Part V: Cryptocurrency Fundamentals: Forks

Main Chain

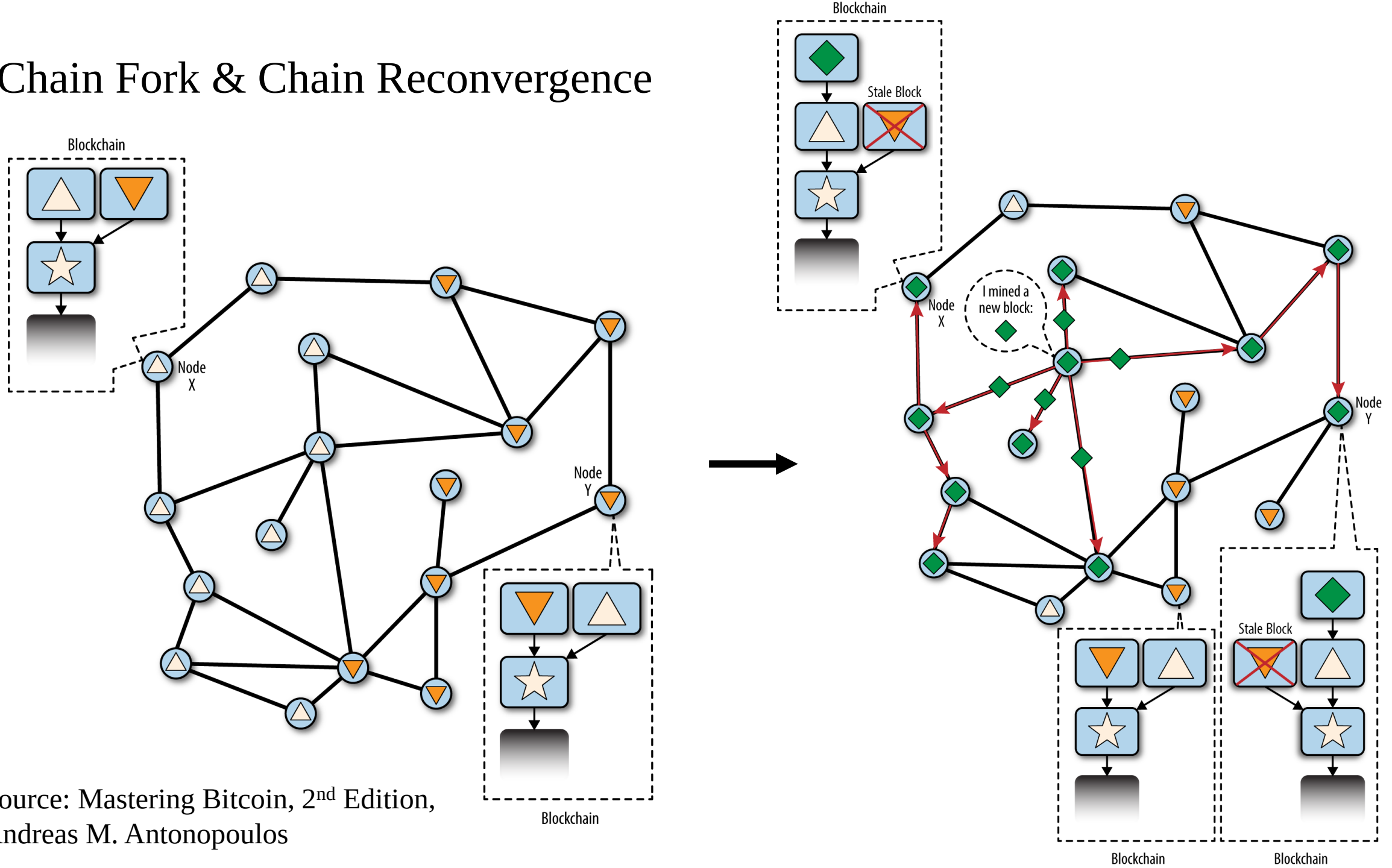
- What is the main chain?

Main chain is the valid chain of block that has the most blocks in it.

If there are two chains with the same amount of blocks, then the chain with more Proof-of-Work is the main chain.

Miners “vote” with their mining power by choosing which chain to extend.

Chain Fork & Chain Reconvergence



Source: Mastering Bitcoin, 2nd Edition, Andreas M. Antonopoulos

Bitcoin Improvement Proposals (BIPs)

- *"A BIP is a design document providing information to the Bitcoin community, or describing a new feature for Bitcoin or its processes or environment. The BIP should provide a concise technical specification of the feature and a rationale for the feature"*. – BIP website

- BIP website: https://github.com/bitcoin/bips

- Why BIPs?

