bitcoin

CS1699: Blockchain Technology and Cryptocurrency

14. Consensus

Bill Laboon

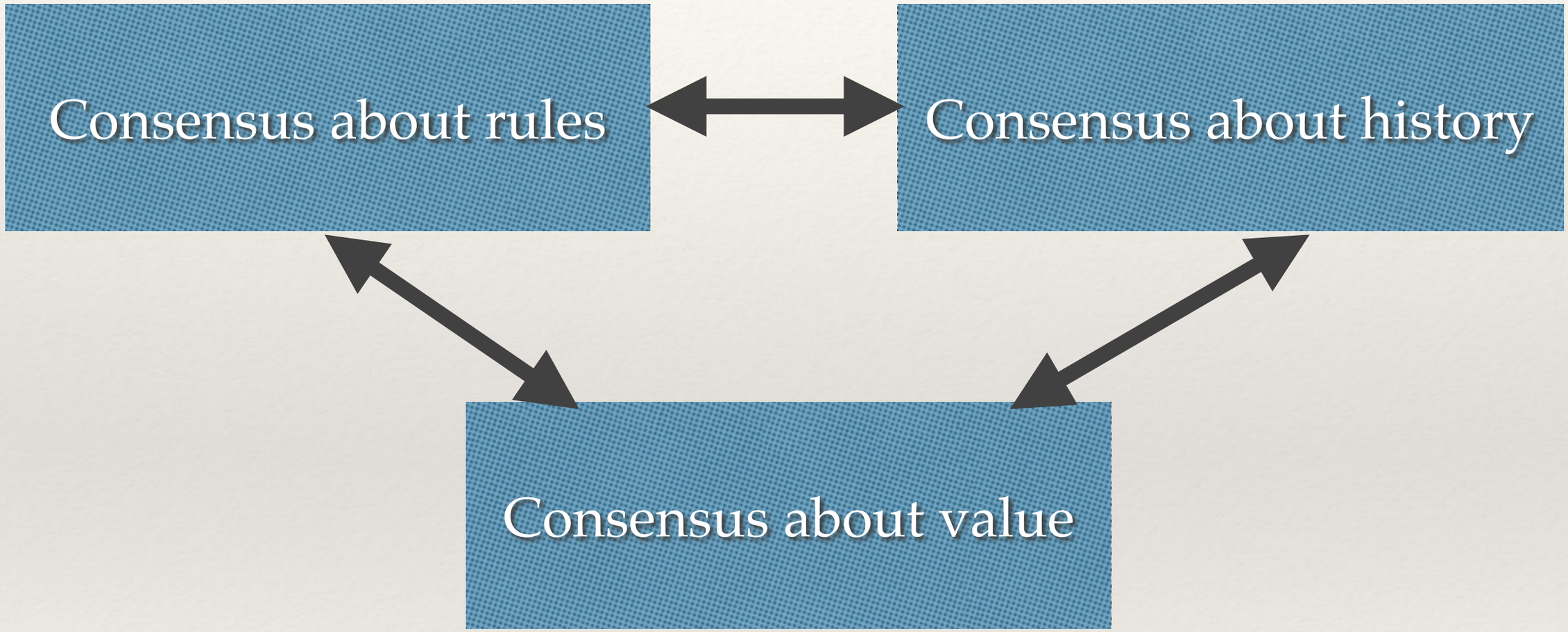
Bitcoin Consensus

1. **Consensus about *rules*** - *How do nodes communicate? What kinds of data is sent over the network? What makes a transaction valid?*

2. **Consensus about *history*** - *What is the correct blockchain?*

3. **Consensus about *value*** - *What is the value of any amount of bitcoin that I use? Is there a value attached to the "token" that I send?*

Consensus Relationships



Consensus in Fiat

- If I were to give you $10 for some goods or services, why do you accept it?
- Why would you accept Bitcoin instead?

Bitcoin Core

- General consensus is that Bitcoin Core is the “model implementation” (although there are others, they tend to defer to Core)
- Uses MIT license
- https://github.com/bitcoin/bitcoin
- Note: Bitcoin Cash uses a very different consensus philosophy! Several competing implementations (https://cash.coin.dance/nodes). They denigrate the “Core implementation” model as “North Corea”

BIP (Bitcoin Improvement Proposal)

- Minor changes are done via pull request to the Bitcoin Core GitHub repository
- Major changes need a BIP
- Formally open to anyone, but there's definitely a lot to learn before you file a BIP!

