SCALING BLOCKCHAIN: CRYPTOCURRENCIES FOR THE MASSES

Gillian Chu
Brian Ho

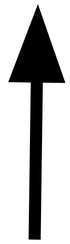
LECTURE OVERVIEW

1. BACKGROUND
2. NAIVE SOLUTION
3. VERTICAL SCALING BY CHANGING PARAMETERS
4. ADVANCED VERTICAL SCALING
5. HORIZONTAL SCALING

1 BACKGROUND

WHAT IS THE SCALABILITY PROBLEM?

SCALABILITY DEFINITION

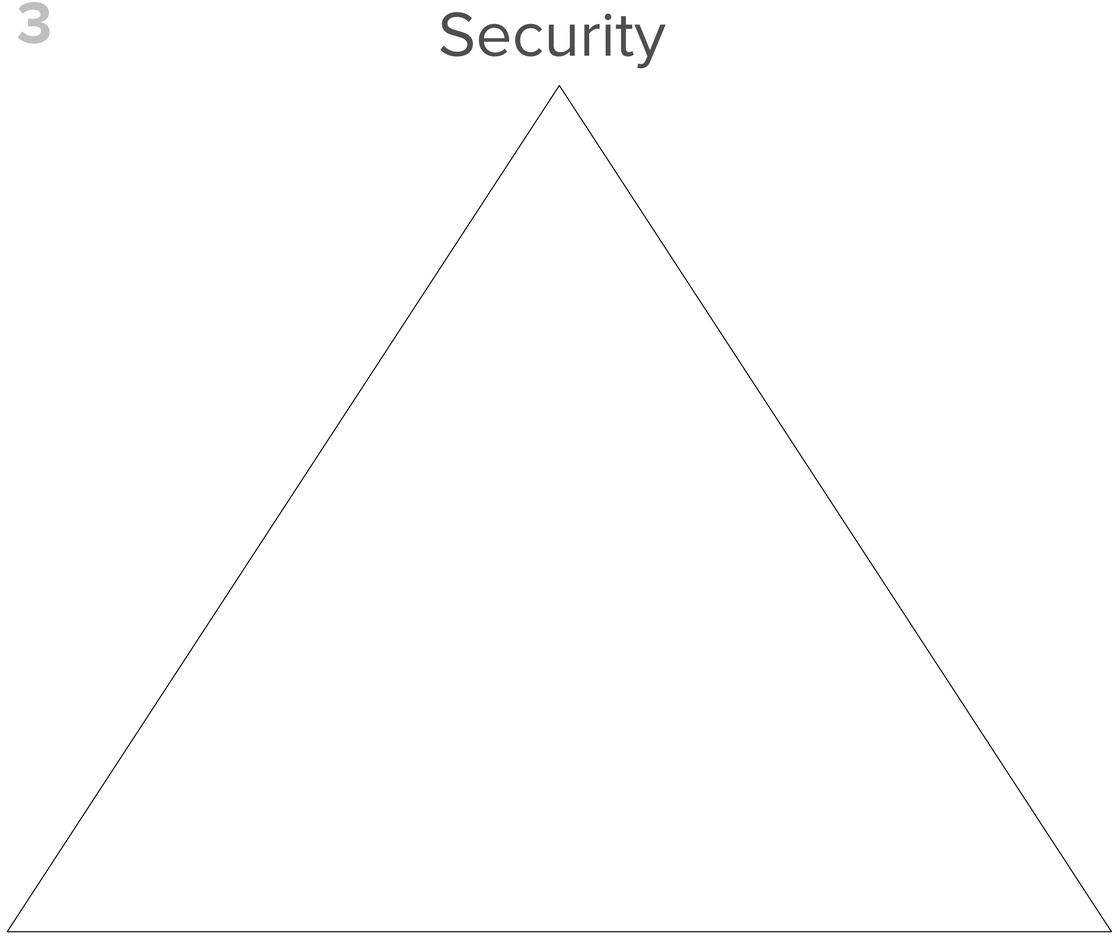


Volume of Transactions

Block Time

SCALABILITY TRILEMMA

PICK 2 OF THE 3



TRANSACTION SIZE

BLOCKCHAIN FUNDAMENTALS

Statistics

	Transaction Size
Observations	500
Mean	546.38
Median	530.94
Mode	391.77
Std. Dev.	69.58

500
546.38
530.94

https://tradeblock.com/bitcoin/historical/1d-f-tsize_per_avg-00271

AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN AT BERKELEY

MAX TRANSACTIONS PER SECOND

BLOCKCHAIN FUNDAMENTALS

From previous slide:

- Average of 546 bytes per transaction.
- Current blocksize is 1 MiB.
- Expected time to next block is 10 min.

Therefore we can compute the sustained maximum transaction volume in tps:

$$\frac{1\ MiB}{1\ block} \times \frac{1\ txn}{546\ bytes} \times \frac{1\ block}{10\ min} \approx 3.2\ tps$$

MAX TRANSACTIONS PER SECOND

BLOCKCHAIN FUNDAMENTALS

AUTHOR: GILLIAN CHU

TPS COMPARISONS

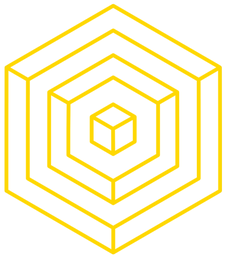
BITCOIN VS MODERN PAYMENTS

How does Bitcoin compare with other traditional payment systems?

	Average	High Load / Maximum
Bitcoin	3 tps	3.2 tps
PayPal*,**	150 tps	450 tps
VISA***	2,000 tps	56,000 tps

* https://investor.paypal-corp.com/secfiling.cfm?filingID=1206774-16-5430&CIK=1633917
** http://www.fool.com/investing/general/2016/02/04/5-things-paypal-holdings-inc-wants-you-to-know.aspx
*** https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf

QUESTIONS?



