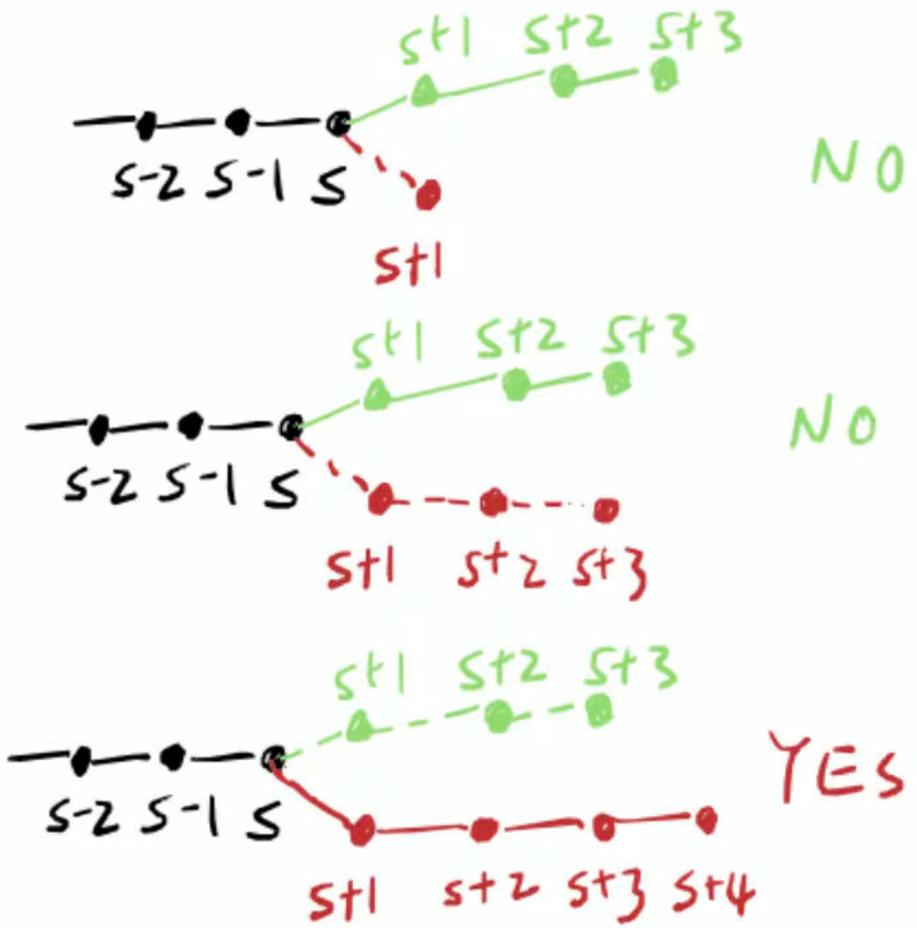
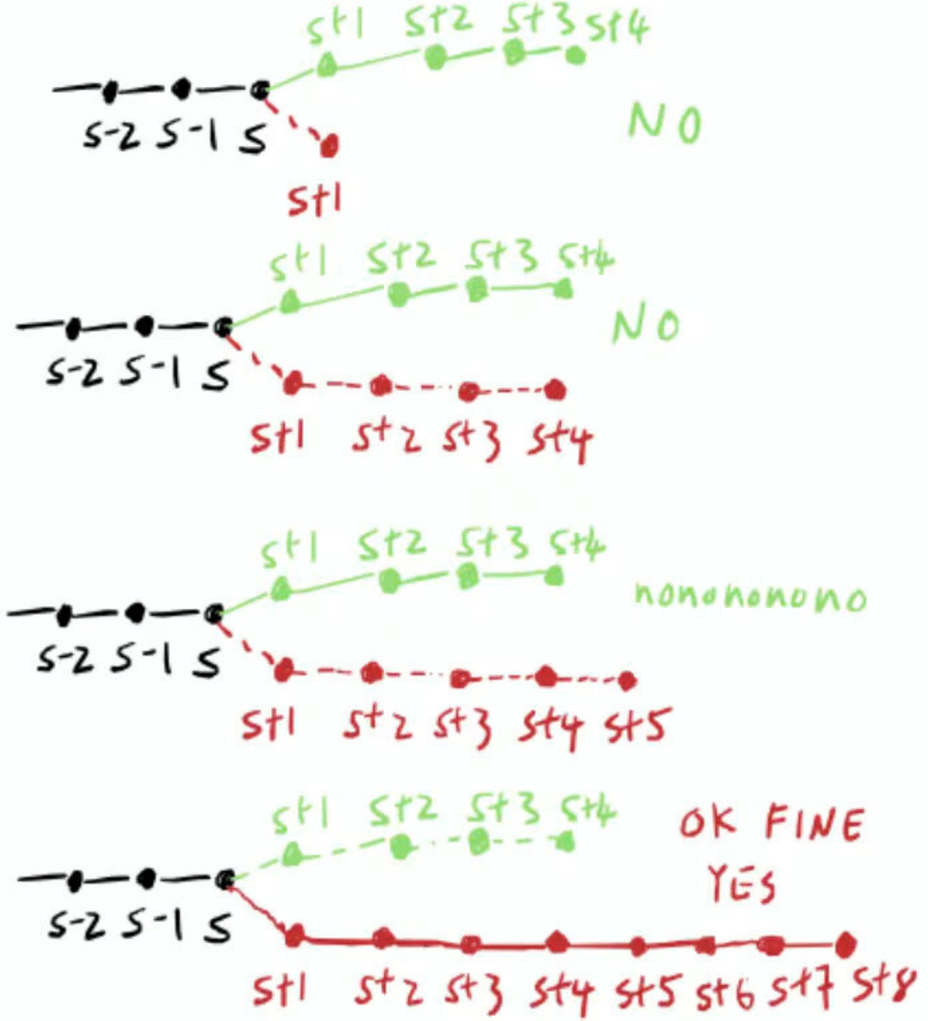
The status quo: Proof of work consensus on Bitcoin circa 2017

- Long chain good! Mine on long chain, only relay long chain
- Switch (“reorg”) anytime a longer chain is seen
- “Catching up” happens abruptly and rapidly
- Don’t tell about a competition happening



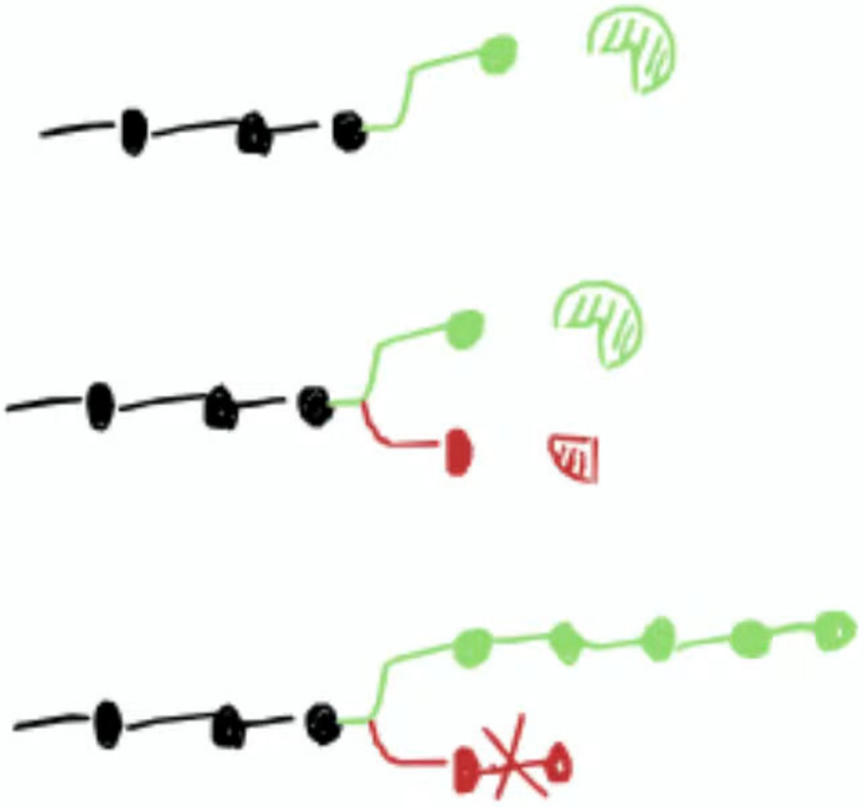
The status quo: Proof of work consensus on BCH (2026)

- Harder to reorg more blocks
- Don’t reorg after 10blocks/2h
- Retains (“parks”) some competition blocks just in case… if you see them
- “Catching up” still happens abruptly and rapidly
- Don’t tell about a competition happening



What does proof of work actually do?

- **Compounds** on **long** things **seen first**
- Expects everyone else to do it, so if I don’t do it I lose money
- Can’t know who hides what, only act on what’s in public
- Hybrid objective/subjective system
- Vs PoS: Explicit members having explicit votes
- Purely subjective



Let’s get the blasphemous stuff out first

Problem 1: Satoshi did the bare minimum (at securing blocks)

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Solving for P less than 0.1%...