Who's In Charge?

- **Developers** - They write the code.
- **Miners** - They write history and decide which transactions are valid.
- **Users** - They decide which consensus to follow.
- **Investors** - They buy and hodl, thus providing a value for Bitcoin.
- **Merchants** - They are the only ones who could make Bitcoin worth anything, by accepting it in return for goods and services.

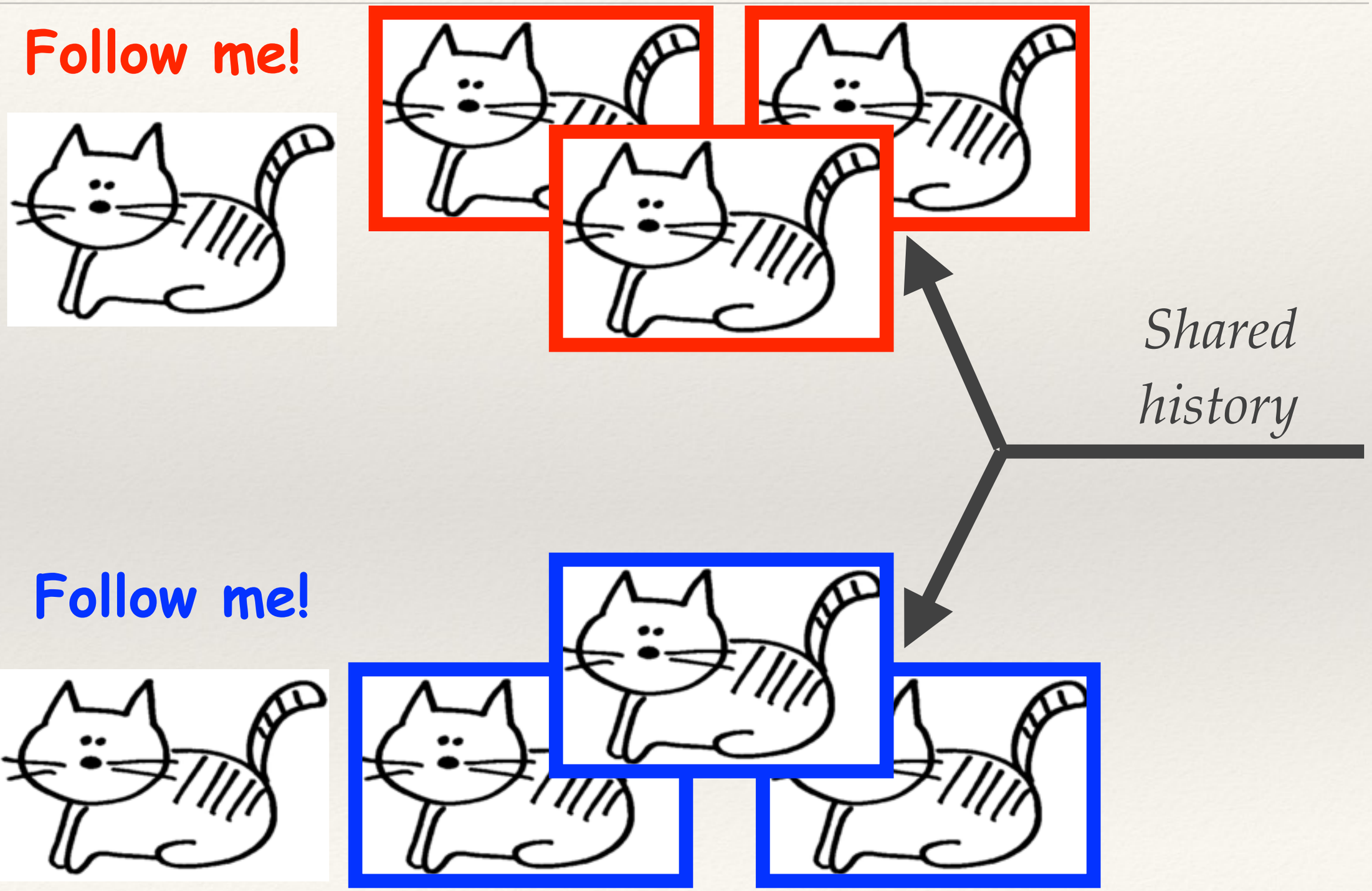
Bitcoin Core

Follow me!