We need a governance process to follow to update the bitcoin protocol. BIPs are the bitcoin community's process to update the bitcoin core code.

How do BIPs work?

- If you have an improvement idea, and this idea has never been proposed and rejected before, submit your idea to Bitcoin development mailing list.

- Once the BIP author (champion) has asked the Bitcoin community as to whether an idea has any chance of acceptance, a draft BIP should be presented to the Bitcoin development mailing list.

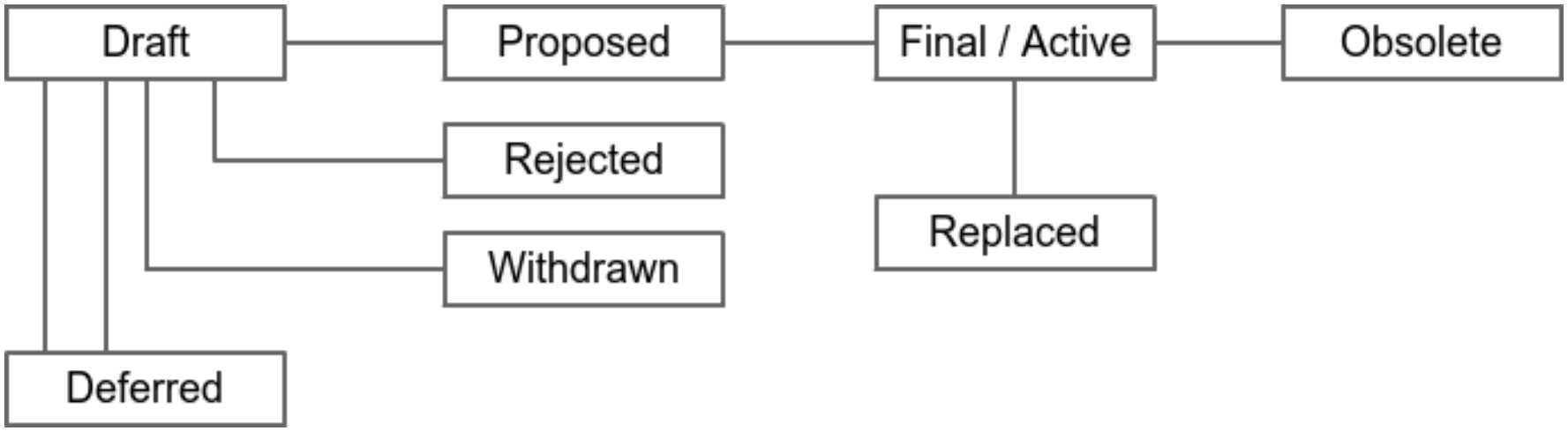
- If the BIP editor approves, he will assign the BIP a number.

- If miners signal support for this BIP, the status will be changed to "Final". It is the miners who have the final say, because they are the ones who have to upgrade their software eventually.

More on BIPs

- Your BIP should follow the correct format
- BIP should include code that implements the change
- A BIP is deemed as accepted after a certain support threshold is reached. There is no hard numbers for this threshold, but 95% support rate is recommended.
- Anyone can proposal a new BIP
- Miners are the voters, more computing power means more votes

BIP process



Deferred: when no progress is being made on the BIP

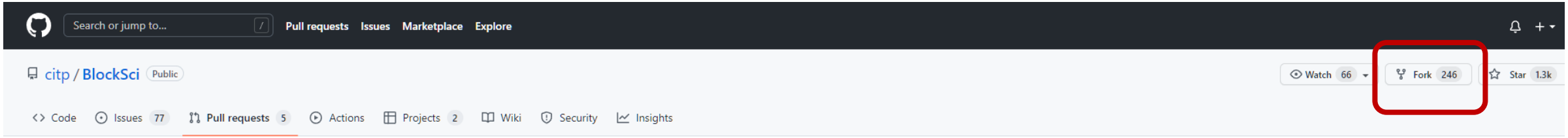
Replaced/Obsolete: when a Final BIP is no longer relevant, its status may be changed to Replaced or Obsolete

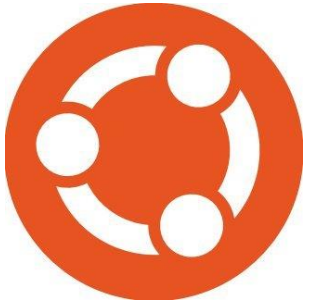
Source: BIP-0002

Forks

- Fork

"In software engineering, a project fork happens when developers take a copy of source code from one software package and start independent development on it, creating a distinct and separate piece of software." – Wikipedia





Forks in Bitcoin Network

- Soft Fork

A soft fork is an upgrade to mining software that does not require all miners participate. The upgrade should be backwards compatible. How to implement a soft fork is documented in BIP9.