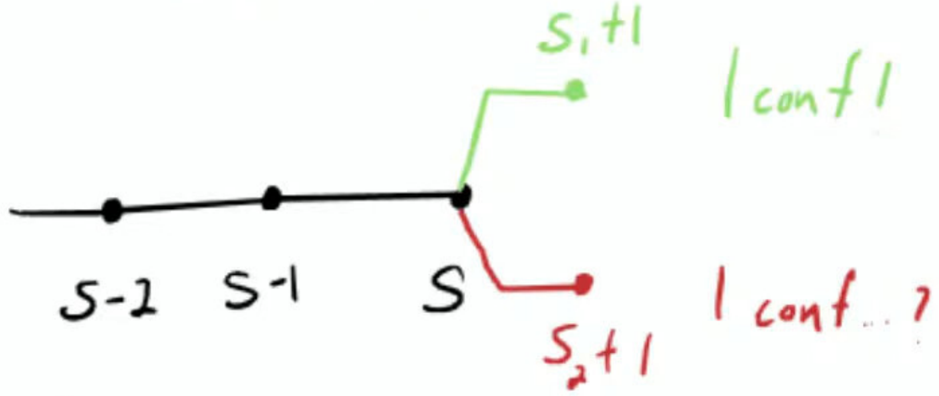
```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

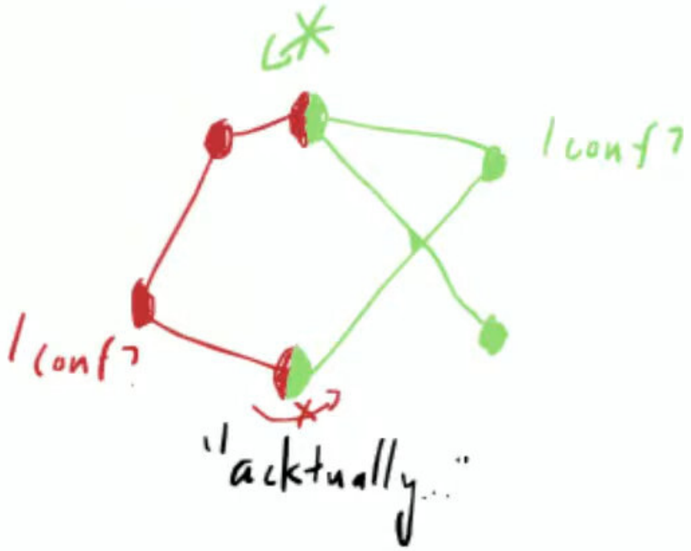
- Catching up takes exactly same amount of money as securing, no matter from how far
- We CAN tell who's public and who's attack, but choose to prepare for nuclear apocalypse instead
- What are those checkpoints for then?
- Wait 6 confs for medium sized amounts? In this economy?

It gets worse:
We don't even have enough information about what's going on (by design)

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$



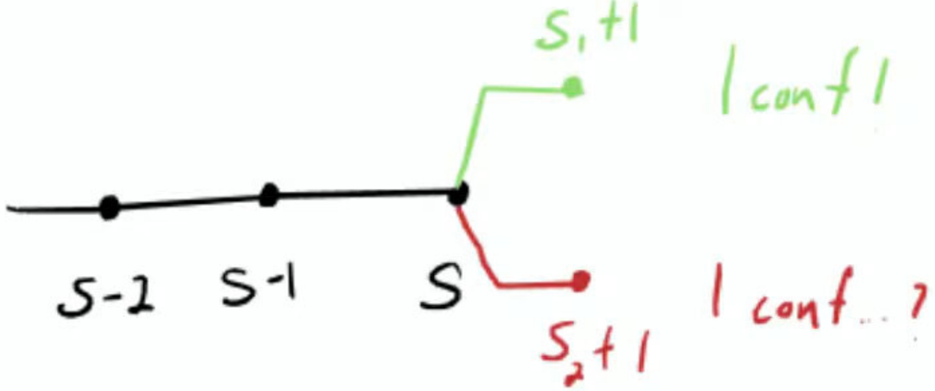


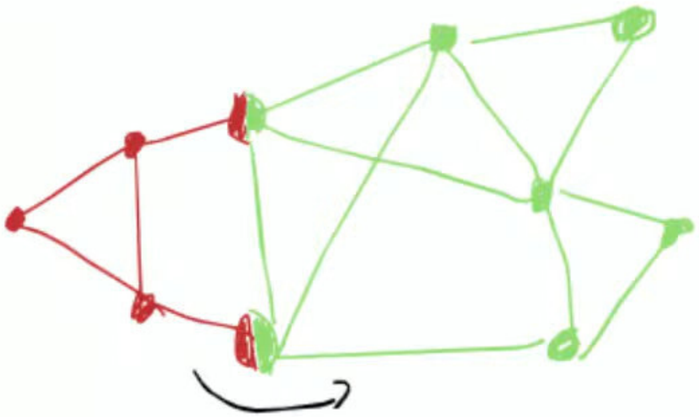
- First seen advantage is fine, but we don't know q because we blind ourselves with first seen *relay*
- So we don't actually know how far we're ahead, only we're *probably* not behind
- It's a miracle we actually can tell people about 1 confirmation
- It happens more often with shorter blocktime, so… just longer blocktime to avoid the problem?