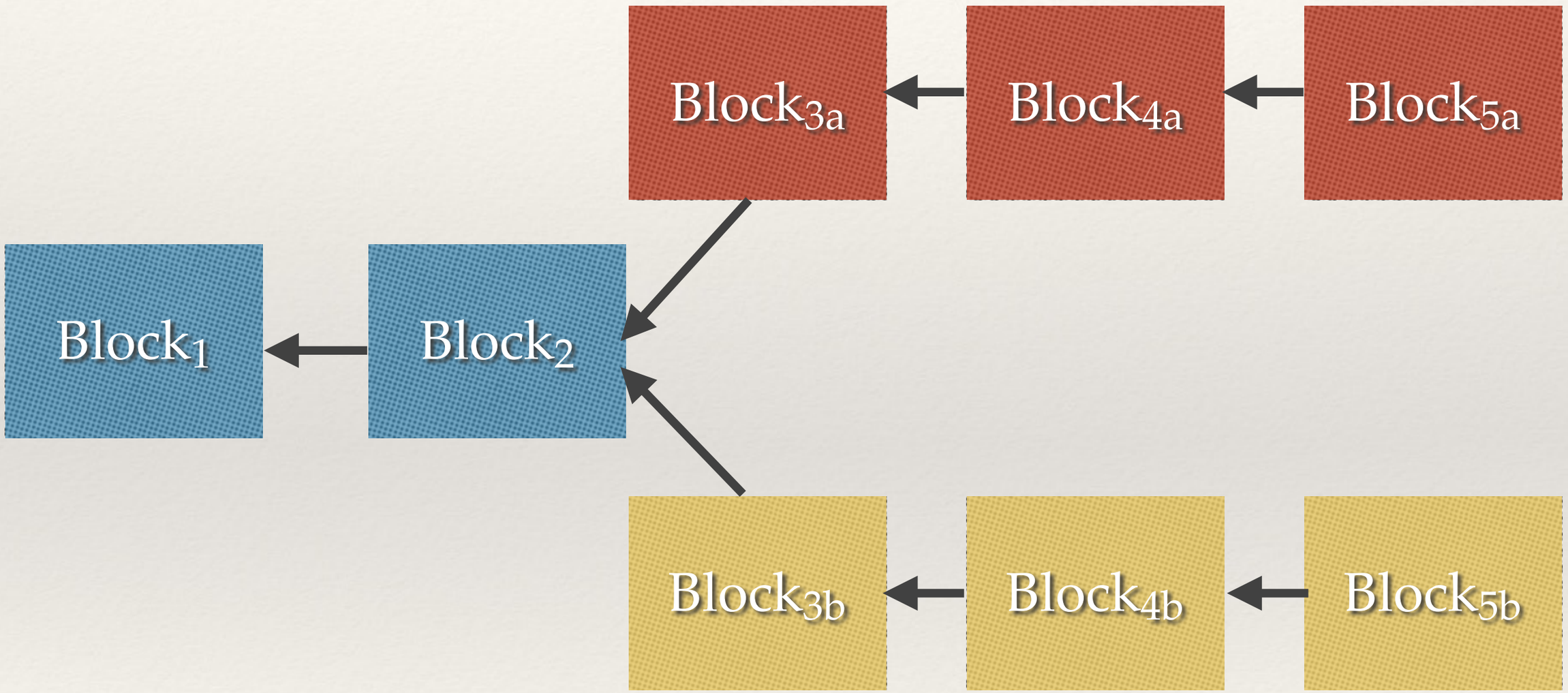
"We hold these truths to be self-evident, that all blockchain users are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are **Forking**, Liberty and the pursuit of Happiness"

–Thomas Jefferson (not really)

