bitcoin

CS1699: Blockchain Technology and Cryptocurrency

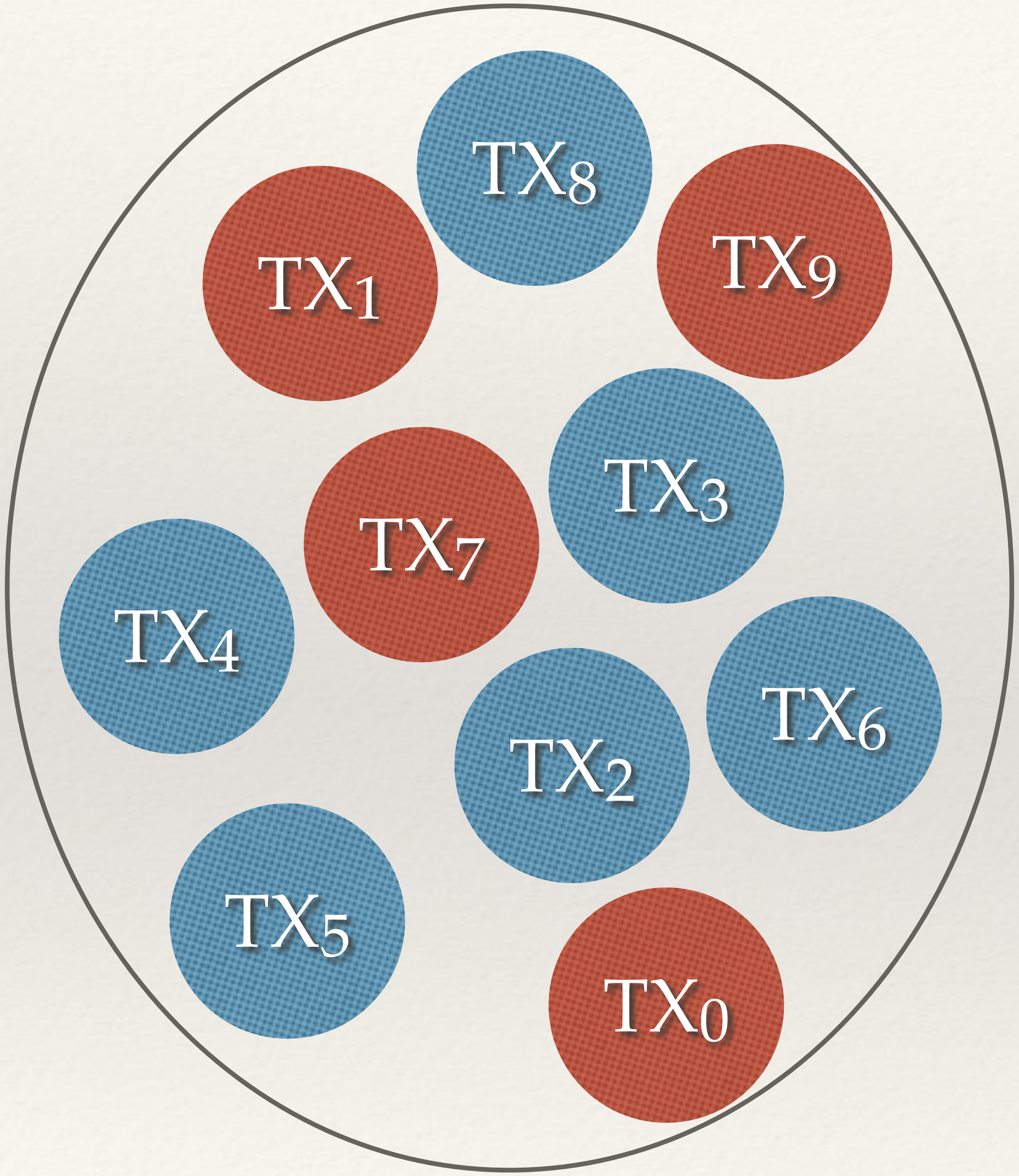
11. Mining In-Depth

Bill Laboon

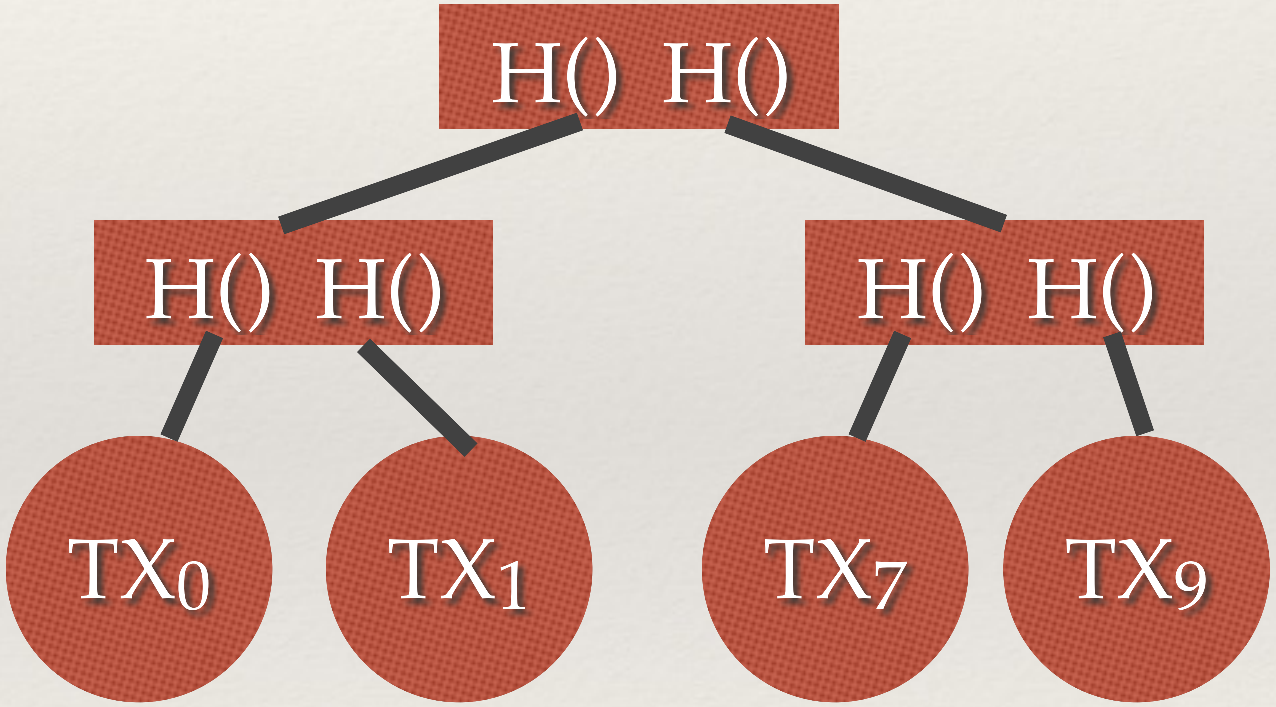
Being A Miner

1. Listen for transactions (maintain tx pool)
2. Maintain and update block chain (listen for new blocks)
3. Assemble a *candidate block*
4. Find a nonce that fits the candidate block where *H(block)* < *target*, or generate a different candidate block
5. If found, broadcast your block (and hope others accept it)
6. Coinbase gets sent to address you control (with locktime)

Finding a Valid Block



Optimize for highest transaction fees -
more transactions, highest fees per transaction



Generate Block Using Merkle Root of Tx Tree

```
{
     "ver":536870912,

"prev_block":"000000000000000000001d1d0669b04466c9636b879fe538e606f56f6
1e04560b",
    "mrkl_root":
"a93c7a87b6e23c3c49348672b8df462107fc84626f5294854c27910d0740affa",
    "time":1538407084,
    "bits":388454943,
    "fee":14746468,
   …
    "tx":[
```

Try Nonces, 0 through 2^{32} - 1

```
{
    "ver":536870912,

"prev_block":"0000000000000000001d1d0669b04466c9636b879fe538e606f56f6
51e04560b",

"mrkl_root":"a93c7a87b6e23c3c49348672b8df462107fc84626f5294854c27910d
0740affa",
    "time":1538407084,
    "bits":388454943,
    "fee":14746468,
    “nonce”:{0,1,2,3… (2^32 - 1)},
 …
   "tx":[
```

Only 2^{32} nonces?