Problem 2: Blockchain is too slow (at letting us know what's going on)

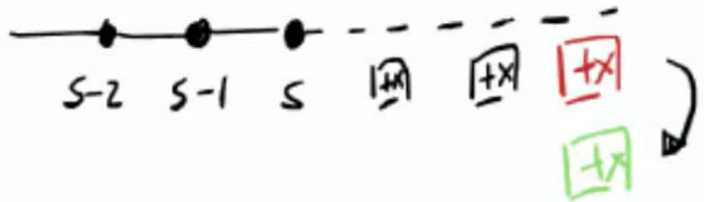
- Which tip is winning?
- Do I have a doublespend? (see also: dsproof)
- Is someone trying to reorg?
- How much hashrate do they have?
- *Are we the baddies?* Can I stop being one?

Problem 2: Blockchain is too slow (at letting us know what's going on)





Can I join the majority early? Would you tell me?

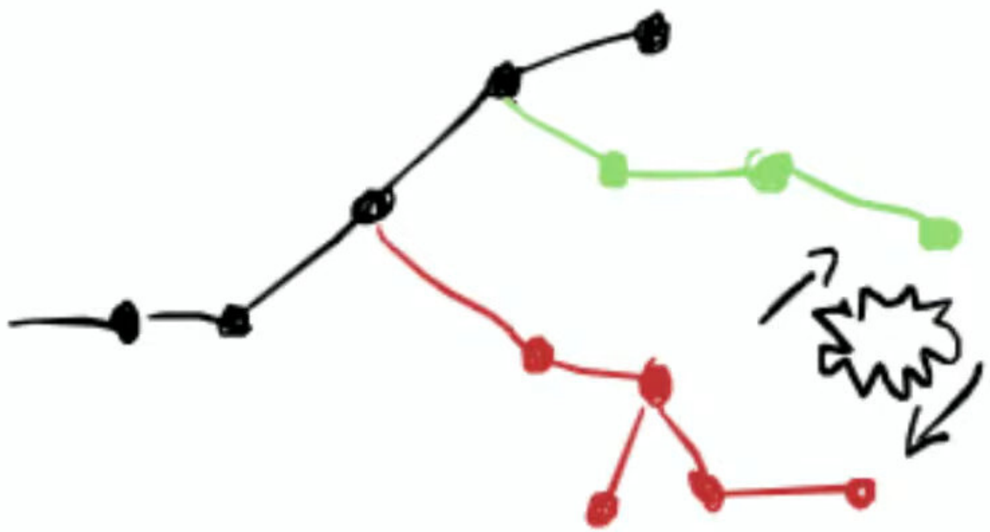


Can I join the majority's *mempool* early? Would you tell me?

Sunlight is subjective and that's okay

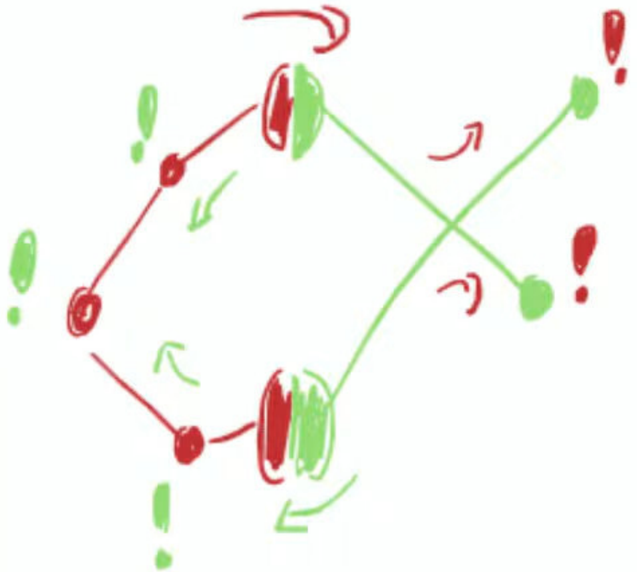
- We already favor doing things in public: Reorg protection, repo checkpoints, and most importantly…
- First seen rule (awkwardly) favors publishing early

Why not just super fast blocks?



