

An overview of proof-of-work and proof-of-stake consensus

Valeria (Lera) Nikolaenko
The 13th BIU Winter School on cryptography

al6z
crypto

Outline

0

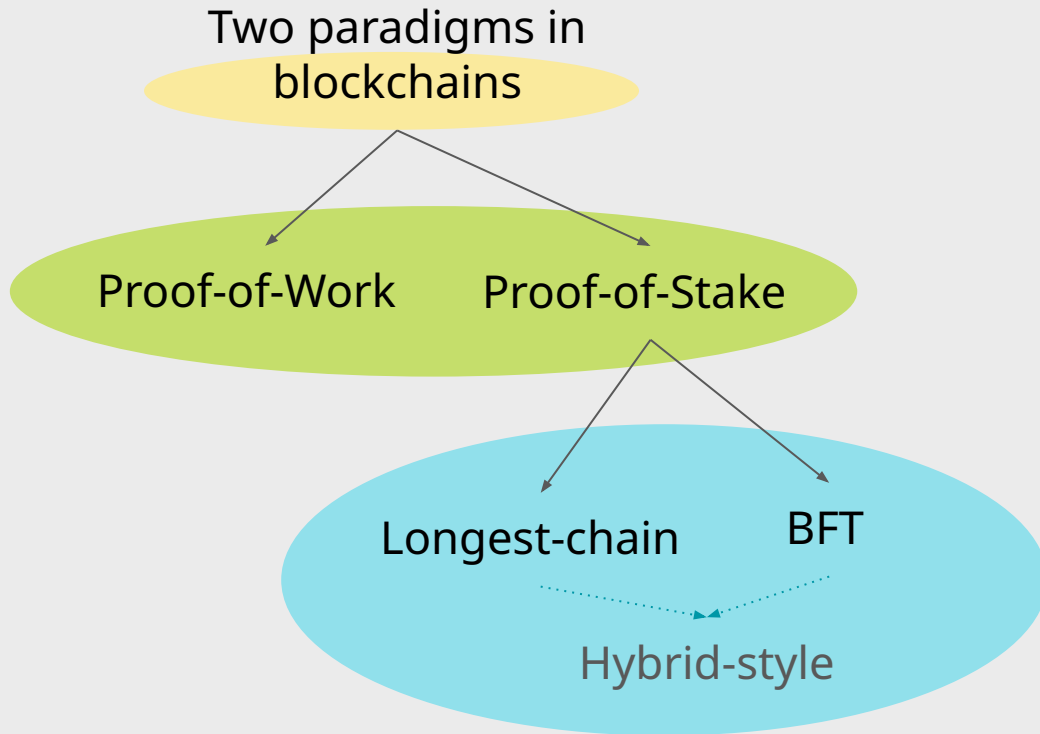
Def a blockchain

1

PoW vs PoS

2

Longest-chain vs BFT



0: What is a blockchain?

Blockchain : what is it?

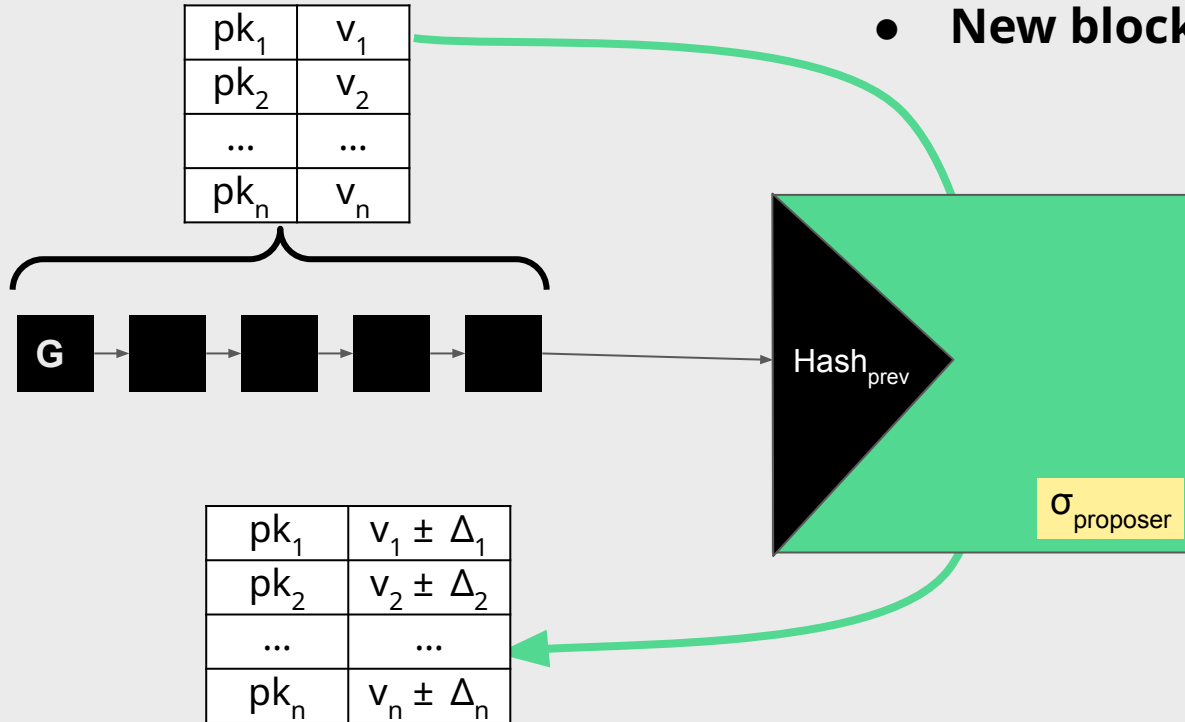
Blockchain is a distributed ledger - a log of transactions*.



- Blockchain is a chain of blocks.
- Each block is a list of transactions + hash of the previous block.
- Safety: everybody agrees on history.
- Liveness: every valid transaction eventually gets added
=> not censoring

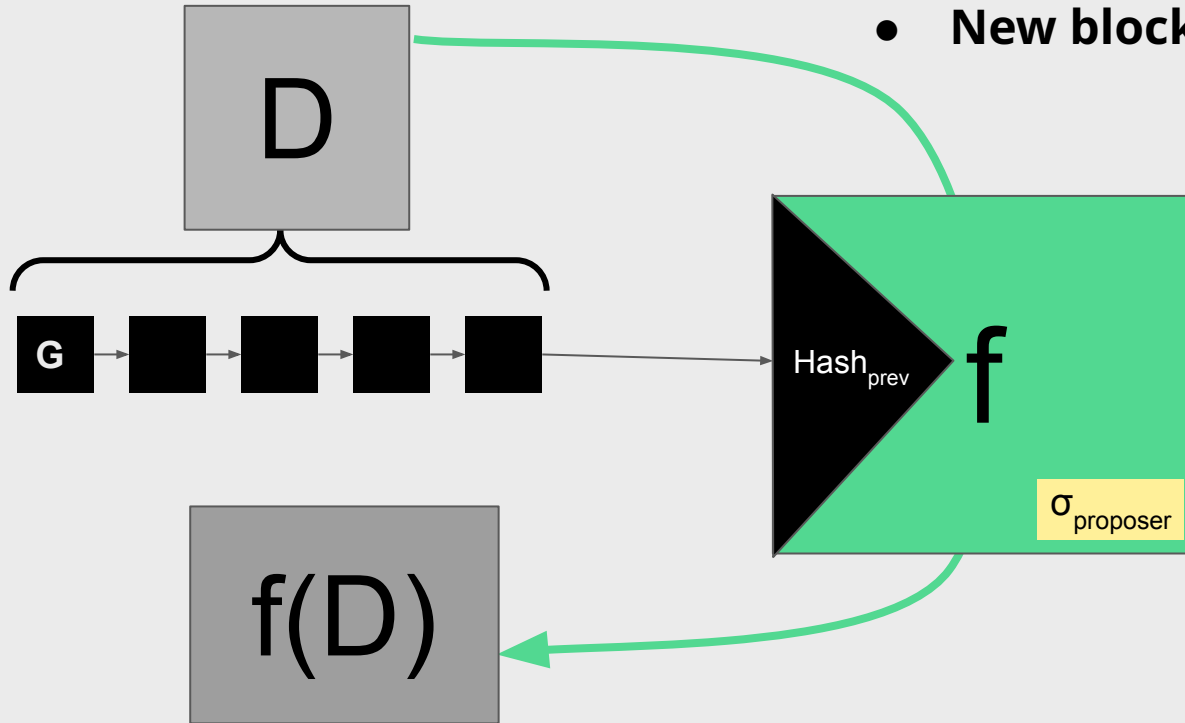
Blockchain : what is it?