Hard Fork



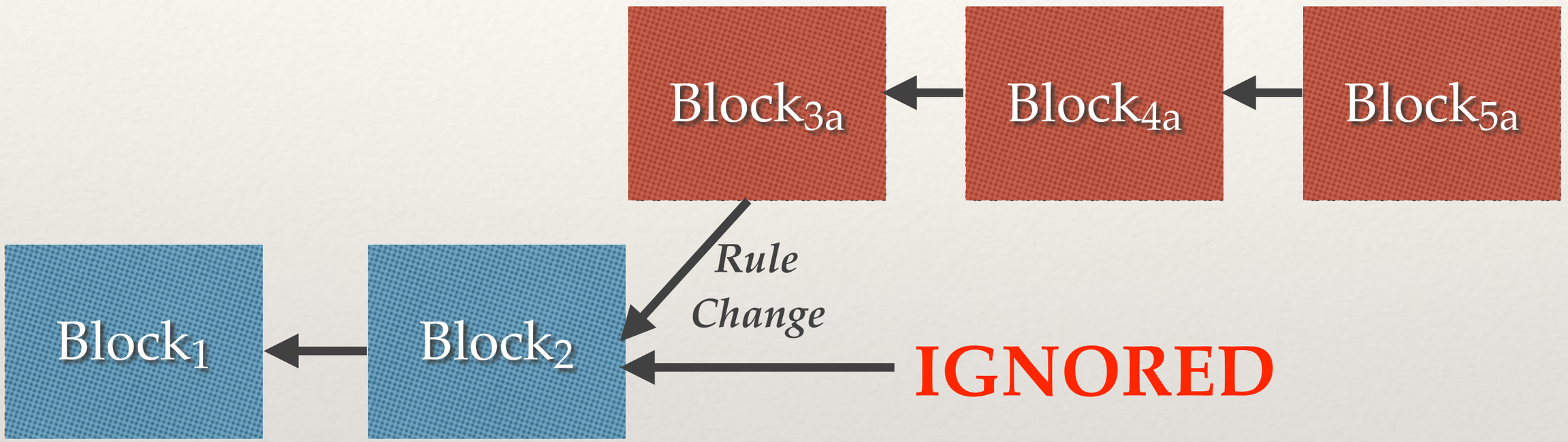
Blockchain Hard Fork



Hard Fork and New Currency

- Hard forks do not *necessarily* lead to a new currency
- Example: Monero hard-forks every six months -
  - “Monero Network Upgrade”
  - http://xmr.noctism.com/

Monero Network Upgrade



Bitcoin - Love it or leave it

- The right to fork and start your own currency - either by building off the current blockchain or creating your own blockchain is extremely powerful
- Nobody is holding you hostage - many people have started their own Bitcoin-related currencies

Major Bitcoin Forks

- **Bitcoin XT** - *8 MB blocks, launched late 2014. Failed to activate (needed 75% consensus).*
- **Bitcoin Classic** - *2 MB blocks, launched early 2016, officially folded in November 2017, officially supported Bitcoin Cash*
- **Bitcoin Cash** - *8 MB (now 32 MB) blocks, forked August 2017. By far the most popular Bitcoin fork.*
- **Bitcoin Gold** - *ASIC-resistant EquiHash algorithm replaced SHA-256, forked October 2017.*
- **Bitcoin Private** - *ASIC-resistant EquiHash algorithm replaced SHA-256, ZCash-style optional anonymity. Forked February 2018.*

Bitcoin Cash Split

- The largest split in Bitcoin history - August 1st, 2017
- **Bitcoin Cash:** Did not implement SegWit; increased block size to 8 MB
- **Bitcoin (Bitcoin Core)**: Implemented SegWit via UASF; modified block size limit to be a block weight limit

User-Activated Soft Fork (UASF)

- Nodes create a soft fork but without the support of miners
- Playing "chicken" with the miners! Proof of work majority will want to follow economic majority.
- Most famous UASFs: introduction of SegWit (BIP 141); introduction of P2SH (BIP 16)

Bitcoin Scalability Debate

- Second-tier scaling (“small-blockers”) vs increasing block size (“big-blockers”)

Small Blocker Arguments

- Increasing block size is a temporary solution
- Larger blockchain makes it harder for nodes to participate, thus centralizing nodes
- Centralized nodes make a future UASF more difficult (putting more power in hands of miners)
- Secondary scaling solutions are available
- Any hard fork is an attack vector on Bitcoin itself

Big Blocker Arguments

- Big blocks = more room for transactions, and thus lower fees
- Big blocks = faster transactions (less jockeying for space in a block, thus less waiting)
- Secondary scaling is ripe for centralization
- Secondary scaling is an additional attack/failure vector
- It might be slightly more difficult to run a node, but more people will use Bitcoin more often, thus incentivizing more people to run nodes

Satoshi's Thoughts

- The original Bitcoin did not have a block size limit
- Satoshi added it IN SECRET as part of another commit!
- Rumors that others who noticed it were asked to keep it secret, as well!
- Although not explained well, generally seen as an anti-DoS measure
- https://github.com/bitcoin/bitcoin/commit/a30b56ebe76ffff9f9cc8a666718617941 3c6349

What is Bitcoin?

- Store of Value? (small-blocker argument)
- Means of Exchange? (big-blocker argument)
- Both?