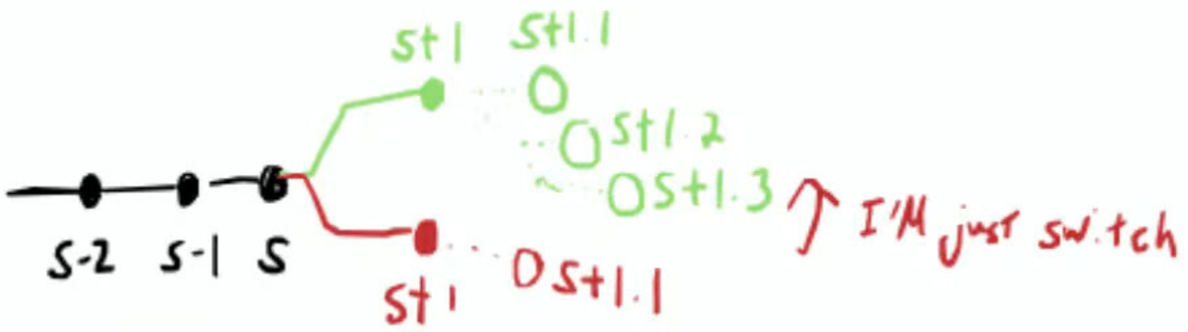
- Latency
- Fracture
- Orphans
- Difficult to secure against many competition

Relay everything (that we block out of paranoia)



- Now that we actually know what's going on and who's the competition...

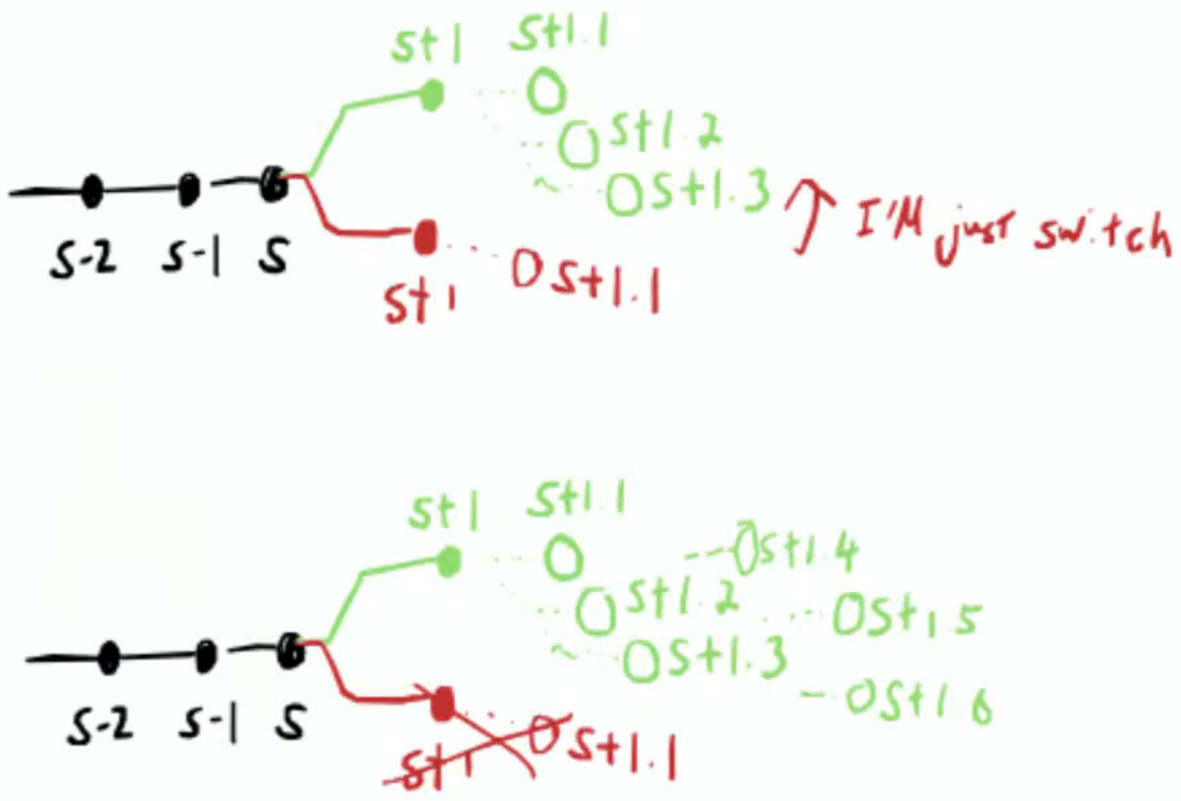
Relay the weaker blocks (don’t bother to order them)



Maybe I should switch to the other guys?