- **Blockchain's prefix defines a state**
- **New block transforms the state**



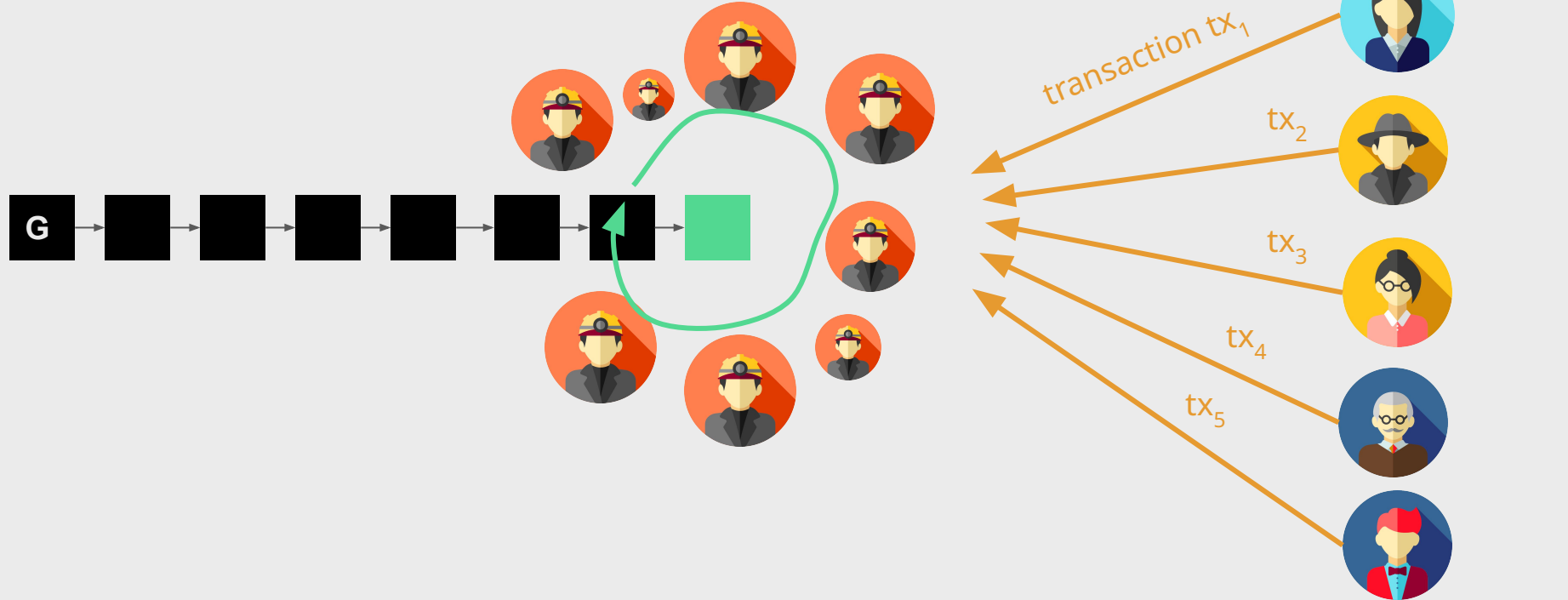
Blockchain : what is it?

- **Blockchain's prefix defines a state**
- **New block transforms the state**

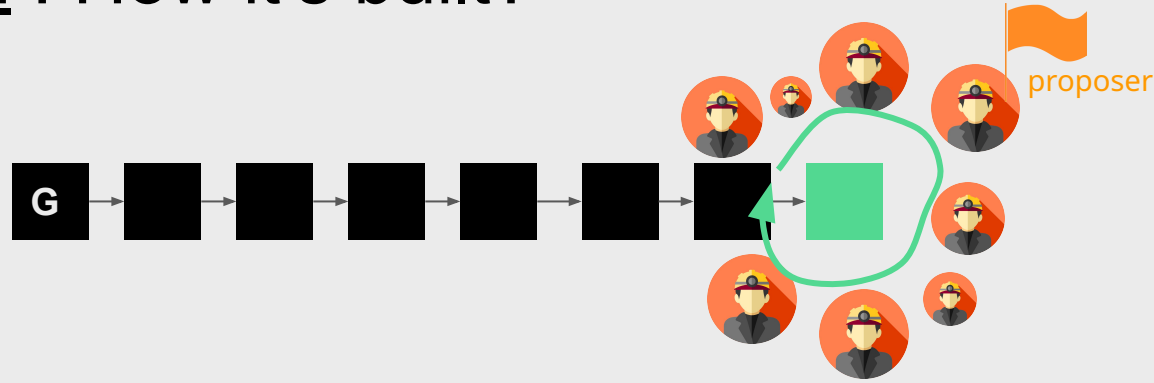


Blockchain : How it's built?

Nodes cooperate on building the next block
Block = a list of ordered transactions



Blockchain : How it's built?



1. A proposer(s) is elected to announce a new block
Pre-electing a proposer limits the options for Step 2
2. Everybody decides whether to accept this block or ignore

Consensus
mechanism

Outline

0

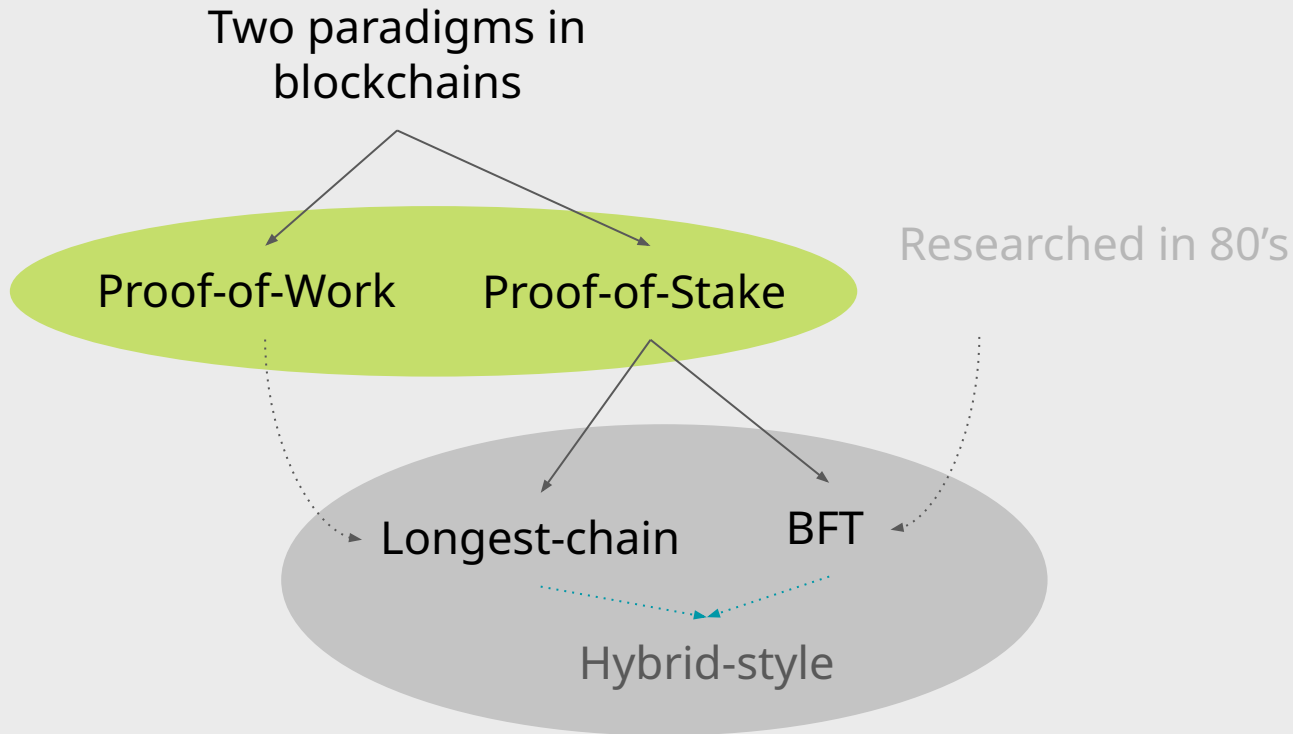
Def a blockchain

1

PoW vs PoS

2

Longest-chain vs BFT



1: Proof-of-Work vs. Proof-of-Stake for proposer election

Proof-of-Work for proposer election

- The proposer searches for a block B , s.t. **Hash(B) < target**.
 - For a hash function Hash: $\{0,1\}^* \rightarrow \{0,1\}^{256}$
 - Find B , s.t. $\text{Hash}(B) < 2^{256} / D$ (takes time $O(D)$ to solve)
 - D - "difficulty"
 - Currently for Bitcoin $D \approx 2^{45}$ a block is found once in 10 min

Proof-of-Work for proposer election

- The proposer searches for a block B, s.t. **Hash(B) < target**.
- Once found, announce B it to peers.
- Easy to verify the proposer.