CURRENT SCALABILITY

BLOCKCHAIN FUNDAMENTALS

Variables we can play with to increase $\frac{\text{Transactions}}{\text{Second}}$

- Size of transactions
- Size of blocks

↑ Volume of Transactions

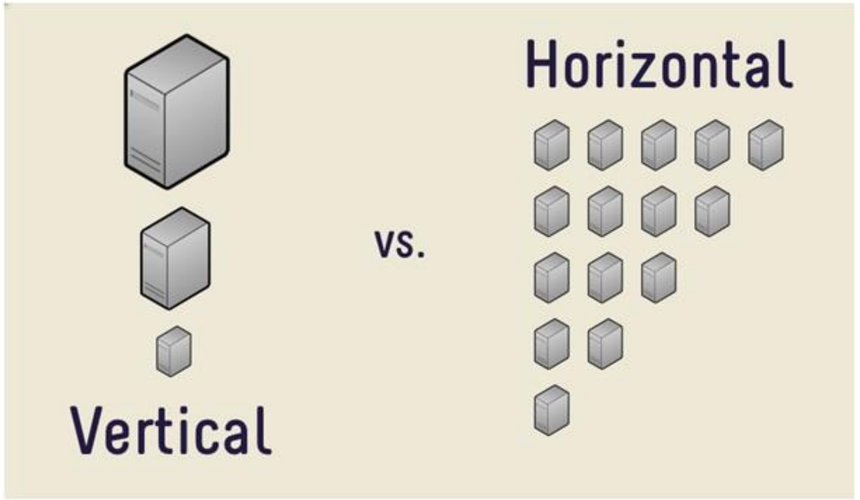
- Block creation rate

↓ Block Time

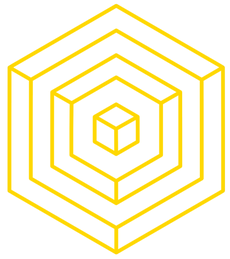
SCALING TECHNIQUES

HOW DO WE SCALE?

- **Vertical Scaling** - add more RAM/ CPU power to each existing machine
- **Horizontal Scaling** - add more machines of the same computational power
- **Diagonal Scaling** - add more powerful machines



AUTHOR: APARNA KRISHNAN
UPDATED: GILLIAN CHU



2

NAIVE SOLUTION

NAIVE SOLUTION

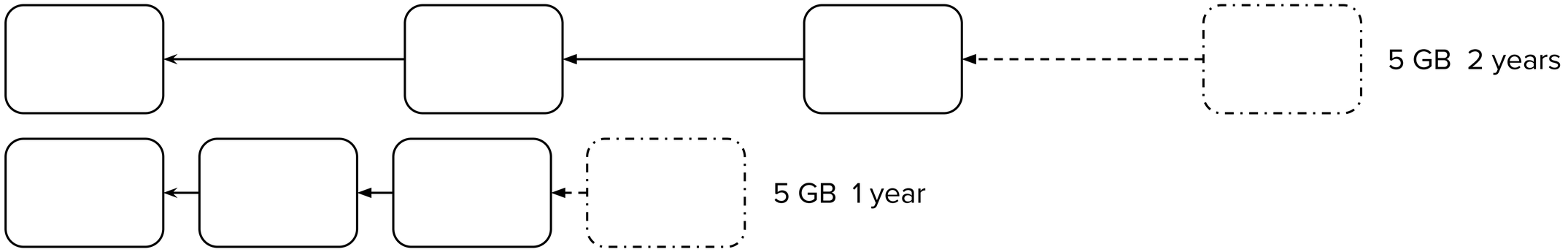
IDEA

Why not increase the speed of blocks by decreasing difficulty of the POW problem?

Time to broadcast block fixed while Block creation time decreases

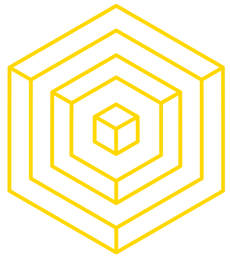
NAIVE SOLUTION

CONS



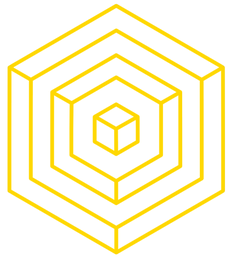
AUTHOR: SUNNY AGGARWAL &
APARNA KRISHNAN
UPDATED: GILLIAN CHU

QUESTIONS?