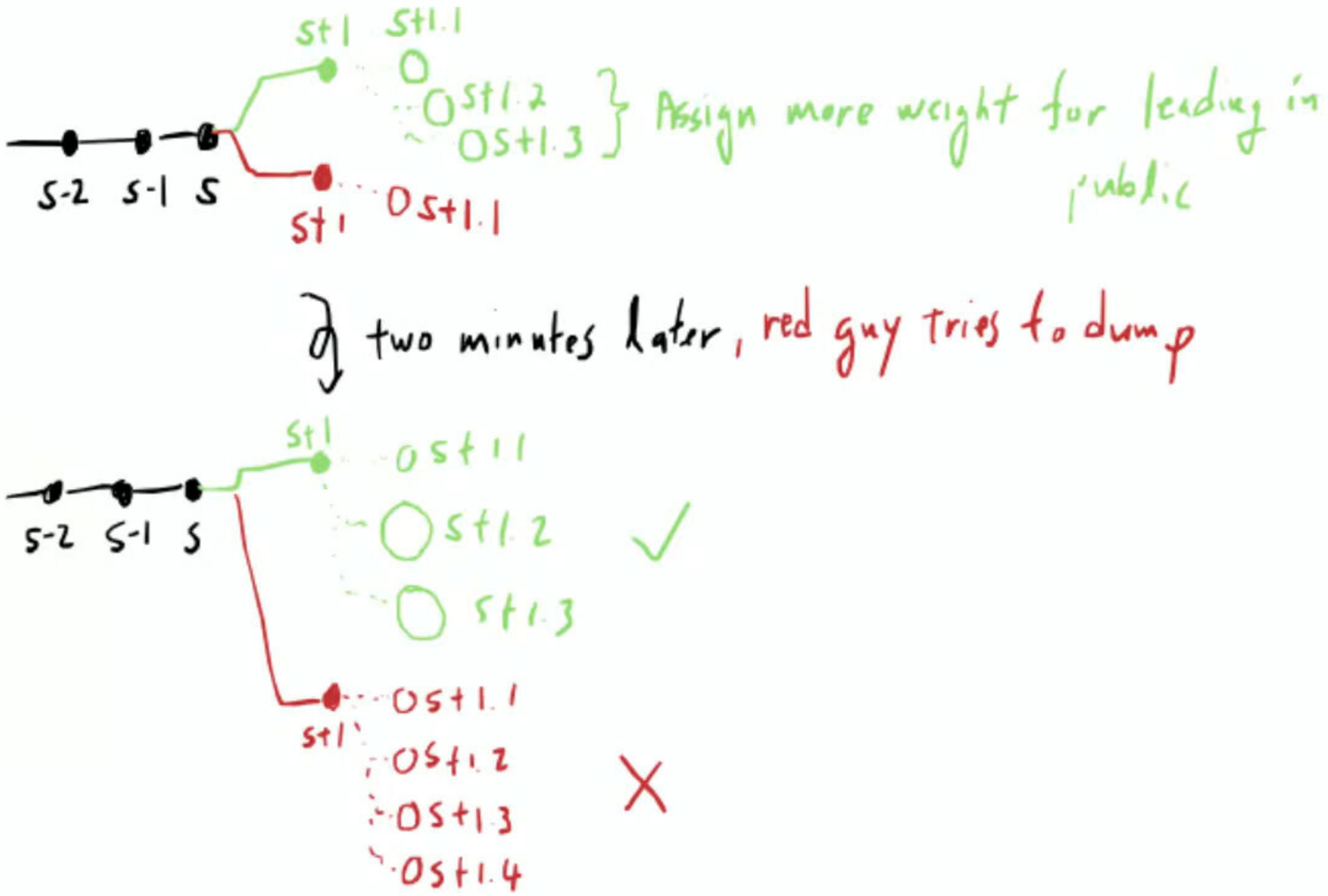
- Stack signals, stack confidence to competing tips
- No additional branching, no additional headaches
- Reuse PoW, no spam no sybil

Relay the weaker blocks (compound and enforce)



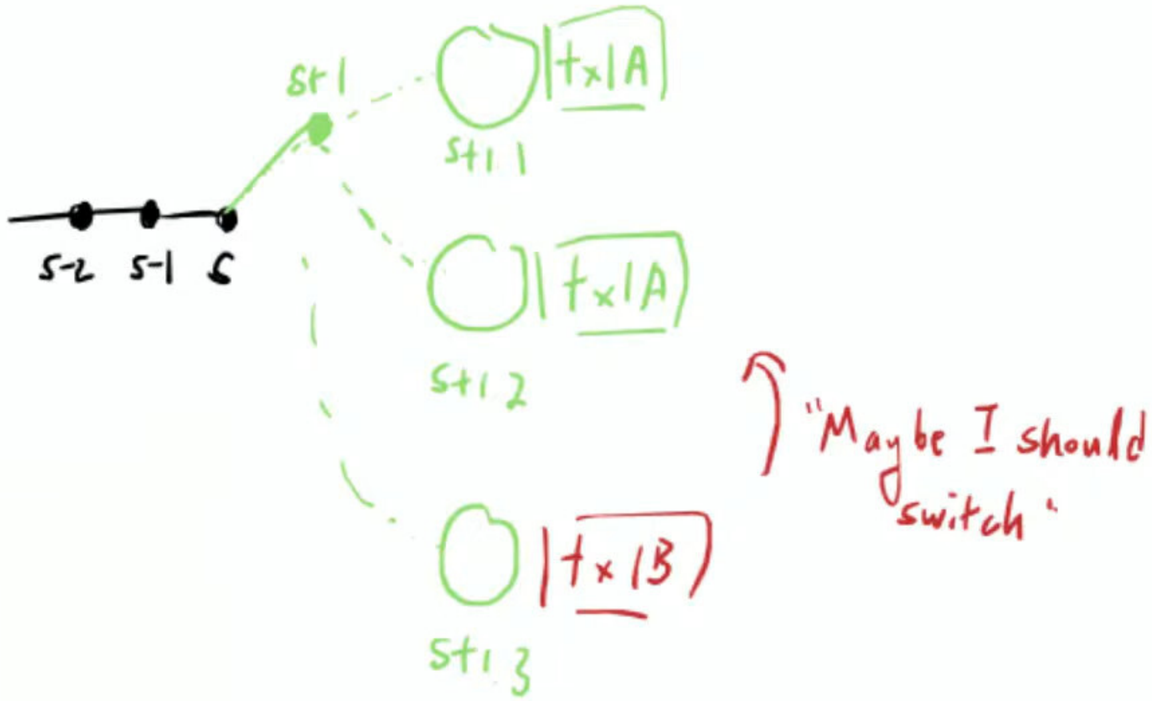
- Stack signals, stack confidence to competing tips
- No additional branching, no additional headaches
- Reuse PoW, no spam no sybil

Dumping and rate limiting



- Magnify lead for tip leading **in public**