Blocks are hard to find =>
small number of possible proposers

This proposer election mechanism:

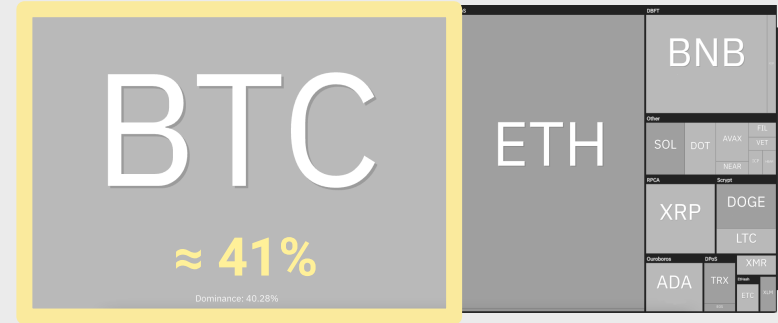
- **Live:** blocks are proposed regularly ✓
- **Fair:** each miner is elected proportional to its computational power ✓
- **Permissionless:** open participation ✓



Proof-of-Work electricity loss

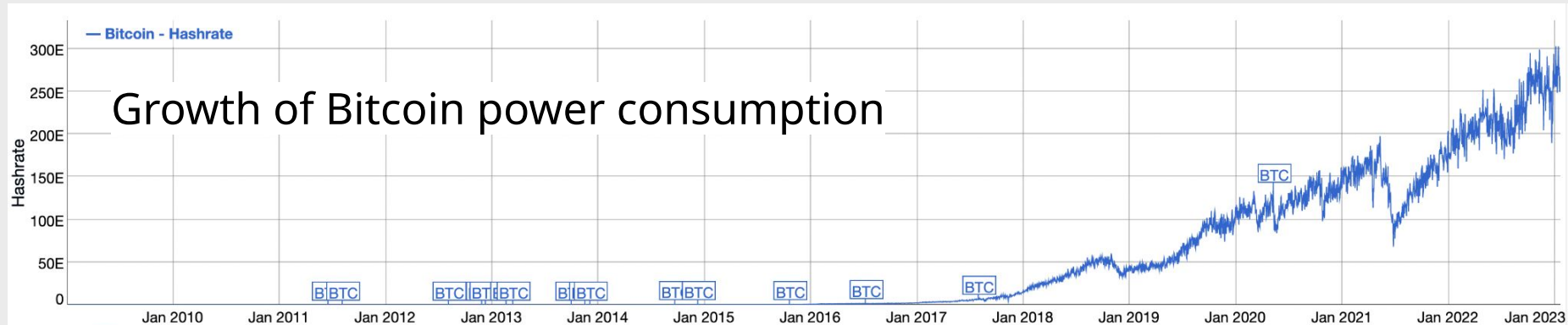
- Bitcoin: 85 TWh/yr (June 2022)
- Ethereum: 50-100 TWh/yr (June 2022)
- Argentina: 130 TWh/yr
- Mining gold: 240 TWh/yr

Market-cap of coins:



Jan 2022, <https://coin360.com/>

| Bitcoin + Ethereum | < Mining gold

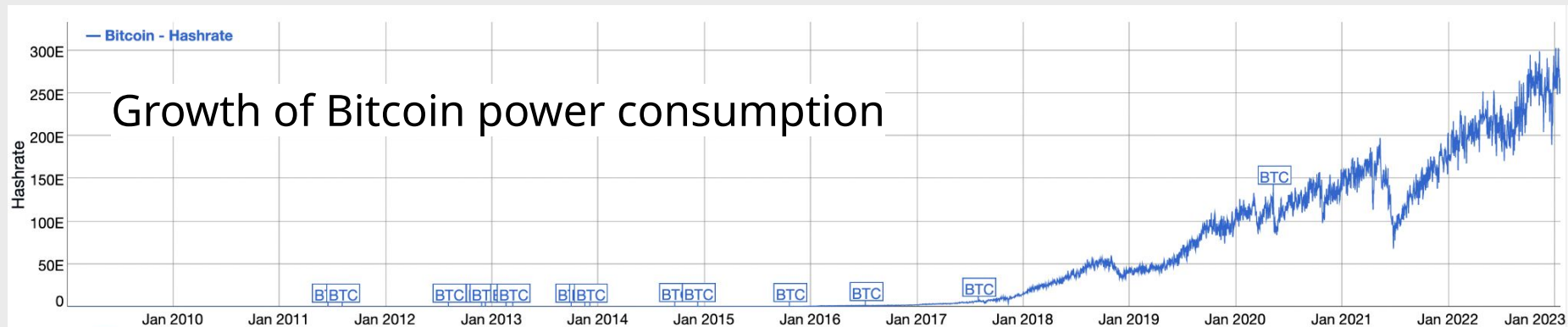


Useful number to keep in mind!

Bitcoin hash-rate:

- 200 EH/s = 2^{76} hashes per 10 min
- 6.25 BTC per block/per 10 min \approx \$150,000

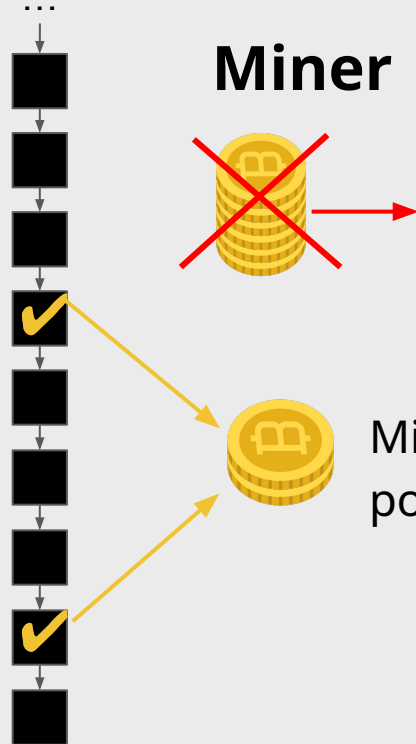
2^{76} hashes per \$150,000



Can we make PoW better?

- Increase the block size
 - Delays in block propagation => chain will fork more => decreases reliability
- Increase the frequency of the blocks
 - Gervais et al. (CCS'16): Bitcoin block frequency can be reduced to 1 min
- Lightning network: off-chain transactions
- Change the proof-of-work puzzle
 - proof-of-**useful**-work
- Bitcoin-NG:
 - use PoW sporadically to elect the leader for a longer duration of time (to propose multiple blocks).

Proof-of-Work mining



Miner spends coins for hardware and electricity.

Miner's reward is proportional to the computational power, i.e. proportional to the money spent.

Proof-of-Stake mining



Proof-of-Stake for proposer election

- The validator (miner) locks* T coins
- N - number of validators
- Simplest approach: round-robin
- The validator is elected as a proposer with probability $1/N$

Desired properties:

- **Live** ✓
- **Fair** ✓
- **Permissionless**: open participation ✓?
 - Validator needs to be able to acquire coins.