- Yes, BUT, we can always modify the candidate block in other ways!
  - Use a different subset of transactions
  - Modify the coinbase (unused scriptSig) attribute
  - Send coinbase to a different address
  - Anything that modifies a transaction will also modify the Merkle root

Keep Modifying Candidate Block Until $H(block) < target$

Once it does, broadcast it ASAP to the network!

How Do I Know the Target?

- Calculated from the mining difficulty, which changes every 2016 blocks:

$$next\_difficulty = \frac{\text{(prev\_difficulty * 2016 * 10 minutes)}}{\text{time\_to\_mine\_last\_2016\_blocks}}$$

$$difficulty = \frac{\text{maximum\_possible\_target}}{\text{current\_target}}$$

$$target = \frac{\text{maximum\_possible\_target}}{\text{difficulty}}$$

SHA-256 and Double-SHA-256

- SHA-256: Secure Hashing Algorithm, part of NSA's SHA-2 series of cryptographic hashes
- Some conspiracy theories!
- H(block) = SHA-256 hash of the SHA-256 hash of the block (double-SHA-256 hash)

How Does SHA-256 work?

- Standard Merkle–Damgård construction (with a few twists)
- Output: 256 bits, Block size: 512 bits
- Initialization vector (by necessity also 256 bits) = fractional parts of the cube roots of the first 64 primes (to avoid accusations of backdoor values)
- Strengthening (padding): a 1 and then as many 0s to get up to 448 bits, followed by a 64-bit length of string
- Walkthrough: http://www.righto.com/2014/09/mining-bitcoin-with-pencil-and-paper.html

SHA-256

- Goal is for miners to compute as many SHA-256 hashes as possible in a short a time as possible to maximize block production
- By-hand rate, 0.67 hashes/day (i.e. about a day and a half of work to calculate a hash by hand)

CPU Mining

- In the original Bitcoin paper, Satoshi Nakamoto seemed to imply that most/many nodes would also mine
- “One CPU, one vote”
- With well-optimized software, on a regular desktop or laptop, you can get several tens of millions of hashes per second

GPU Mining

- Soon after Bitcoin’s release (~2010), GPU programming became popular
- GPUs allow you to massively parallelize relatively simple operations (such as the ones necessary for SHA-256 calculations)
- Took Satoshi by surprise! https://bitcointalk.org/index.php?topic=1327.msg15112#msg15112

GPU Mining

- GPUs increased hashpower by approximately an order of magnitude over a CPU
- AND you could run multiple GPUs off a single computer!
- The era of *mining rigs*

The Brief Reign of FPGAs

- GPUs are better for mining than CPUs, but still not optimized - lots of superfluous hardware, e.g. for floating-point arithmetic
- Around 2011, people moved to field-programmable gate arrays - basically "programmable integrated circuits"
- Performance of FPGAs about an order of magnitude better than GPUs, but prone to failure and costly

ASICs: From 2012 to Now

- Application-Specific Integrated Circuits - specialized computers that can do nothing BUT mine Bitcoin
- Although not as fast as in the years of 2012-2014, improvements still come quickly
- Once newer generation mining hardware is out there, older hardware rapidly becomes a very expensive electric heater

Energy Consumption

- Recall that we need proof-of-work to allow for decentralized generation of valid blocks (need to have "skin in the game" to avoid spamming network with invalid blocks/building off other chains/etc.)
- But this comes at a cost - currently estimated at ~73 TWh/year (0.33% of worldwide electricity usage, approximately equivalent to Austria)
- https://digiconomist.net/bitcoin-energy-consumption

Efficiency

- Definitely! As we have already seen!
    - …but Bitcoin mining is a Red Queen's Race (have to go faster just to stay still) - as long as it is profitable to mine, people will do so, and mining is a zero-sum game
- Plus, limits on efficiency - *Landauer's Principle*
- Could we eliminate mining entirely? Hmmm… we'll come back to this later on in the term!

Is Bitcoin Mining Wasteful?

- Any payment system requires energy (digging gold out of the ground, printing dollar bills, running a bank, etc.)
- Mining = *securing the network;* under Bitcoin's rules, the security of a network comes from the vast amount of hashing that is being done
- Mining rewards can be thought of as "stored electricity"

Can we make it less wasteful?

- Renewable energy
- Use otherwise-wasted electricity
- Bitcoin miners are essentially space heaters - can we utilize the generated heat instead of venting it?

You STILL want to mine Bitcoin?