- Punish catching up from obscurity

Relay everything (conveniently, also your current mempool)



- After a while this can be enforced for the next block, no ~~tx1B~~ allowed for that same UTXO
- “Faster confirmation”

Security in seconds

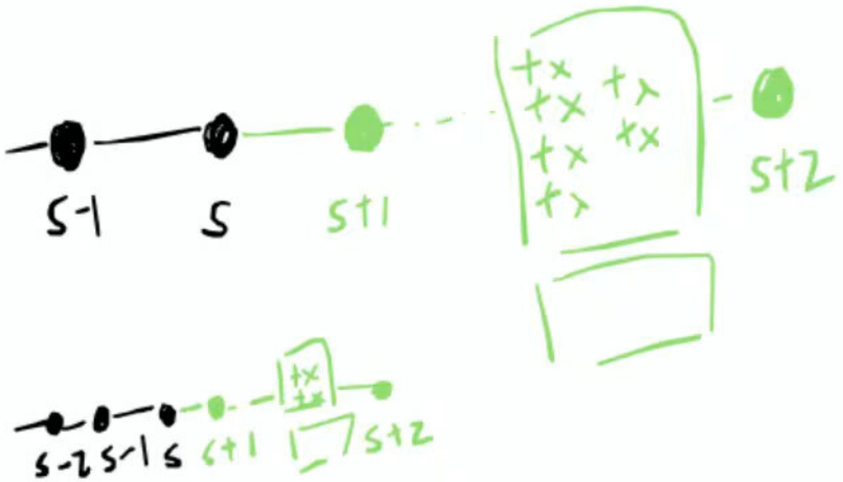
- With good compression, each signal can be as small as a header plus transaction you should’ve already seen
- Start increasing leading weight after assumption of >99% reach
- ~2.5s in 2018?