- Hark Fork

A hard fork is an upgrade to mining software that require the participation of all miners. The upgrade is not backwards compatible.

- Contentious Hard Fork

A hard fork when there is a disagreement within the bitcoin community.

“Final” criteria for different BIPs

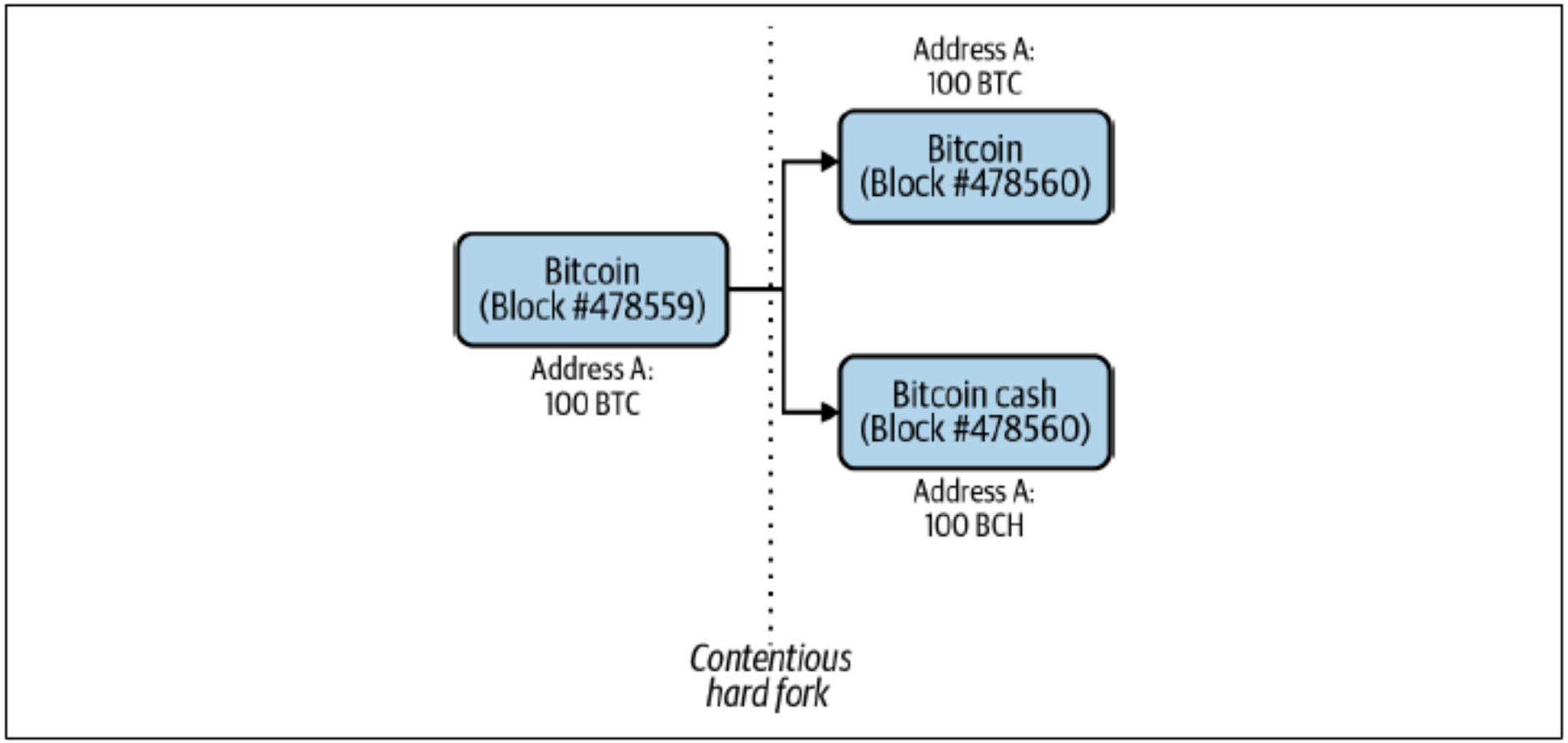
- A soft-fork BIP strictly requires a clear miner majority support expressed by blockchain voting. A supermajority approval rate around 95% is recommended, unless rationale is given for a lower threshold.