- OK, you go out and spend $10,000 on ASICs from Bitmain - https://shop.bitmain.com/?lang=en
- You start paying an extra $500/month in
- But your income is sporadic - an entire year can easily go by without you finding a block (so you just spent $500 * 12 + $10,000 = $16,000 with no return)
- Or you could find two blocks in a row the day after you set up your rig, giving you ~ $170,000 in block rewards

Mining Pools

- What if you could work with others to make a "collective" where you all pitched in to work and smoothed your earnings (reduce variance)?
- A *mining pool* is a collective of miners generally run by a *pool manager* (who takes a small cut).

Mining Shares

- How do you prove that you're contributing to the pool?
- Turn in near misses AND hits (where H(block) < (target + value))
- Only way to generate misses is using your hashpower!
- Each entry is a "share" in the next block reward

Mining Payout

- Pay-per-share: every share you submit to the pool entitles you to a flat amount of bitcoin
- Proportional: every share you submit gives you a higher proportion of bitcoin found in the next block - if no block is ever found, no reward for you!
  - Note: most proportional mining pools actually use PPLNS (Pay-Per-Last-N-Shares) or Score algorithm (proportional weighted by time submitted) due to *pool hopping* and other game theory

Can Pools Be Too Powerful?

- Recall that a pool acts under the supervision of a pool manager but otherwise act as one “giant miner”
- GHash.IO briefly had > 50% of hashpower in 2014
  - Intentionally reduced it themselves to avoid potential loss in trust to the Bitcoin network
- Could super-powerful miners be hiding their actual hashpower by joining multiple pools?
  - This is called *hash laundering*

Mining Pools: Good or Bad?

- Pros: reduce variance for smaller miners, make it easier for miners to get involved, easy way to upgrade network (can't join pool unless you have upgraded to latest version of Bitcoin software)
- Cons: One form centralization, reduce the number of fully validating Bitcoin nodes (only one necessary per pool)

Mining Decisions

- You have access to hardware, cheap electricity, and an Internet connection. You can mine - either on a pool or on your own. Now you (or your mining software) needs to decide:
  - Which transactions should I include in the next block?
  - Which block should I mine on (deal with *chainsplits*)?
  - What do I do if there are two blocks at the same height?
  - If I find a block, should I announce it immediately?