3

VERTICAL SCALING BY CHANGING PARAMETERS



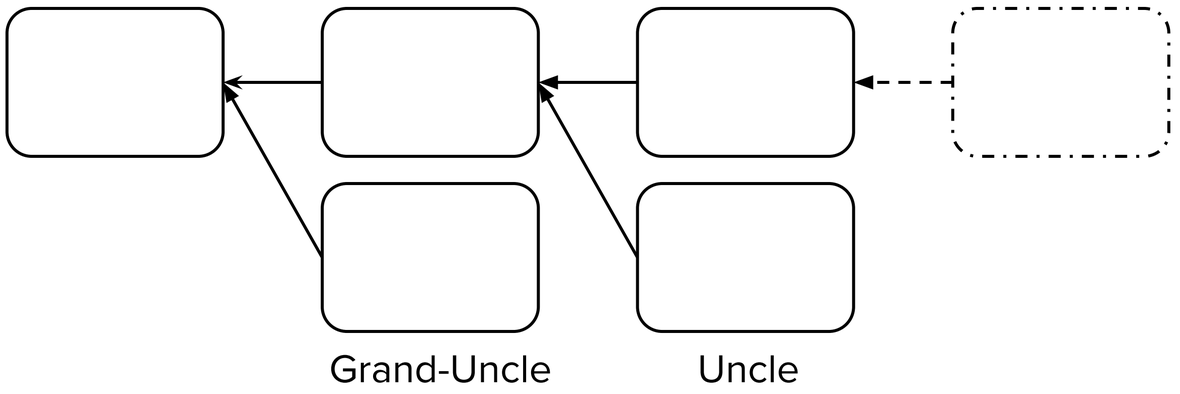
3.1

DECREASE BLOCK CREATION TIME

GHOST

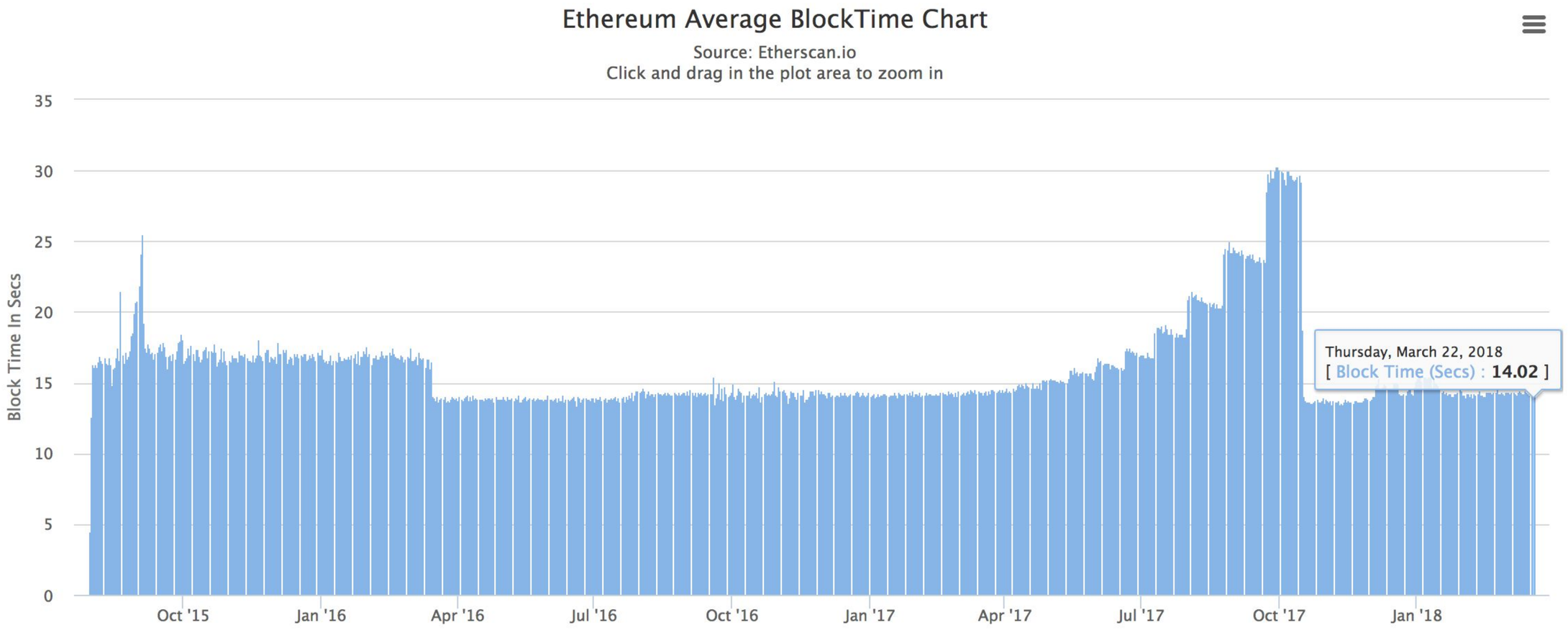
IDEA

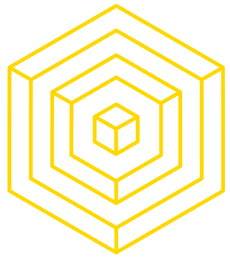
- Increase the speed of blocks by **decreasing difficulty of the POW + weighted POW blockchain** (instead of longest)
- + Decrease Incentive for Pooled Mining!



GHOST

IDEA


Ethereum Average BlockTime Chart
Source: Etherscan.io
Click and drag in the plot area to zoom in
Block Time In Secs
35
30
25
20
15
10
5
0
Oct '15
Jan '16
Apr '16
Jul '16
Oct '16
Jan '17
Apr '17
Jul '17
Oct '17
Jan '18
Thursday, March 22, 2018
[Block Time (Secs) : 14.02]



3.2

INCREASE BLOCKSIZE

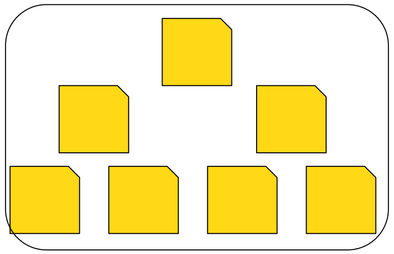
BLOCKSIZE INCREASE

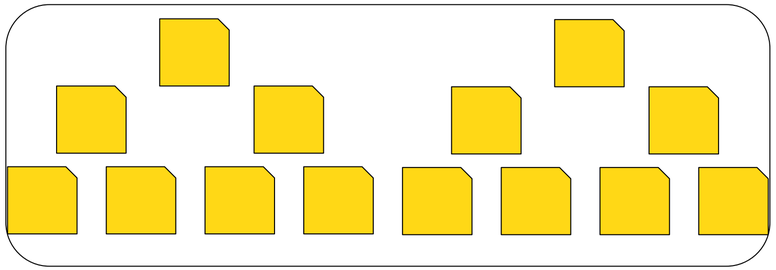
IDEA

If we just increase the blocksize, we can fit more transactions in a single block!

Pros:

- It's an "easy" implementation. Just get miners to agree.
- Lower transaction fees for users



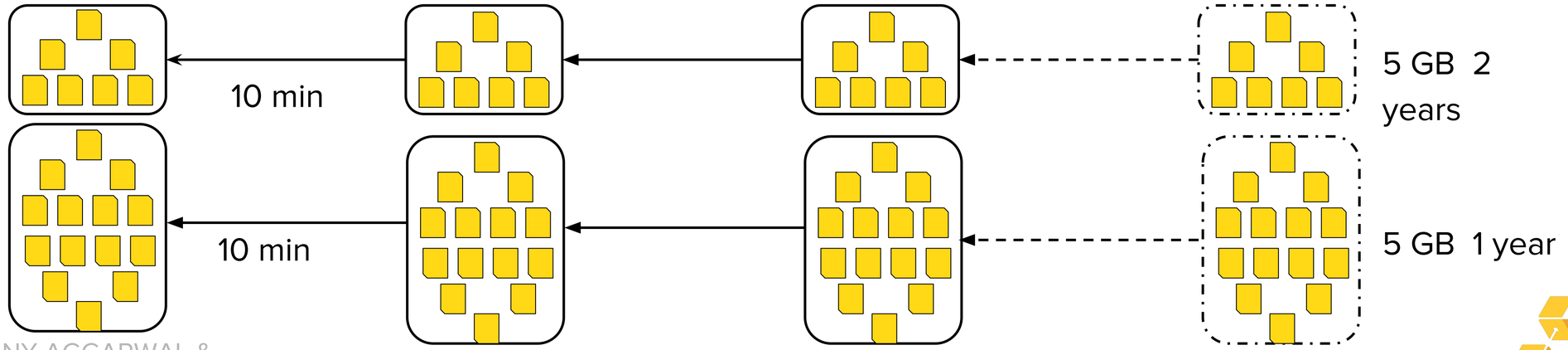


BLOCKSIZE INCREASE

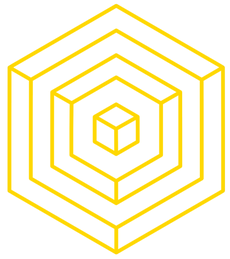
CONS

- Hard fork
- Lessen transaction fees
- Size increases very fast

- Longer Propagation Times
  - Authoring miner has better shot at next block
- One time linear capacity increase
  - Temporary Fix
- Large Transaction attack