* "locking" coins requires the blockchain to have basic smart-contract capabilities

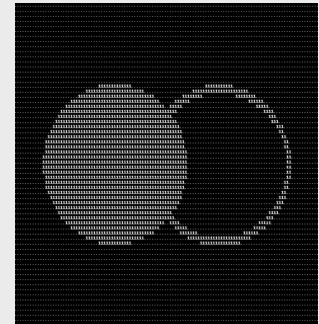
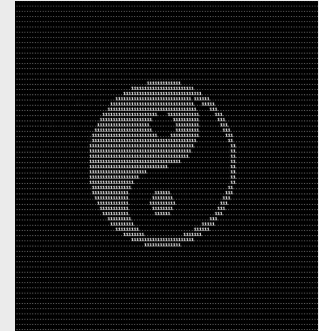
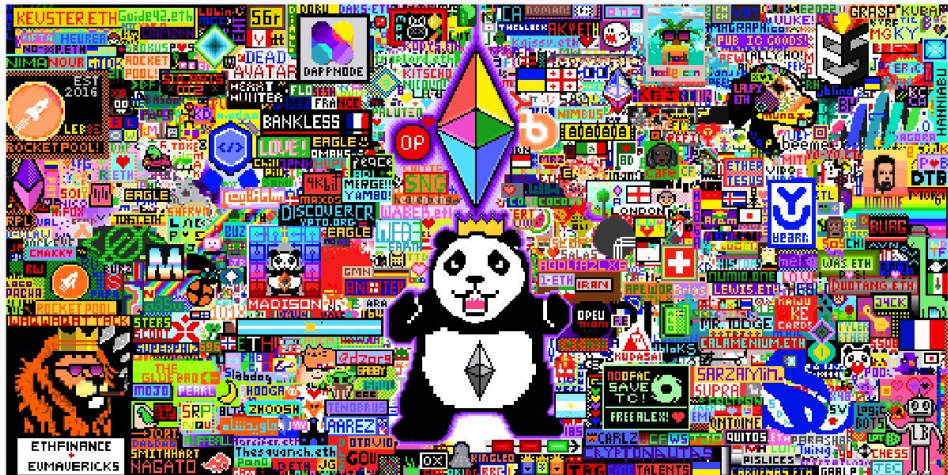
Staking design choices

- Required coins to be locked can be
 - fixed (e.g. Ethereum 2.0: 32 ETH) or
 - variable
- Delegated-proof-of-stake : allows stakeholders delegate their stake to validators.
- Some protocols want to limit the number of validators:
 - Random selection of a subcommittee
 - Delegate stake to active nodes

This talk: fixed staking, no delegation.

Ethereum switched from PoW to PoS

- The Merge - Sep 15, 2022
- Ethereum reduced electricity use by 30,000x
- World electricity consumption → ~99.8%



Blockchain : How it's built?



1. A proposer(s) is elected to announce a new block
 - a. Proof-of-Work or
 - b. Proof-of-Stake
2. Everybody decides whether to accept this block or not
 - a. Longest-chain or
 - b. BFT

Consensus
mechanism

Outline

0

Def a blockchain

1

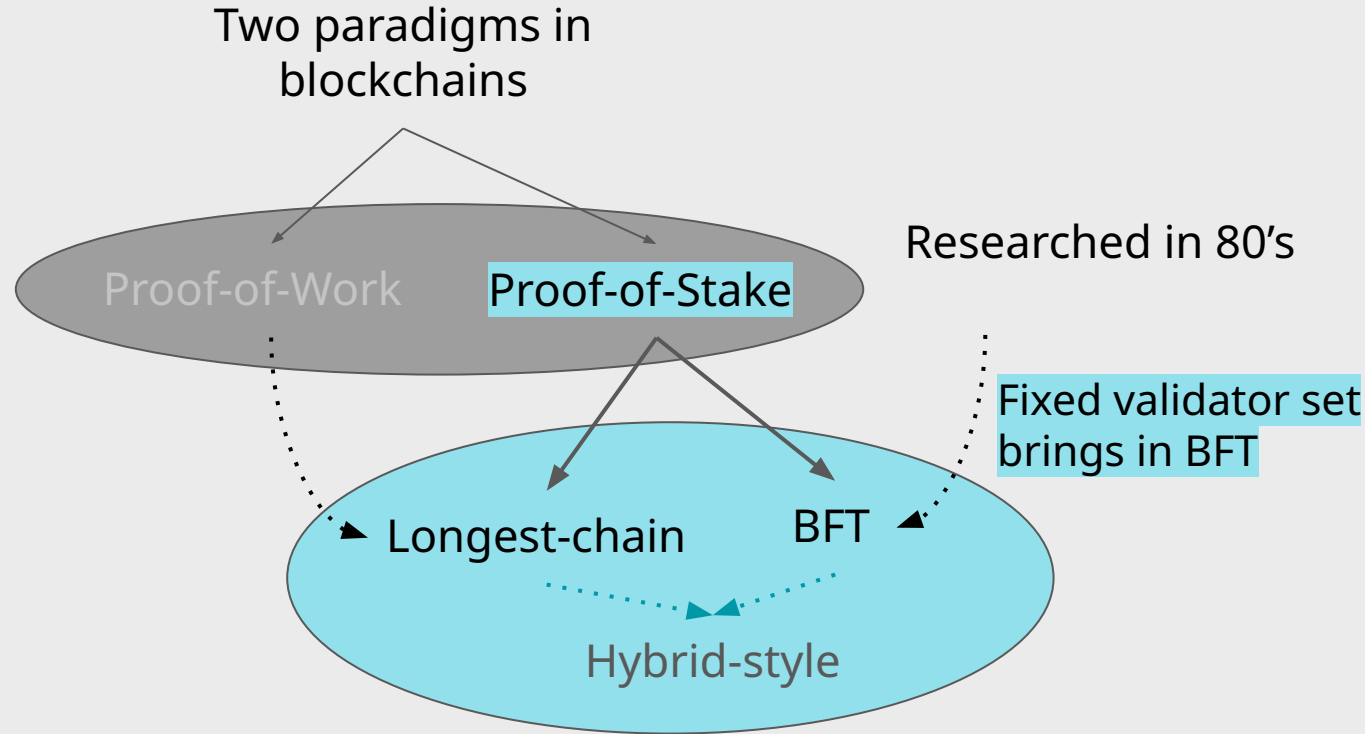
PoW vs PoS

2

Longest-chain vs BFT

3

Research



Consensus: agree on proposed block

- **Safety:** everybody agrees on history
- **Liveness:** every valid transaction eventually gets added
- Resilience against byzantine validators
- Minimal network assumption
 - **Synchronous:** shared global clock + known bound Δ on network delay
 - **Partially-synchronous:** shared global clock + exists unknown bound Δ on network delay (equivalent: synchronous after unknown GST)
 - **Asynchronous:** no bounds on network delays (subsumes network partitions)

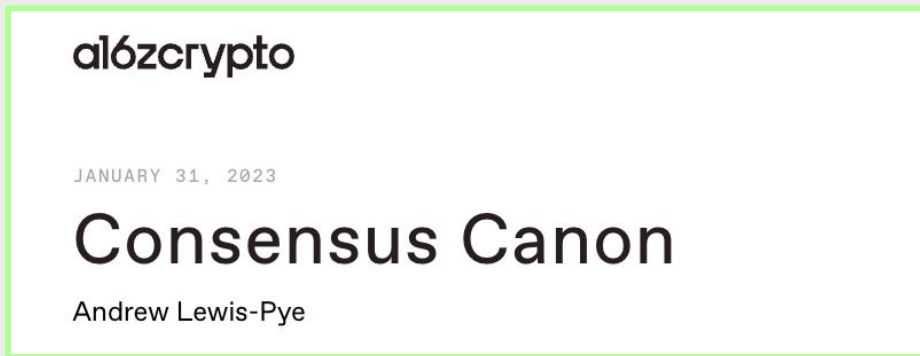
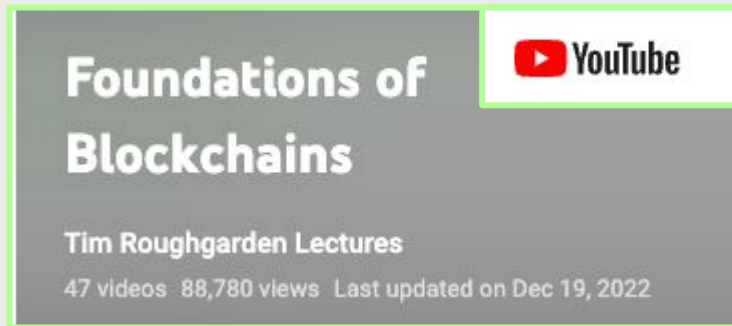
Possibility-Impossibility Results are well known for fixed validator set

	Liveness	Safety	Byzantine threshold
Synchrony	YES	YES	ANY* (<50%)
Partial-synchrony	YES	YES	< 33%
Asynchrony*	NO*	NO*	≤ 1
(Partial)-Synchrony with network partitions	YES	NO	1
	NO	YES	1