- To be measured again 2026

Key insights

- **Unordered** piles has no risk of fracture, can go way faster than ordered chains
- **More information good,** even about competition
- **Reward public**, punish hiding (as latency allows)
- …as long as you know what the public is doing!
- It’s what pools already do when given more information (spying on other pools)
- More research…

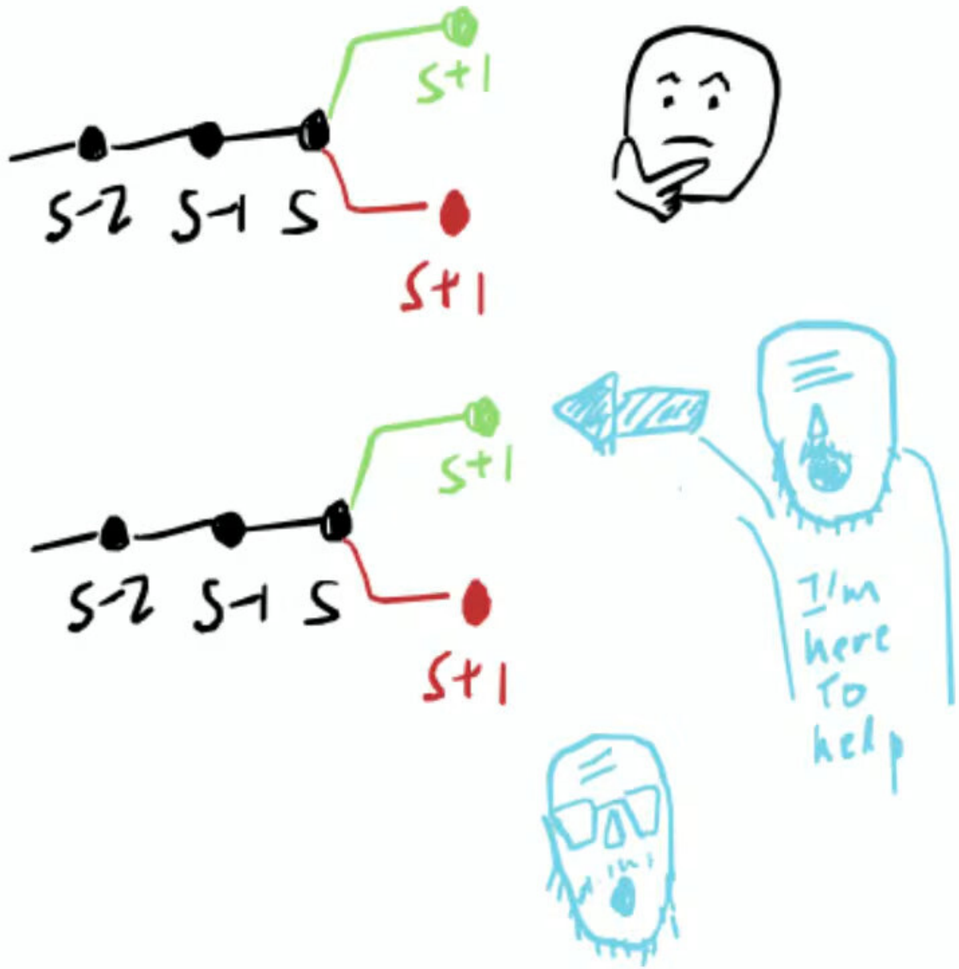
Faster blocks?

- Faster blocks are likely to be *beneficial* for this scheme
- Reduce worst case load and latency of signals
- Faster blocks are still *ordered*, fracture and orphan still apply
- Ordered chain can’t go too fast, unordered piles can’t have incentives, each has their place



The alternatives

- The old Satoshi consensus just hides information between 10 minutes
- BCH Consensus has many elements, but does so awkwardly
- DSProof removes the information blockage, but only for individual transactions and awkwardly
- **Avalanche** introduces **arbitrary new incentive** to do the same thing
- Pure PoS never recovers to objectivity



Good enough?

- We've been talking "0 conf is good enough" since Satoshi was still around
- It is! *for some usecases*.
- We can do better
- We can even do better **using what we already have**, no weird new incentives
- Thank you