AUTHOR: SUNNY AGGARWAL &
APARNA KRISHNAN



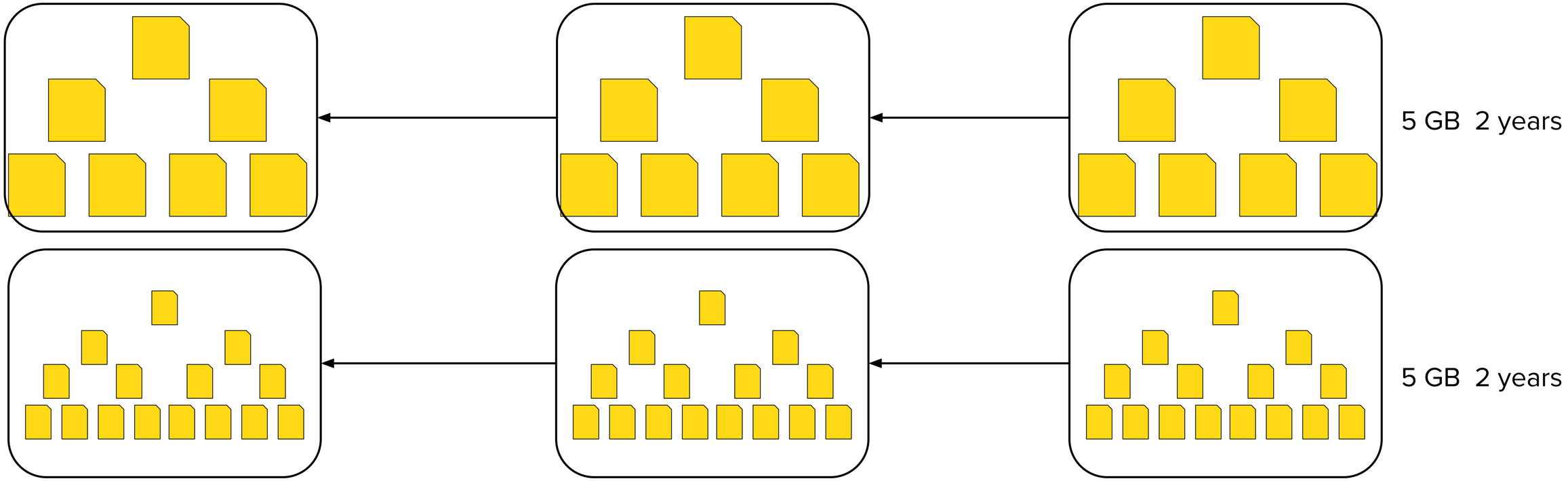
3.3

DECREASE SIZE OF TRANSACTIONS

DECREASE TRANSACTION SIZE

IDEA

- Segwit
- Recursive Snarks



SEGREGATED WITNESS

IDEA

SEGREGATED WITNESS

AVOID HARD FORK

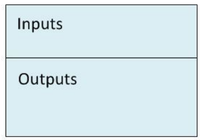
- Bitcoin Core is super conservative and wanted to avoid a hard fork
  - “Hacky fixes” in order to make it work with a soft fork

How:

Segwit P2W*

For Old Nodes:

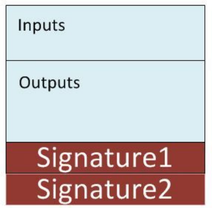
ScriptPubKey: 0 e4873ef43eac347471dd94bc899c51b395a509a5
ScriptSig: Empty
Result: **Valid**



Segwit P2W*

For New Nodes:

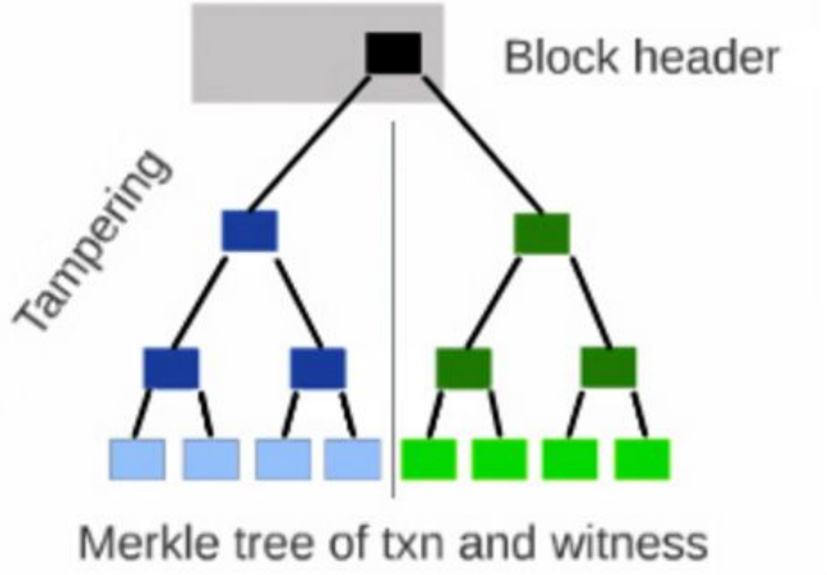
ScriptPubKey: 0 e4873ef43eac347471dd94bc899c51b395a509a5
ScriptSig: Empty
WitScript: Signature1
Result: **Valid**

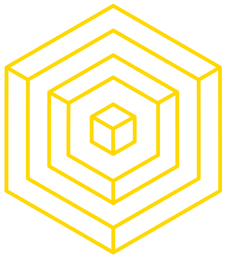


SEGREGATED WITNESS

MIRROR SIGNATURE TREE

But now, the blockchain doesn't have any evidence that correct signatures were included in transactions?