OUR FOCUS

More Resources

- [Youtube Lectures](#) by Tim Roughgarden
- Consensus cannon from a16z:
<https://a16zcrypto.com/consensus-canon/>
- Ittai Abraham:
<https://decentralizedthoughts.github.io/>

































Desired consensus properties





















- **Safety**: validators agree on history
- **Liveness**: every valid transaction eventually gets added
- Resilience against $\frac{1}{3}$ **byzantine validators**
- **Partially-synchronous**: exists unknown bound Δ on network delay
+ shared global clock

2: Longest-chain vs. BFT consensus

Blockchains by market cap : 30

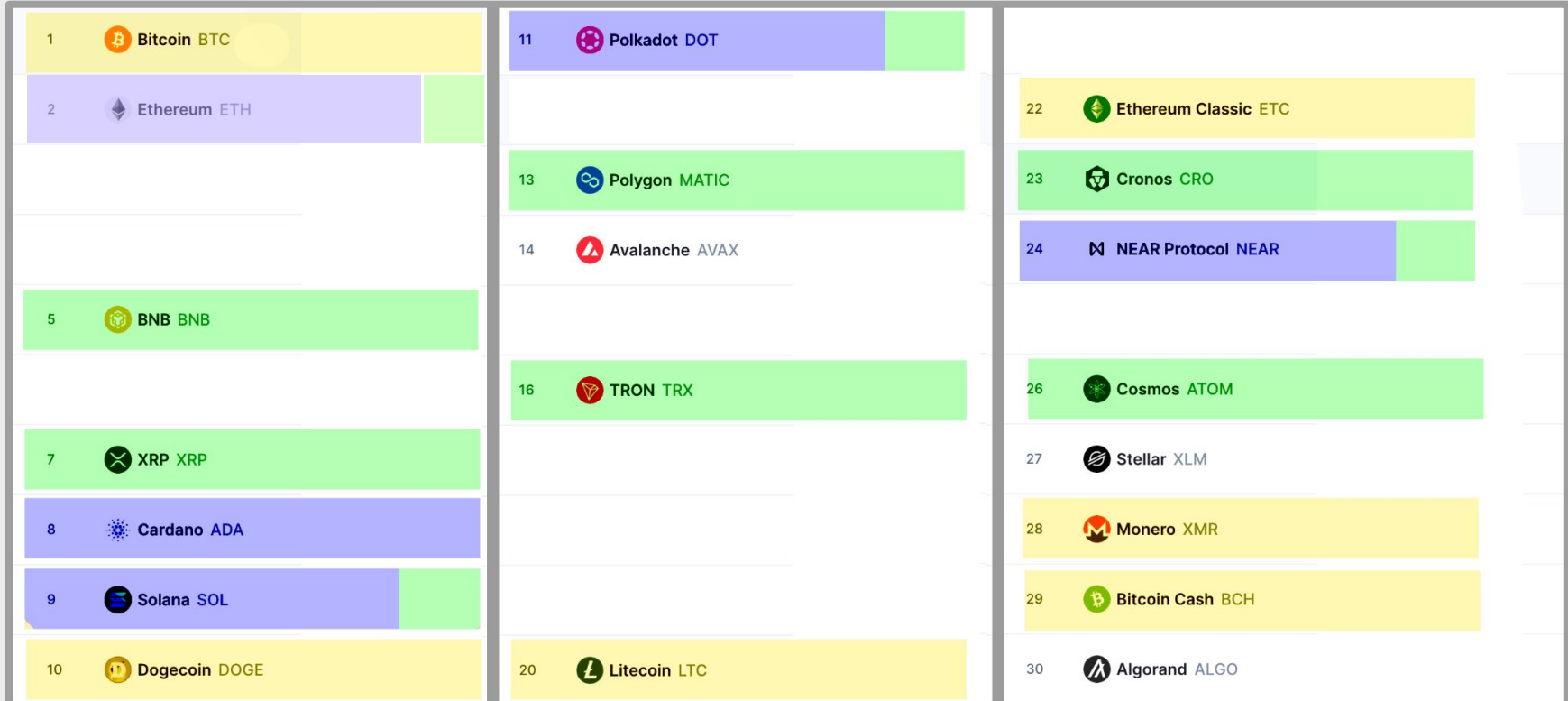
1	 Bitcoin BTC	11	 Polkadot DOT	21	 FTX Token FTT
2	 Ethereum ETH	12	 Dai DAI	22	 Ethereum Classic ETC
3	 Tether USDT	13	 Polygon MATIC	23	 Cronos CRO
4	 USD Coin USDC	14	 Avalanche AVAX	24	 NEAR Protocol NEAR
5	 BNB BNB	15	 Shiba Inu SHIB	25	 Chainlink LINK
6	 Binance USD BUSD	16	 TRON TRX	26	 Cosmos ATOM
7	 XRP XRP	17	 Wrapped Bitcoin WBTC	27	 Stellar XLM
8	 Cardano ADA	18	 Uniswap UNI	28	 Monero XMR
9	 Solana SOL	19	 UNUS SED LEO LEO	29	 Bitcoin Cash BCH
10	 Dogecoin DOGE	20	 Litecoin LTC	30	 Algorand ALGO

Blockchains by market cap : 20 non-ERC-20

1	 Bitcoin BTC	11	 Polkadot DOT	22	 Ethereum Classic ETC
2	 Ethereum ETH			23	 Cronos CRO
		13	 Polygon MATIC	24	 NEAR Protocol NEAR
		14	 Avalanche AVAX		
5	 BNB BNB			26	 Cosmos ATOM
		16	 TRON TRX	27	 Stellar XLM
7	 XRP XRP			28	 Monero XMR
8	 Cardano ADA			29	 Bitcoin Cash BCH
9	 Solana SOL			30	 Algorand ALGO
10	 Dogecoin DOGE	20	 Litecoin LTC		

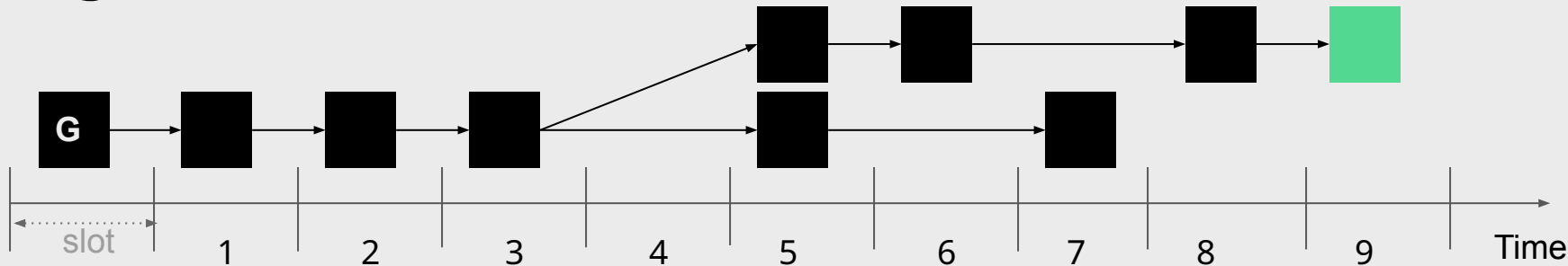
Blockchains by market cap

Longest-chain PoW ,
BFT PoS ,
Longest-chain PoS .