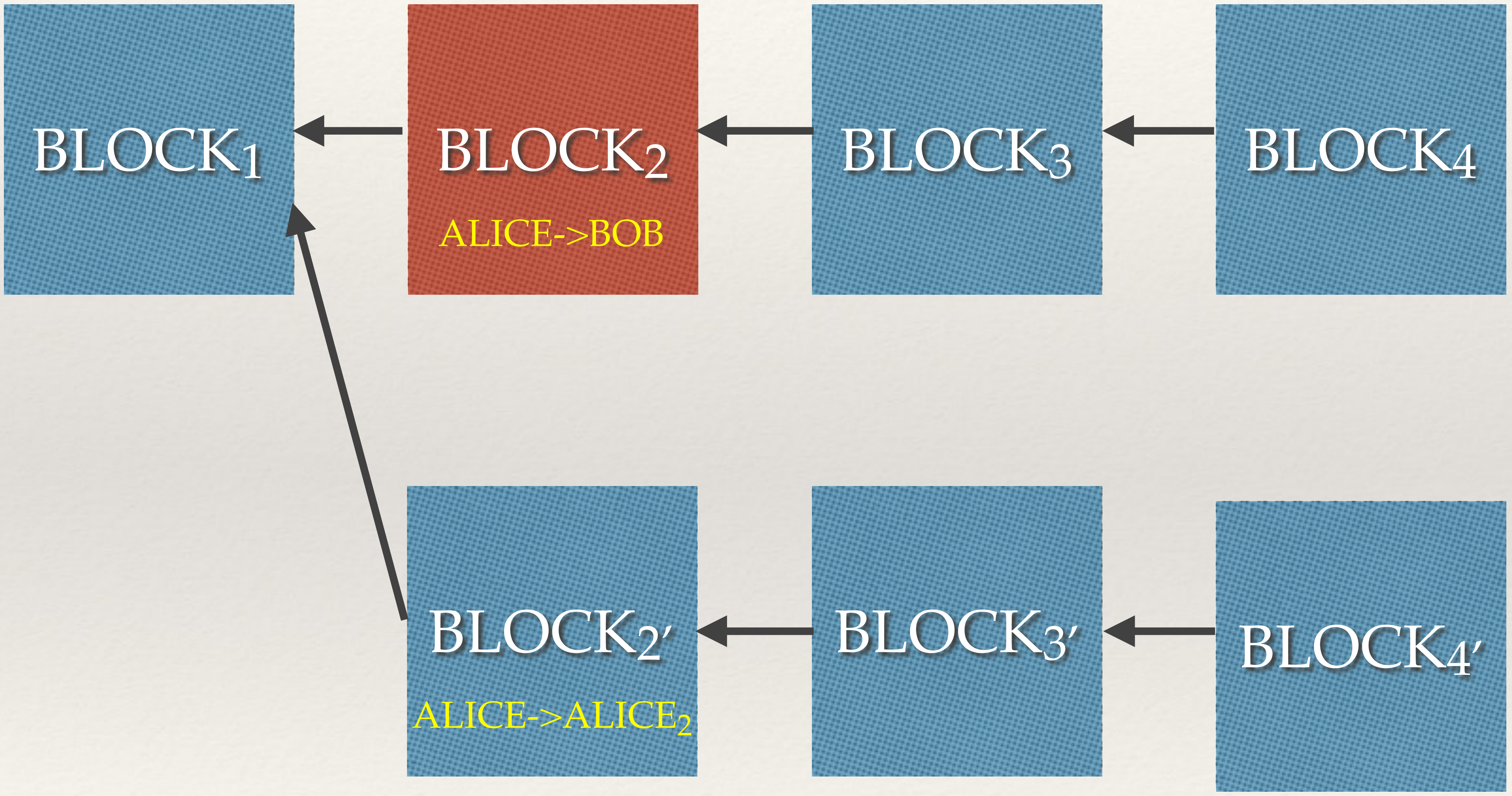
Attacks By Miners

- Seems like there are some good default answers built-in to the software
- But could we maximize our payout by modifying these algorithms?
- This will most likely have a negative impact on other users which is why they are often called *attacks*.

Forking Attack

- Just like a basic double-spend, but can go back multiple blocks in the blockchain
- Miner builds upon previous block in the blockchain to create an alternative chain
- Very detectable and would require a large amount of hashpower

Forking Attack



BLOCK$_1$

BLOCK$_2$

ALICE->BOB

BLOCK$_3$

BLOCK$_4$

BLOCK$_{2'}$

ALICE->ALICE$_2$

BLOCK$_{3'}$

BLOCK$_{4'}$

Forking Attack via Bribery

- Out-of-band: Go to biggest pool managers with a bag of cash with a giant dollar bill painted on the side
- Run a pool at a loss (i.e. pay more for shares than they're worth) - attract hashpower
- Leave big "tips" (i.e. transactions) in transactions only valid on the forked chain to entice others to build on it
- Note: something similar appears to have happened recently on EOS, an altcoin blockchain - https://twitter.com/mapleleafcap/status/1044958643731533825?s=21