SEGREGATED WITNESS

PROS AND CONS

Pros:

- Only soft fork
- Fixes Transaction Malleability
  - Allows Lightning Network and sidechains to work
- No slippery slope
- Efficiency Gains
- Smaller Size of Blockchain

Cons:

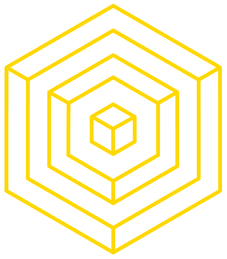
- One time linear capacity increase
- Introduces new type of DOS attack (go-fish-wit-ddos)
- Very complicated and ugly (Over 500 lines of code)
- Other ways to solve malleability
- Wallets have to incorporate it

RECURSIVE SNARKS SCALABILITY

BLOCKCHAIN FUNDAMENTALS

zk - SNARKS - Zero Knowledge Succinct Non-Interactive Arguments of Knowledge

QUESTIONS?

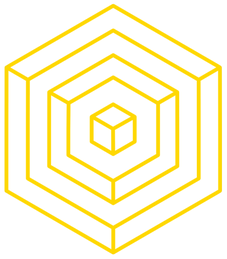


RECURSIVE SNARKS SCALABILITY

IDEA

Generate proof that you can send a valid transaction from Alice to Bob.

- Include this proof and changes to the balance sheet instead of the transaction itself.
- Any machine in the network can verify the proof in milliseconds



RECURSIVE SNARKS SCALABILITY

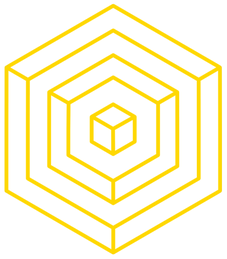
IMPROVEMENTS

Miner can merely include a single proof that they validated all the other proofs and changes to the state.

```
BLOCK = root hash of the content of the ledger +
        proofs of valid transactions that changed
        ledger to current state +
        proof that previous block's proof is valid
```

Verify blockchain in under 1s + include 2x transactions per block

avg tx size = 546 bytes, avg proof size = 288 bytes



RECURSIVE SNARKS SCALABILITY

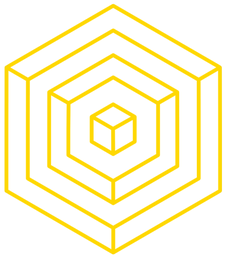
DRAWBACKS

Generate proof that you can send a valid transaction from Alice to Bob.

- Include this proof and changes to the balance sheet instead of the transaction itself.
- Any machine in the network can verify the proof in milliseconds

Drawbacks

- Proofs are too time consuming to generate, could take hours.
- Requires Trusted Setup



NOW WHAT?

BLOCKCHAIN FUNDAMENTALS

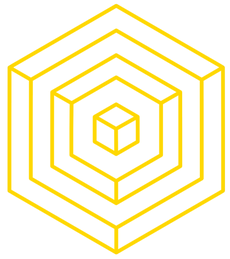
What are the variables we can play with?

- Size of blocks
- Size of transactions
- Block creation rate

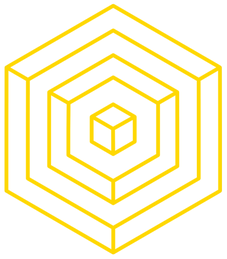
$$\frac{1\ MiB}{1\ block} \times \frac{1\ txn}{546\ bytes} \times \frac{1\ block}{10\ min} \approx 3.2\ tps$$

We need to change something else. Let's just not use the blockchain!


BREAK
SECTION
BLOCKCHAIN
AT BERKELEY



4 VERTICAL SCALING OFF-CHAIN

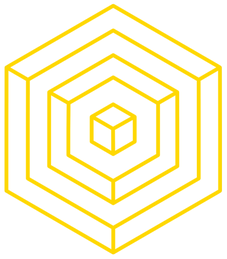


RECALL: BITCOIN TRANSACTIONS

ISSUE WITH BITCOIN PAYMENTS

- **Long delays**
  - 6 confs = about 1 hour wait
- **High Fees**
  - = **$6.75 avg tx fees** (as of 2017-11-04)
  - Not economical for Alice to buy low-value items

Source: https://bitcoinfees.21.co/



PAYMENT CHANNEL BUILDUP

PRIVATE CHANNELS

Idea:

- Can Alice and Bob make payments between themselves without always needing to consult the blockchain?

PAYMENT CHANNEL BUILDUP

PRIVATE CHANNELS

Idea:

- What if Alice and Bob maintain a **private balance sheet**
  - update the private balance sheet with every payment
  - only consult the blockchain when they want to settle the balance

Alice and Bob's Balance Sheet	
Alice	Bob
10 BTC	5 BTC

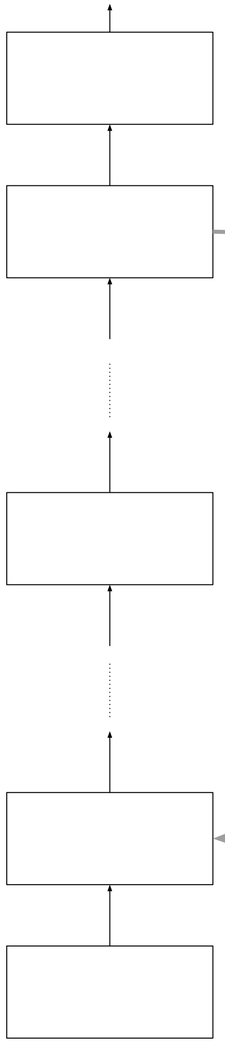
Alice pays Bob 2 BTC

Alice and Bob's Balance Sheet	
Alice	Bob
8 BTC	7 BTC

PAYMENT CHANNEL BUILDUP

PRIVATE CHANNELS

Alice and Bob only make a transaction on the blockchain when they want to settle their private balances.



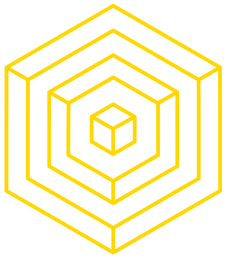
Alice and Bob open a private balance sheet

Alice and Bob's Balance Sheet	
Alice	Bob
10 BTC	0 BTC

Alice and Bob make several private txns.