2: Longest-chain vs. BFT consensus

Longest-chain consensus



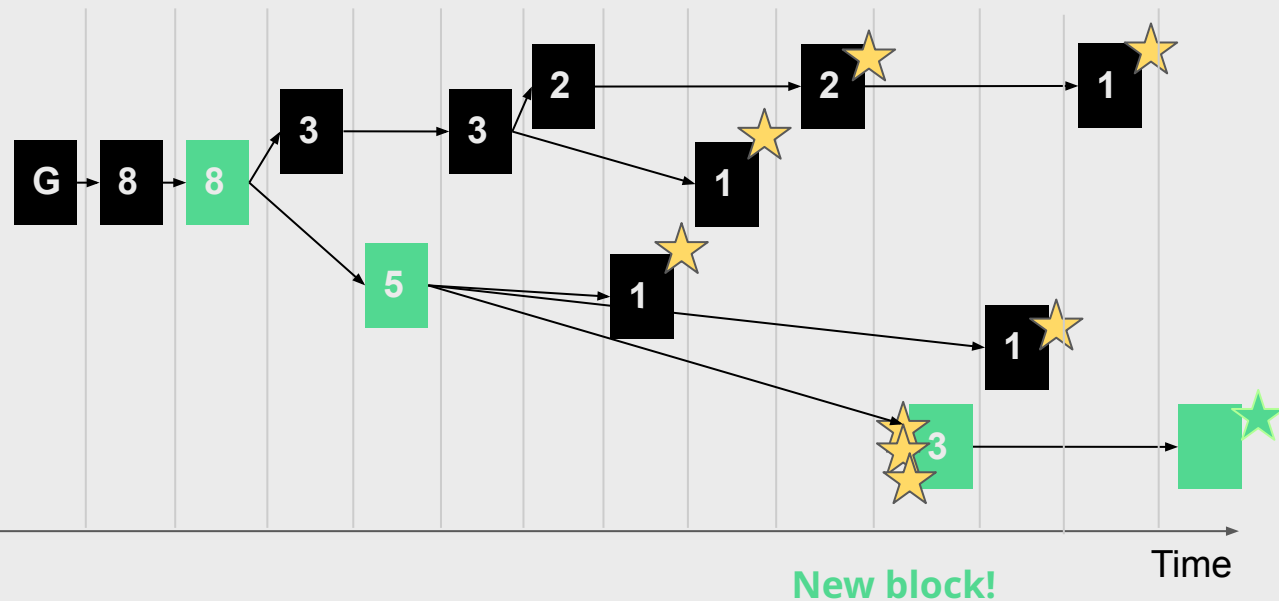
1. Each validator stores the tree of blocks.
2. Proposer is elected per slot from the validator set (can have multiple proposers).
3. Proposer picks a chain to extend according to “fork-choice rule”.
4. Creates a block on top, publishes it to the network.

Fork-choice rules: usually greedy, e.g. longest (more blocks in it)

Parameters are tuned so that with high probability only one chain **eventually** wins.

Ethereum's fork-choice rule “LMD GHOST”:

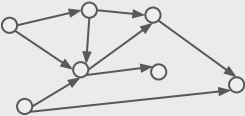
grows the blockchain on sub-branches with the “most activity”.



LMD GHOST:

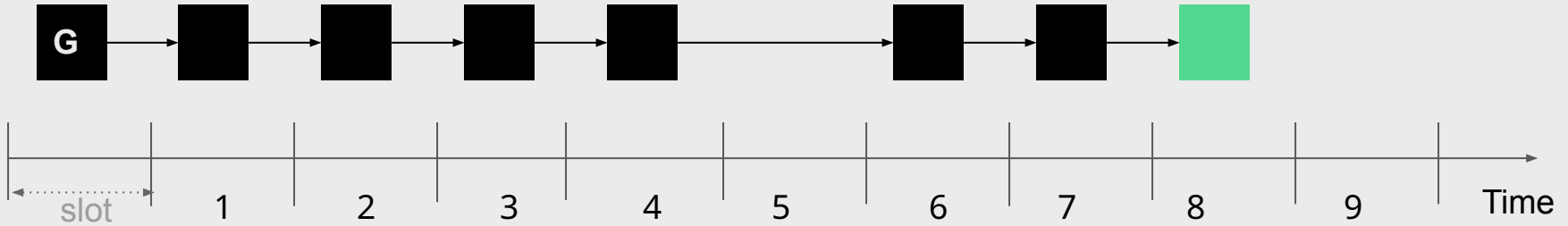
- One leader is selected per slot to propose a block.
- Each validator votes once in an epoch (32 slots) at its designated slot.
- Latest vote ★ per validator is counted.
- The number on each block is the number of validators' votes on the subtree.
- The greedy algorithms walk the tree choosing the “heaviest” blocks.

Most popular PoS approaches

	Longest-chain consensus
Examples:	Ethereum,Peercoin,Ouroboros
Finality:	Eventual = Probabilistic
Safety under partition:	NO
Liveness under partition:	YES
#validators:	unlimited
Typical network topologies:	Flexible: 

2: Longest-chain vs. BFT consensus

BFT-consensus

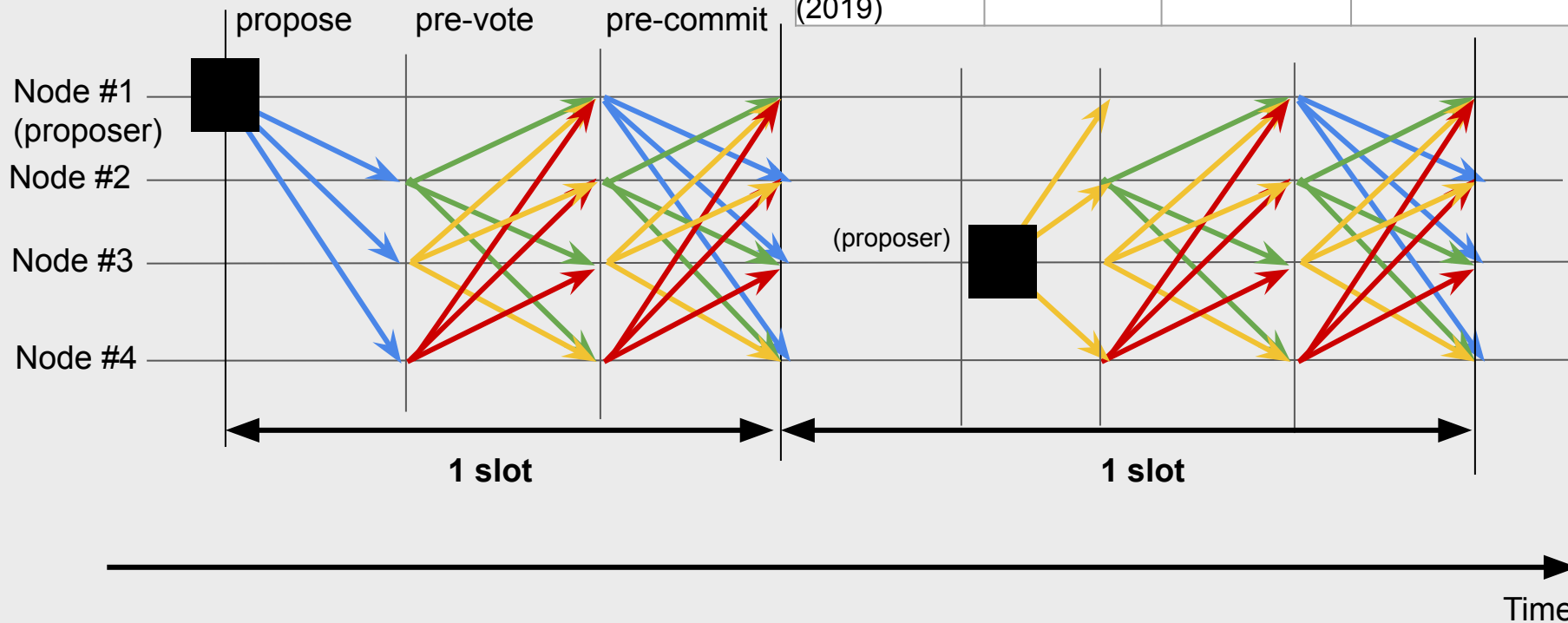


Each slot:

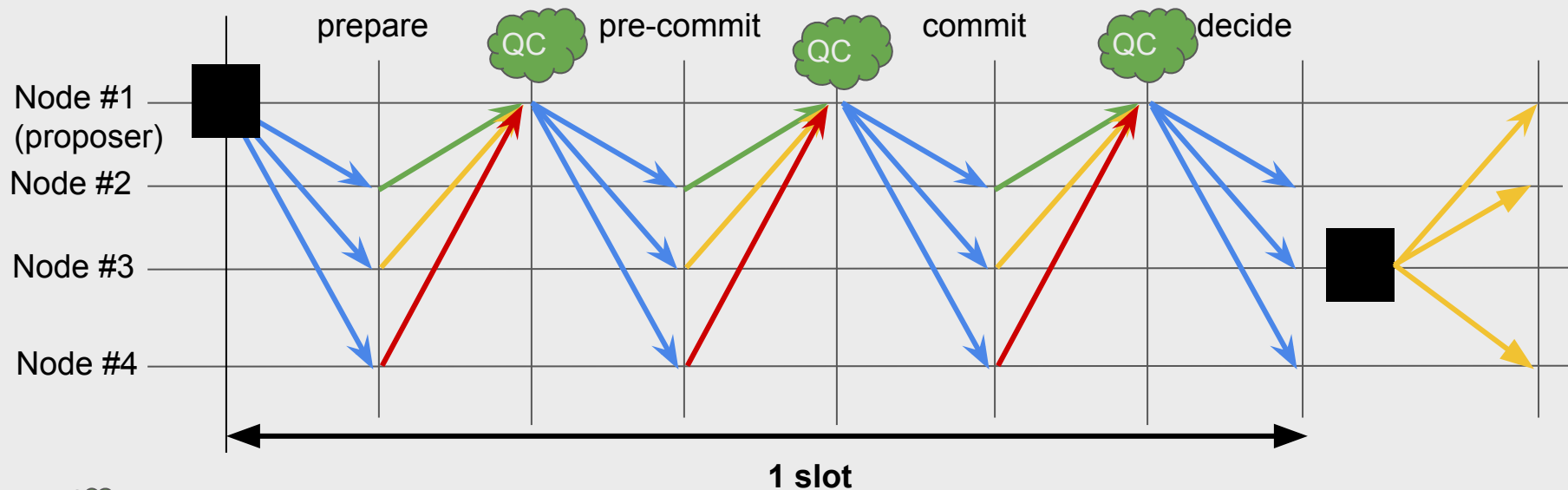
1. A proposer is elected from the validator set.
2. The proposer proposes a new block.
3. Validators work on finalizing the block, it either gets finalized or not.


Tendermint BFT (2016)

	Correct proposer	Proposer failure	Responsiveness
Tendermint (2016)	$O(n^2)$	$O(n^2) / O(n)$	✗
HotStuff (2019)	$O(n)$	$O(n)$	✓



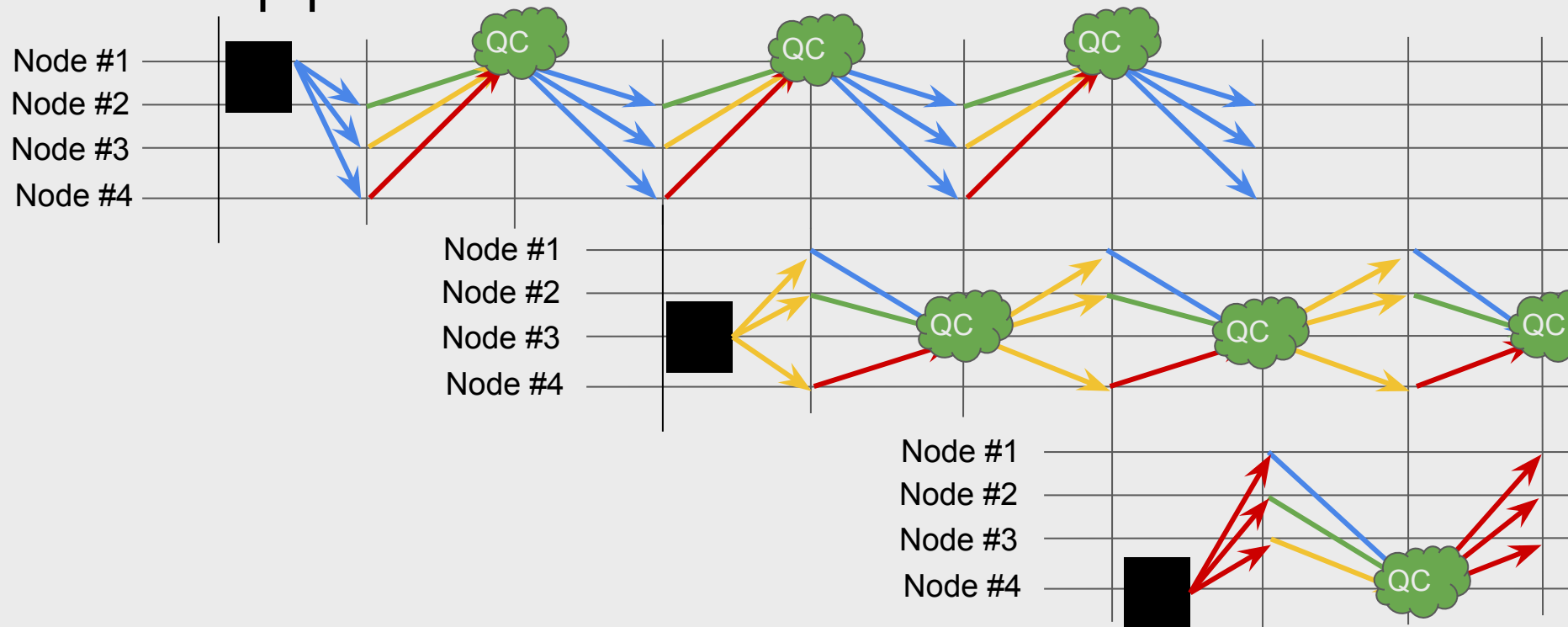
Hotstuff: rerouting through the proposer and use aggregatable signatures



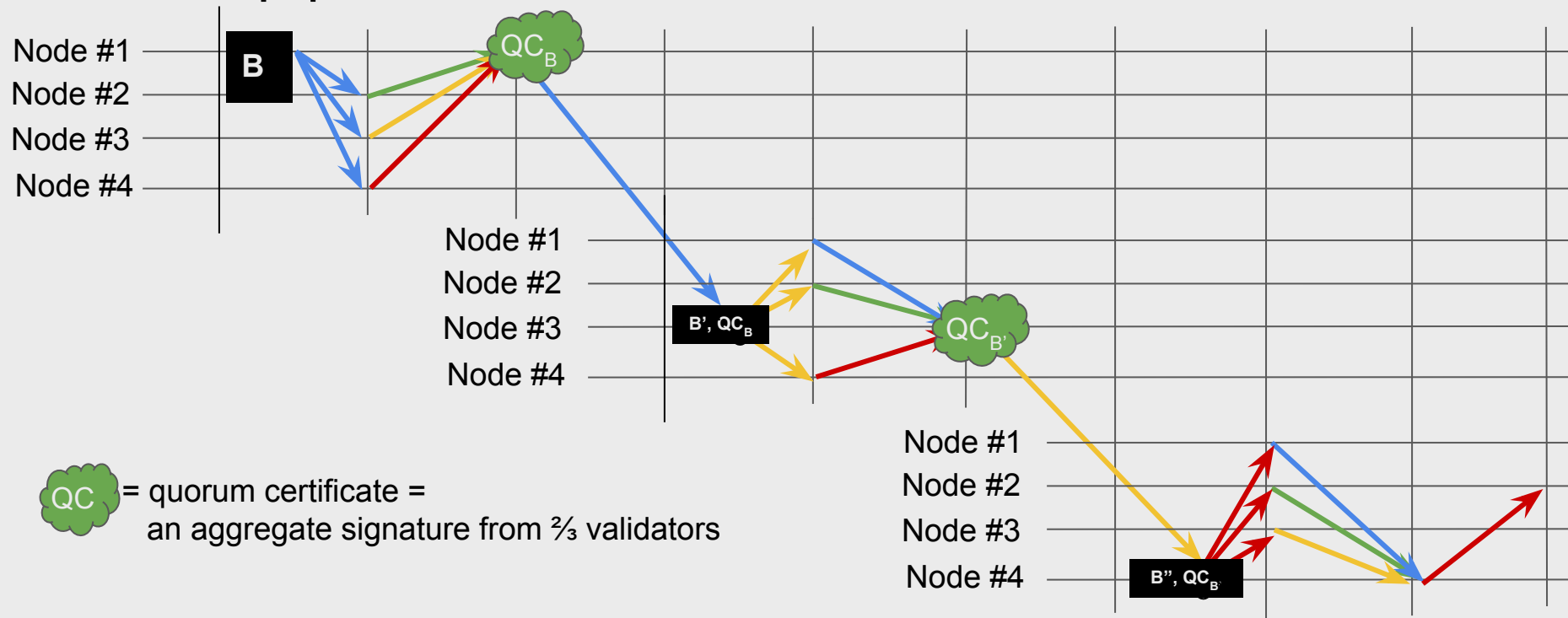
 = quorum certificate =
an aggregate signature from $\frac{2}{3}$ validators