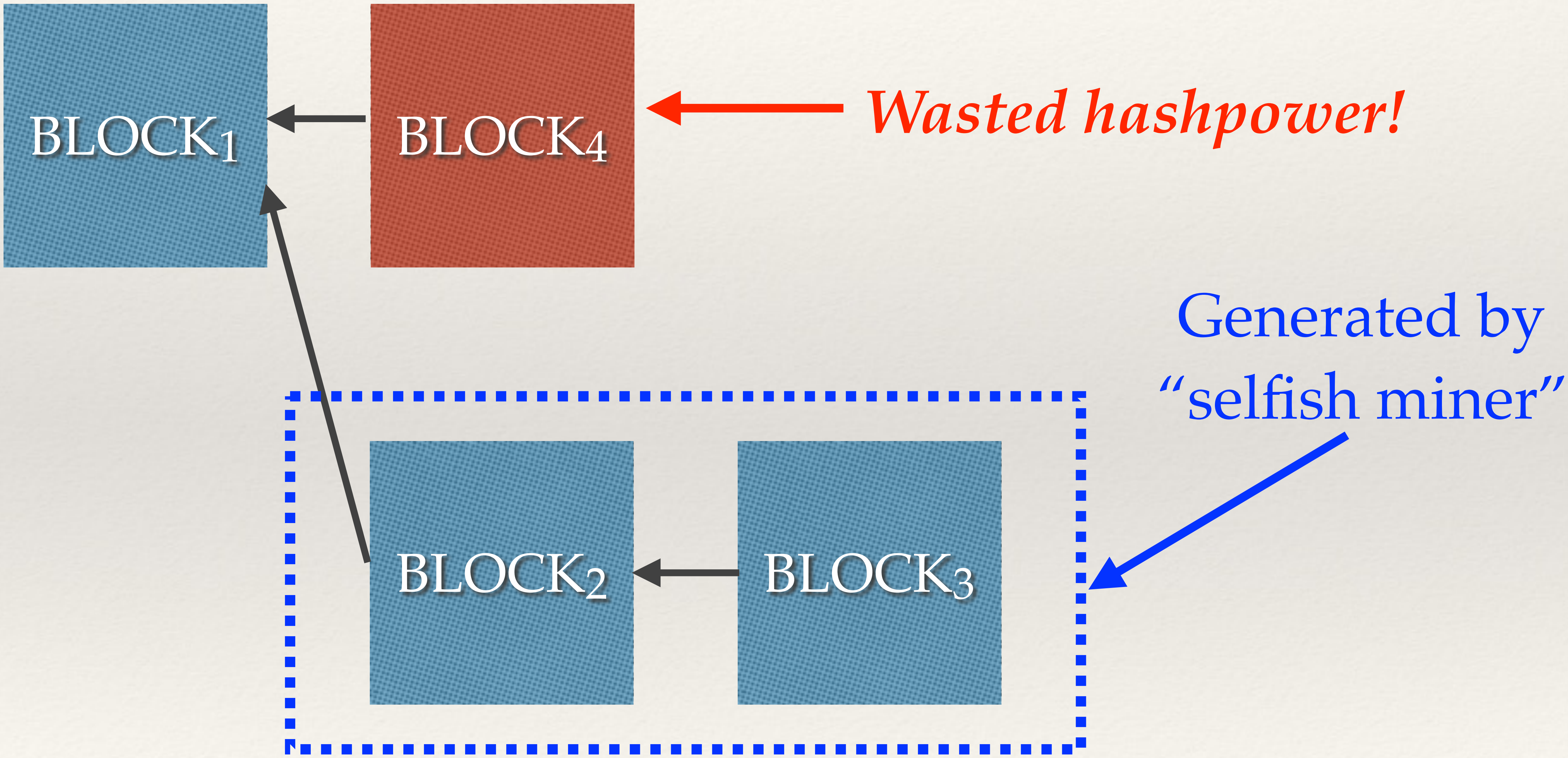
Block-Withholding

- Generally, you want to announce immediately to the world that you found a block - at any moment someone else could find one, and general algorithm is to build on the block you found first
- But what if you hold on to your block, then try to build a second block on top of that one before you broadcast it?

Block-Withholding

- If you are now two blocks ahead of the network, all of the hashpower they've been using has been wasted
- *Selfish mining* - all other blocks produced are immediately orphaned, and you have a head start on reating the third block
- Can be an improvement over default strategy if your hashpower is over 1/4 of the network! Kind of a back-door 51% attack