Alice and Bob's Balance Sheet	
Alice	Bob
3 BTC	7 BTC

Alice and Bob later close the balance sheet



PAYMENT CHANNEL BUILDUP

IDEA

- Use Bitcoin script to create blockchain-enforceable contracts between Alice and Bob so that neither party can cheat the other, while maintaining the private balance sheet functionality!
- In blockchain land, we call these **payment channels**.
- Payment channel's full name: *Hash Time-locked Bi-directional Payment Channel* or *HTLC*.

PAYMENT CHANNEL PAYMENTS

BLOCKCHAIN FUNDAMENTALS

State 0: Total 10 BTC	What Bob needs to claim 1st (on chain)	What Alice needs to claim 1st (on chain)
Alice: 10 BTC	Alice Sig	Bob Sig + Alice Secret 1 or Alice Sig + 1000 blocks
Bob: 0 BTC	Alice Sig + Bob Secret 1 or Bob Sig + 1000 blocks	Bob Sig

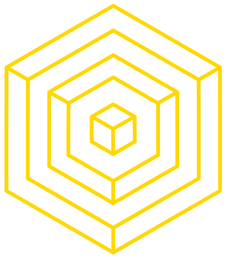
PAYMENT CHANNEL PAYMENTS

BLOCKCHAIN FUNDAMENTALS

State 0: Total 10 BTC	What Bob needs to claim 1st (on chain)	What Alice needs to claim 1st (on chain)
Alice: 10 BTC	Alice Sig	Bob Sig + 32874494 or Alice Sig + 1000 blocks
Bob: 0 BTC	Alice Sig + 1273394 or Bob Sig + 1000 blocks	Bob Sig

State 1: Total 10 BTC	What Bob needs to claim 1st (on chain)	What Alice needs to claim 1st (on chain)
Alice: 7 BTC	Alice Sig	Bob Sig + Alice Secret 2 or Alice Sig + 1000 blocks
Bob: 3 BTC	Alice Sig + Bob Secret 2 or Bob Sig + 1000 blocks	Bob Sig

Alice sends 3 BTC to Bob!

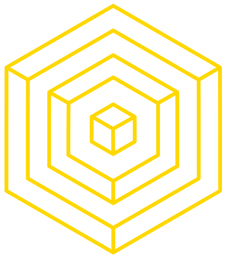


PAYMENT CHANNEL CONCLUSIONS

BLOCKCHAIN FUNDAMENTALS

Observation:

- If one tries to cheat, the other can always override and take all the money in the deposit.
- If Alice and Bob always cooperate
  - never have to touch the blockchain, except when creating the payment channel and settling the balance.
- Only two transactions on the blockchain
  - Supports arbitrary number of local transactions between Alice and Bob.



PAYMENT CHANNEL CONCLUSIONS

BLOCKCHAIN FUNDAMENTALS

Issue:

- Alice and Bob need to have capital locked up in this HTLC (Hash Time-Lock Contract) before they can send money between each other.

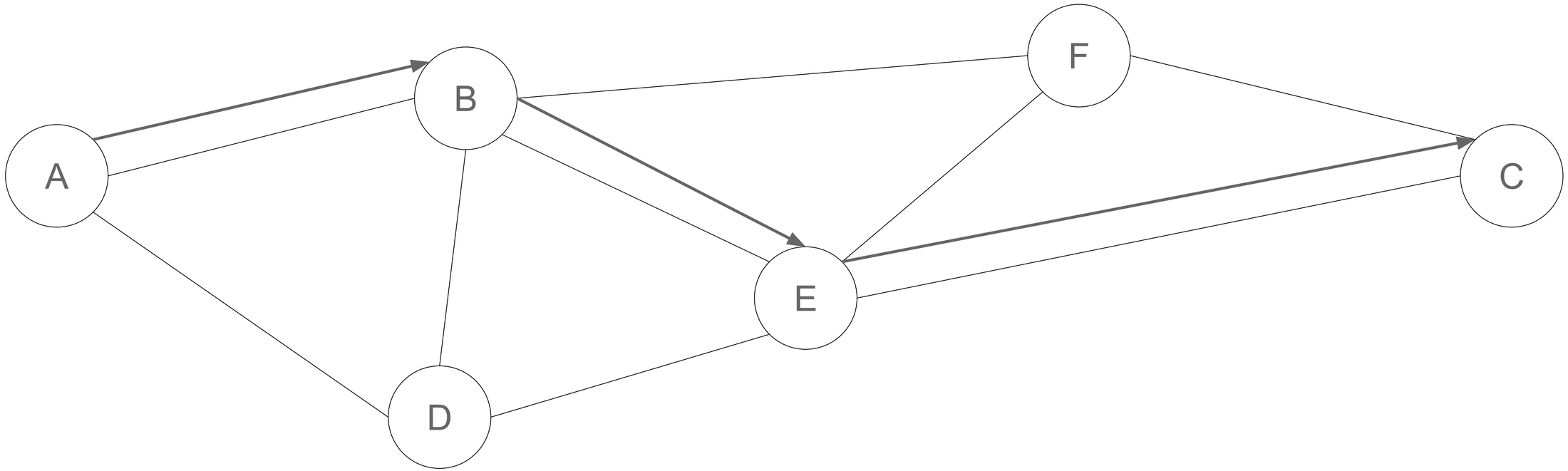
Issue:

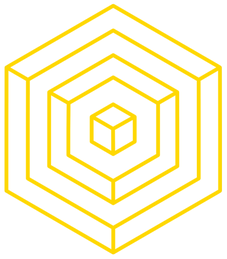
- With this payment channel, Alice and Bob can only easily and scalably send money between themselves.

LIGHTNING NETWORK

BLOCKCHAIN FUNDAMENTALS

- Alice sends money to Charlie through this hypothetical payment channel network





LIGHTNING NETWORK

BLOCKCHAIN FUNDAMENTALS

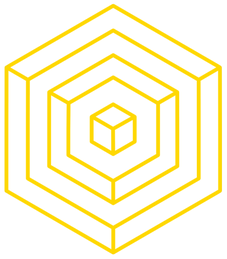
Can we do this securely?

- With some small additions on top of our HTLC construction, we can trustlessly send money across a network of HTLCs!

