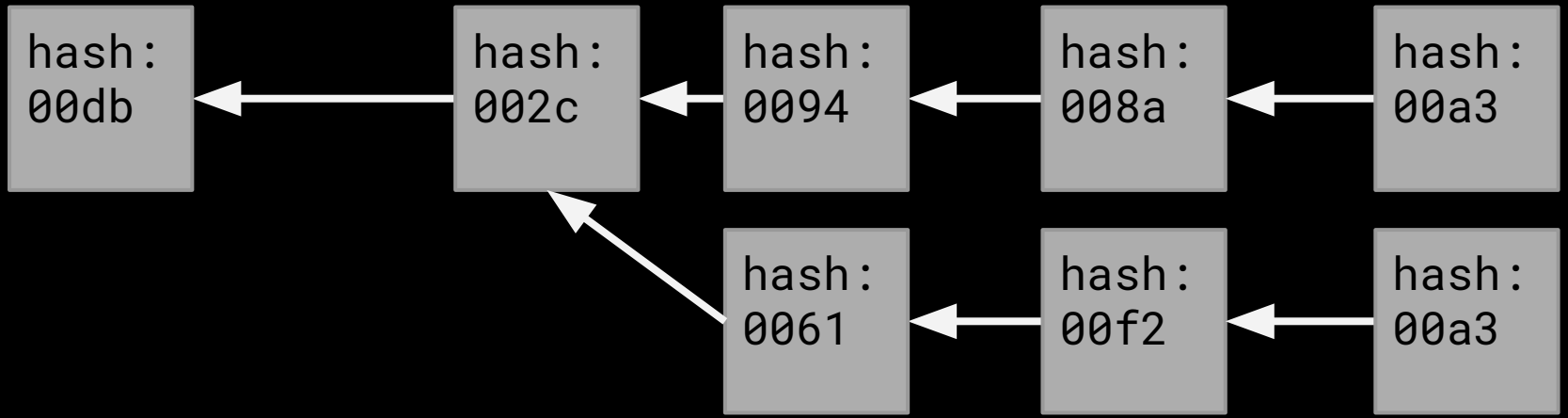
PoS splits

then this happens



PoS splits

then this happens



nothing at stake

faced with two blocks, why not build on both? No cost to sign

mitigations: prove signatures from another chain ("slasher")

Problem with mitigation: maybe block signers ignore your proof

long range attacks

rewrite history from a long time ago

online nodes will reject the reorg

new nodes will see 2 long chains

solution: delete old keys, assume 50% honest. (but old keys can be sold...)

DPoS

signing requires online keys

risky! instead endorse a leader by signing with your coins

supernode / masternode / p2p? or client server?

PoS in general

Hard to resolve conflicts in the system using only the system itself

rich get richer? probably also in PoW

different assumptions:

- honest / rational

proof of space

still proof of work, but memory rather than CPU

several ideas, some complex

one example

proof of space

Buy 10TB drive

Precompute 100G keypairs
Store pub:priv key:value in DB

key closest to current block hash can sign; closer is worth more

work, but amortized

directed acyclic graphs

MIT favorite: iota

blocks can (must) have 2 parents

can potentially reduce latency and orphan based centralization

doesn't help scalability at all

(custom ternary hash functions don't help much either)

proof of idle

old idea (Dryja 2014)
(probably doesn't work that well)
even if it works, just moves costs:
opex -> capex

prove that you're not mining
and get paid

proof of idle

difficulty adjusts so that blocks come out every 10 min

new miners make it harder for existing miners

2X mining leads to 1X coins mined

marginal product of labor = 0

proof of idle

say there are 2 miners, each mining with 2GW

If they both turned down 5%...

proof of idle

cartel forming is hard; lots of profit for defecting

nobody trusts each other

solution: trustless collusion

proof of idle

A pays B not to mine

A posts block header, asks B to mine for 10 sec, respond with work

A creates 2 of 2 multisig tx, sends 1 BTC to the address, builds 2 txs with B

proof of idle

Bounty Tx: Locktime height + 144	
input	output
fund txid Alice's Signature Bob's Signature	Alice 1 coin

proof of idle

Bounty Tx: Locktime time + 24 hours	
input	output
fund txid Alice's Signature Bob's Signature	Bob 1 coin

proof of idle

If blocks come out fast, Alice gets her money back

If blocks come out slow, Bob can get the bounty output

Bob may slow down his mining to get the bounty coins

proof

many new ideas out there

proof of work seems to work, but incompatible with Kurzweil / Roddenberry future

... further research required?
it's happening regardless!

MAS.S62 Cryptocurrency Engineering and Design

Spring 2018