Time

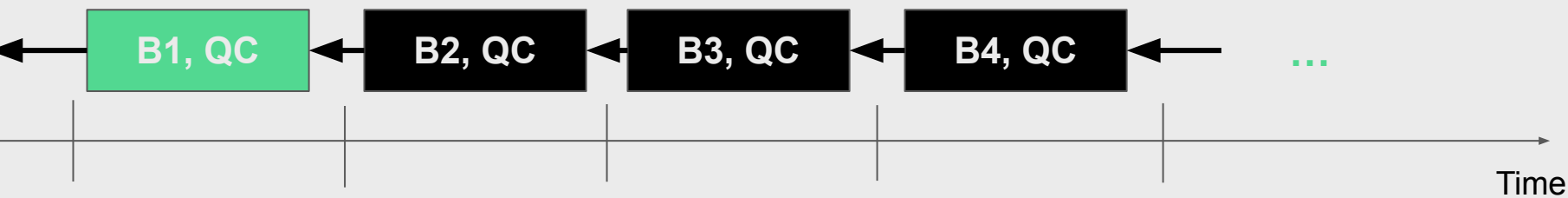
Hotstuff pipelined



Hotstuff pipelined



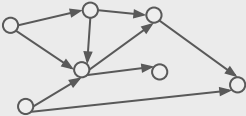
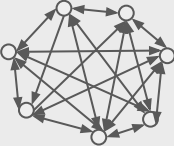
HotStuff: 3-chain commit rule



Hotstuff: B_1 is committed after there are three blocks with QCs on top of it.

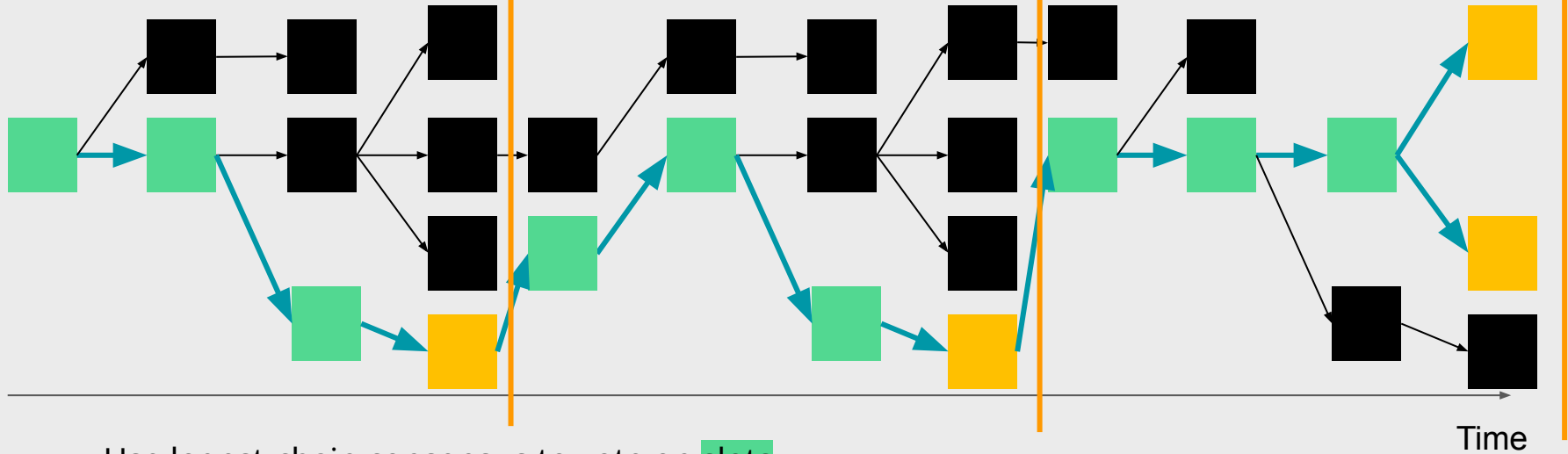
<https://malkhi.com/posts/2019/08/hotstuff-three-chain-rules/>

Most popular PoS approaches

	Longest-chain consensus	BFT consensus
Examples:	Peercoin, Ouroboros-*	Tendermint, Hotstuff
Finality:	Eventual = Probabilistic	Deterministic Immediate
Safety under partition:	NO	YES
Liveness under partition:	YES	NO
#validators:	unlimited	4-100 <small>slower with more validators</small>
Typical network topologies:	Flexible: 	Complete: 

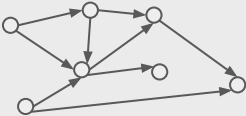
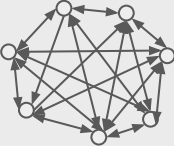

3: Hybrid consensus: Longest-chain + BFT

Hybrid-consensus / finality gadgets



- Use logest-chain consensus to vote on slots
- Use BFT consensus to vote on epochs
- Epoch is a fixed number of slots
 - Ethereum: 32 slots per epoch, 12 second per slot, 6.4 min per epoch
- Typically: 2-stage BFT voting, hence 2 epochs to finality

Most popular PoS approaches

	Longest-chain consensus	BFT consensus	Hybrid
Examples:	Peercoin, Ouroboros-*	Tendermint, Hotstuff	
Finality:	Eventual = Probabilistic	Deterministic Immediate	Deterministic Slow
Safety under partition:	NO	YES	YES
Liveness under partition:	YES	NO	TEMPORAL LOSS
#validators:	unlimited	4-100 <small>slower with more validators</small>	unlimited
Typical network topologies:	Flexible: 	Complete: 	Flexible: 

Algorand : multiple leaders per slot

- No locked tokens, **no slashing**. A user registers a participation key for a certain number of rounds.
- Each node runs a VRF privately twice:
 - to determine whether it is elected as a leader, and
 - to determine whether it is elected in a committee (new committee is selected for every step).
- There could be multiple leaders per round
- Similar to longest-chain: the lowest block (by hash) is propagated.
- Committee then votes twice on the block (in BFT-style).
- Forward-secure: nodes discard old keys disabling attacks on the past.
- Network-partition-resilient: halts during the partition, resumes when the network is restored.

2: Longest-chain vs. BFT consensus more...

Avalanche : leaderless consensus

- Snowball/Snowman leaderless consensus protocol!
- UTXO model, thus txs form a DAG.
- Establishes a partial order.
- Each node accepts a valid transaction tx_1 and sends it to other nodes, until it sees a conflicting transaction, tx_2 . If it hears about tx_2 from a $>$ threshold of peers, it switches tx_1 to tx_2 and sends that to its peers.
- Finality: probabilistic

Disclosures

The views expressed here are those of the individual AH Capital Management, L.L.C. (“a16z”) personnel quoted and are not the views of a16z or its affiliates. Certain information contained in here has been obtained from third-party sources, including from portfolio companies of funds managed by a16z. While taken from sources believed to be reliable, a16z has not independently verified such information and makes no representations about the current or enduring accuracy of the information or its appropriateness for a given situation. In addition, this content may include third-party advertisements; a16z has not reviewed such advertisements and does not endorse any advertising content contained therein. This content is provided for informational purposes only, and should not be relied upon as legal, business, investment, or tax advice. You should consult your own advisers as to those matters. References to any securities or digital assets are for illustrative purposes only, and do not constitute an investment recommendation or offer to provide investment advisory services. Furthermore, this content is not directed at nor intended for use by any investors or prospective investors, and may not under any circumstances be relied upon when making a decision to invest in any fund managed by a16z. (An offering to invest in an a16z fund will be made only by the private placement memorandum, subscription agreement, and other relevant documentation of any such fund and should be read in their entirety.) Any investments or portfolio companies mentioned, referred to, or described are not representative of all investments in vehicles managed by a16z, and there can be no assurance that the investments will be profitable or that other investments made in the future will have similar characteristics or results. A list of investments made by funds managed by Andreessen Horowitz (excluding investments for which the issuer has not provided permission for a16z to disclose publicly as well as unannounced investments in publicly traded digital assets) is available at <https://a16z.com/investments/>. Charts and graphs provided within are for informational purposes solely and should not be relied upon when making any investment decision. Past performance is not indicative of future results. The content speaks only as of the date indicated. Any projections, estimates, forecasts, targets, prospects, and/or opinions expressed in these materials are subject to change without notice and may differ or be contrary to opinions expressed by others. Please see <https://a16z.com/disclosures> for additional important information.



Thank you!