The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments

- By Joseph Poon & Thaddeus Dryja

https://lightning.network/lightning-network-paper.pdf



LIGHTNING NETWORK SCALABILITY

BLOCKCHAIN FUNDAMENTALS

What does the Lightning Network mean for scalability?

1. If we assume that there is enough capital in this payment channel network, *people can make payments instantly*.
   a. don't need to wait for confirmation times
   b. transactions as fast as communication delay across network.
2. Only use the Bitcoin Blockchain as an arbiter to settle disputes and close out payment channels
   a. far fewer (expensive) transactions on the Blockchain.

LIGHTNING NETWORK SCALABILITY

BLOCKCHAIN FUNDAMENTALS

What does the Lightning Network mean for scalability?

3. Instead of 3 tps, the Bitcoin network can support 10,000's+ of tps
   a. delegate payments to simple bookkeeping in each payment channel
   b. kept off-chain 99% of the time!
4. Sending packets across the internet is very cheap and fast.
   a. Lightning Network transaction fees will be several orders of magnitude cheaper.
   b. Only pay expensive fees on channel open / close.

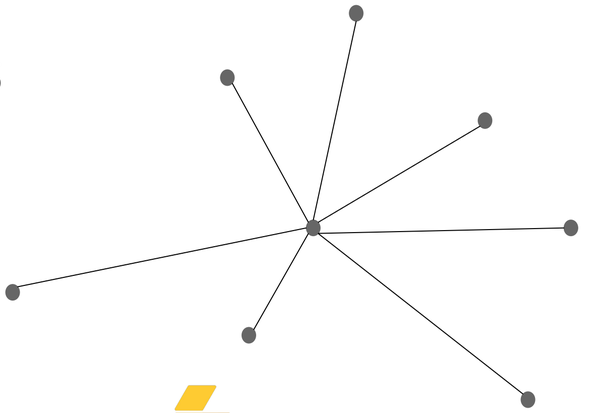
LIGHTNING NETWORK SCALABILITY

BLOCKCHAIN FUNDAMENTALS

Issues with Lightning Network:

1. Nodes need to keep very large amounts of capital locked up in payment channels.
    a. problematic if most payments in only one direction
2. **Strong centralization force**, since only nodes with significant capital can afford to hold payment channels for long.
    a. Larger payment channels get settled less often, less fees
3. **Less capital is required with less nodes** on the network
    a. ⇒ tendency towards *hub-and-spoke network topology*.

Hub-and-Spoke Topology

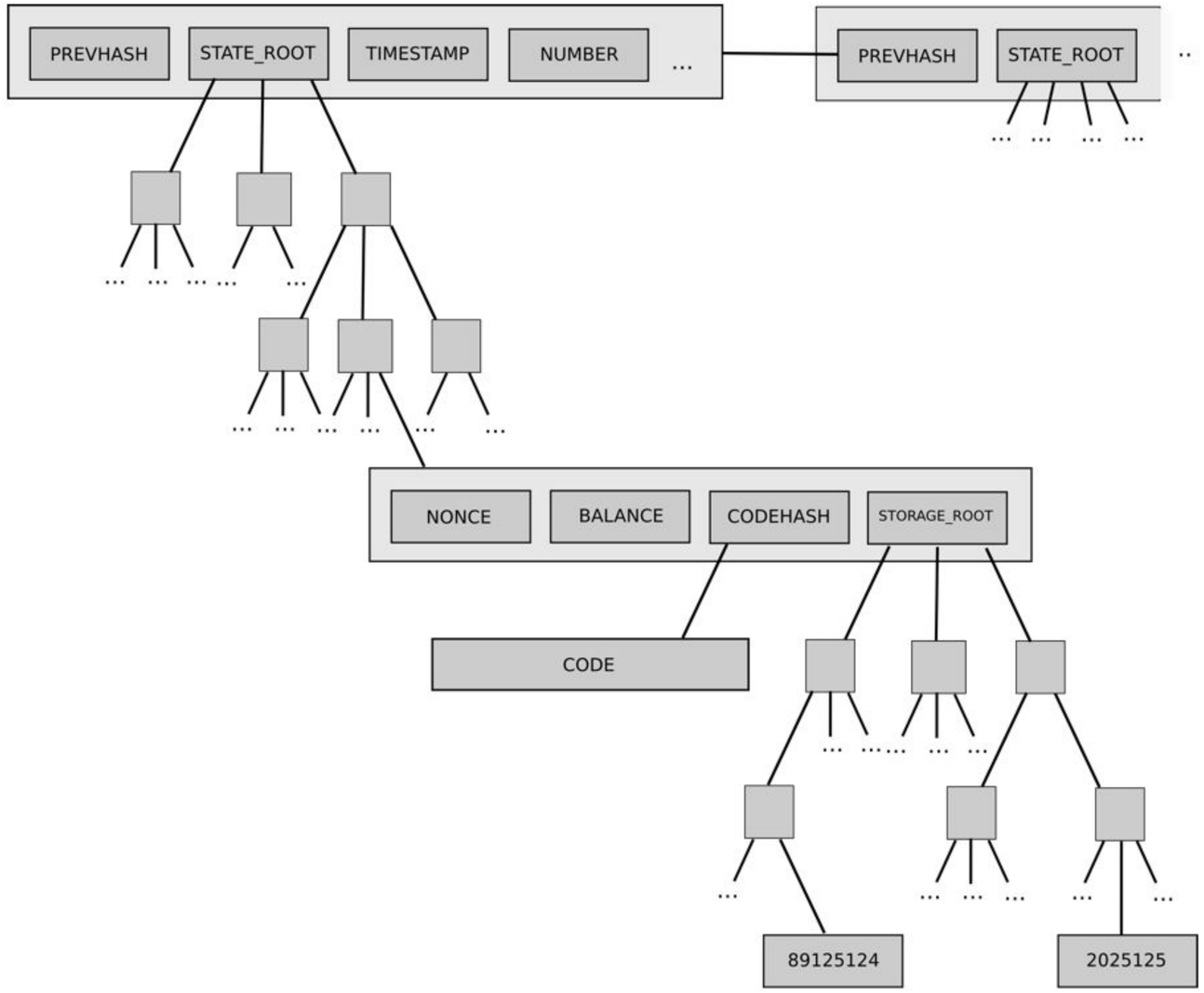


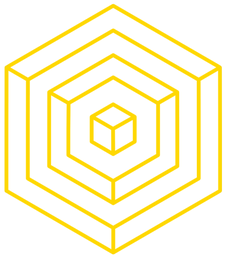
5 HORIZONTAL SCALING

SHARDING

IDEA

Sharding is the idea of not requiring every miner to be working on every single block, essentially creating parallel but connected blockchains.