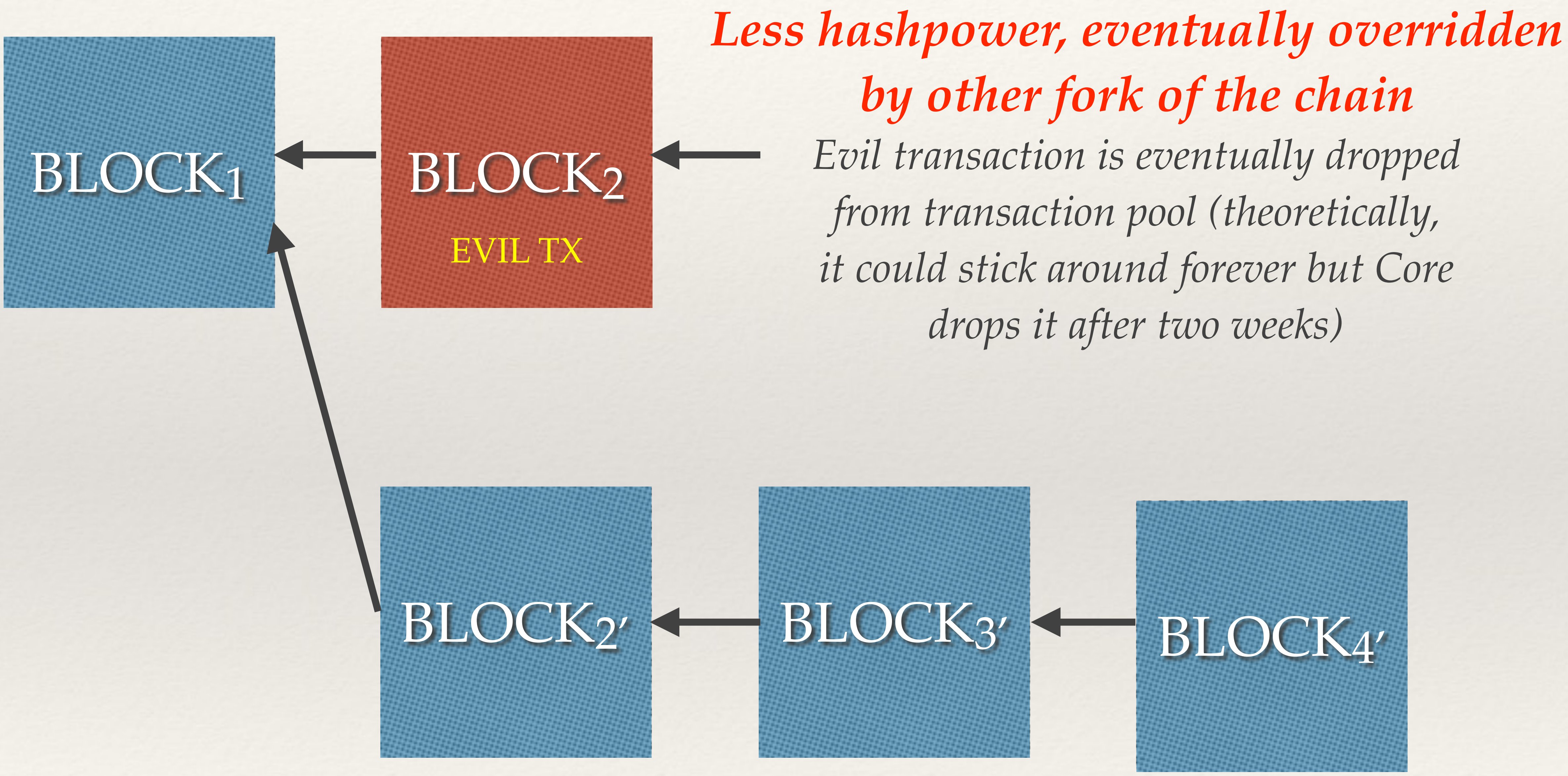
Block-Withholding



Blacklisting / Punitive Forking

- We have already discussed blacklisting particular UTXOs/addresses
- However, in the absence of a centralized controller, others could always include transactions in a block, it just might take longer
- But if we have sufficient mining power, we can take this to the next level with *punitive forking*
  - Not only will I not include those transactions, I won't mine on any chain that includes those transactions

Punitive Forking



Less hashpower, eventually overridden by other fork of the chain

Evil transaction is eventually dropped from transaction pool (theoretically, it could stick around forever but Core drops it after two weeks)

Feather Forking

- Punitive forking is really only an issue if you have a majority of hashpower (variation of 51% attack), otherwise a big waste of time (you waste your hashpower on a chain nobody else is following, blacklisted transaction goes through anyways on main chain)
- *Feather forking* - You'll attempt to fork, but eventually give up if you can't do it. Probability of success is α^2 (where α = your percentage of hashpower of entire network)
- Why α^2 and not α? You need to get at least one block ahead of everybody else (i.e. generate two blocks before someone else generates one).

So what?

- Assume you have 15% of hashpower (note that many pools have had this or more - I chose this number because it is current approximate hashpower of both the btc.com and AntPool pools)
  - Source: https://www.blockchain.com/en/pools
- Probability of a successful feather fork = $(0.15)^2 = 0.0225$ = 2.25%
- But - if you are another miner, and you don't care about the transaction one way or the other, will you take that risk?