SIDECHAINS

BITCOIN SIDECHAINS

Idea: If you can't speed up the bitcoin blockchain, why not create multiple blockchains with approx. 10 minute block times?

One could move their bitcoin over to a faster, less-secure blockchain for purchasing their morning coffee.

Pros:

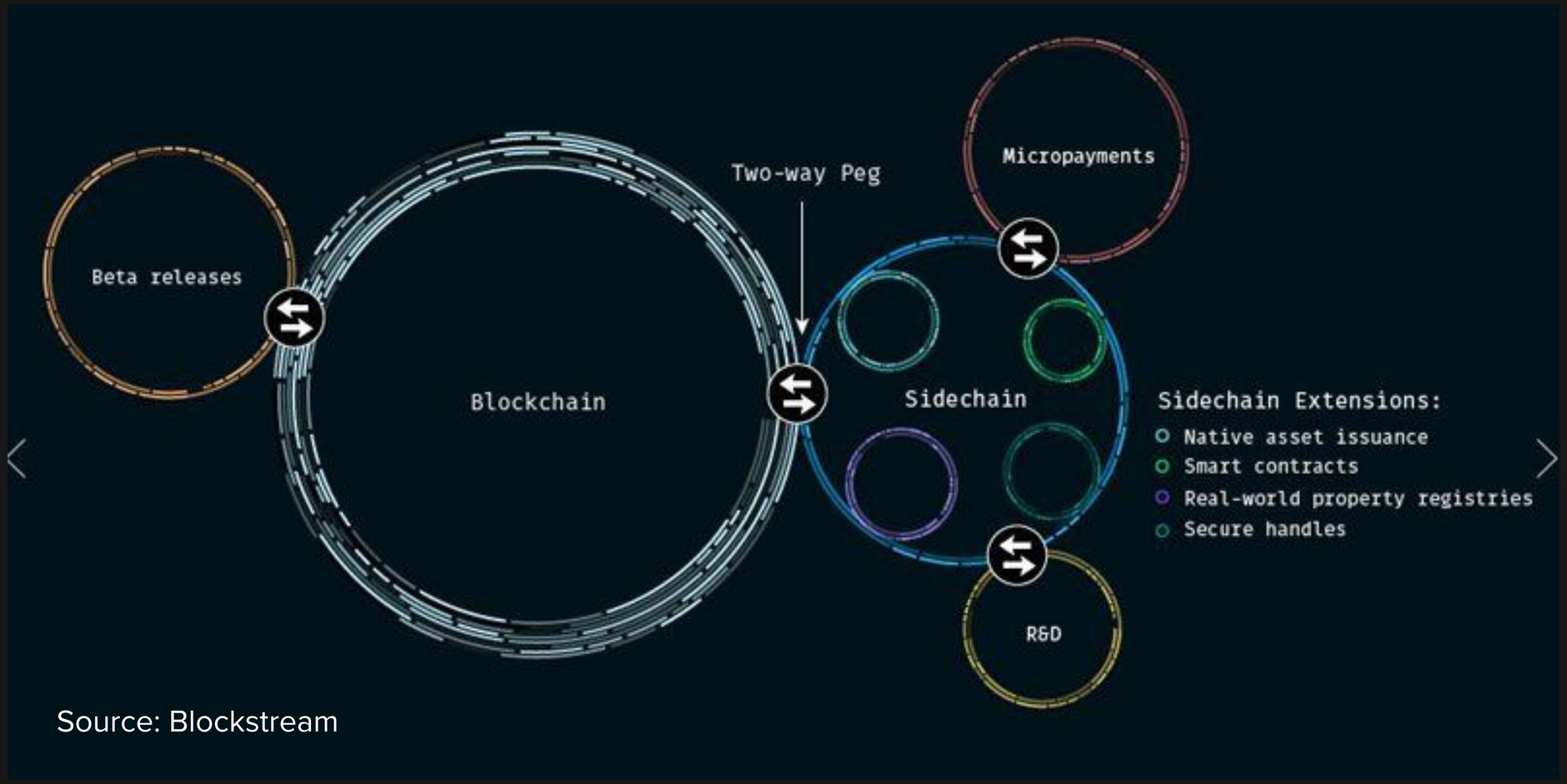
Less things on bitcoin blockchain, but can still be pegged to it.

Cons:

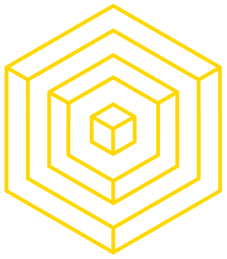
Loses security as hashing power is spread over multiple chains.

SIDECHAINS

BLOCKCHAIN FUNDAMENTALS



Source: Blockstream

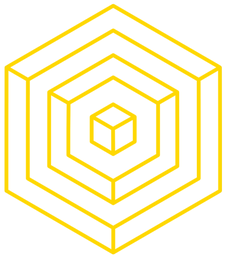


SCALABILITY SUMMARY

BLOCKCHAIN FUNDAMENTALS

Bitcoin and other similar Blockchains have an inherent scalability issue:

- If they want to be used on a global scale, they need to support global transaction volumes.
- Can we solve this issue without compromising Bitcoin's original vision of secure, decentralized, trustless payments?



SCALABILITY SUMMARY

BLOCKCHAIN FUNDAMENTALS

1. **Blocksize Capacity Increase**
   a. Small scalability boost with larger blocks.
   b. Centralization risk as minimum server requirements for nodes increases.
2. **Segregated Witness (SegWit)**
   a. Small scalability boost since blocks don't need to store signatures.
3. **Sidechains**
   a. Potential for large scalability boost
   b. Potential novel sidechains with better scalability (yet to be seen in practice)
4. **Lightning Network**
   a. Large potential for orders-of-magnitude scalability boost.
   b. Significant restructuring of payment process.
   c. Centralization risk due to capital prereqs.