- A hard-fork BIP requires adoption from the entire Bitcoin economy. Adoption must be expressed by de facto usage of the hard-fork in practice.

- Criteria for other kinds of BIPs, see BIP0002

Effects of Contentious Hard Forks

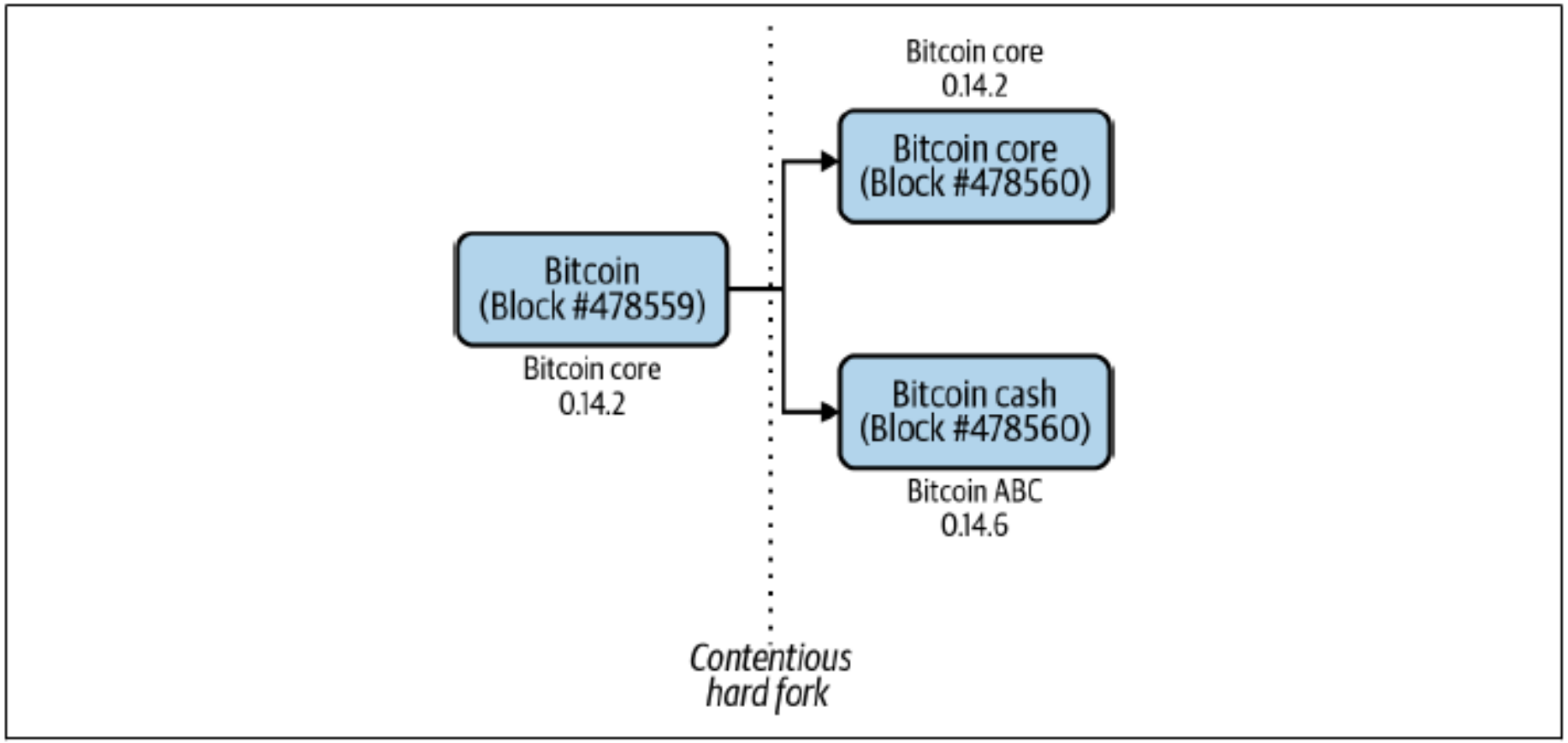
- Users



Source: Mastering Blockchain, Lorne Lantz & Daniel Cawrey

Effects of Contentious Hard Forks

- Miners



Source: Mastering Blockchain, Lorne Lantz & Daniel Cawrey

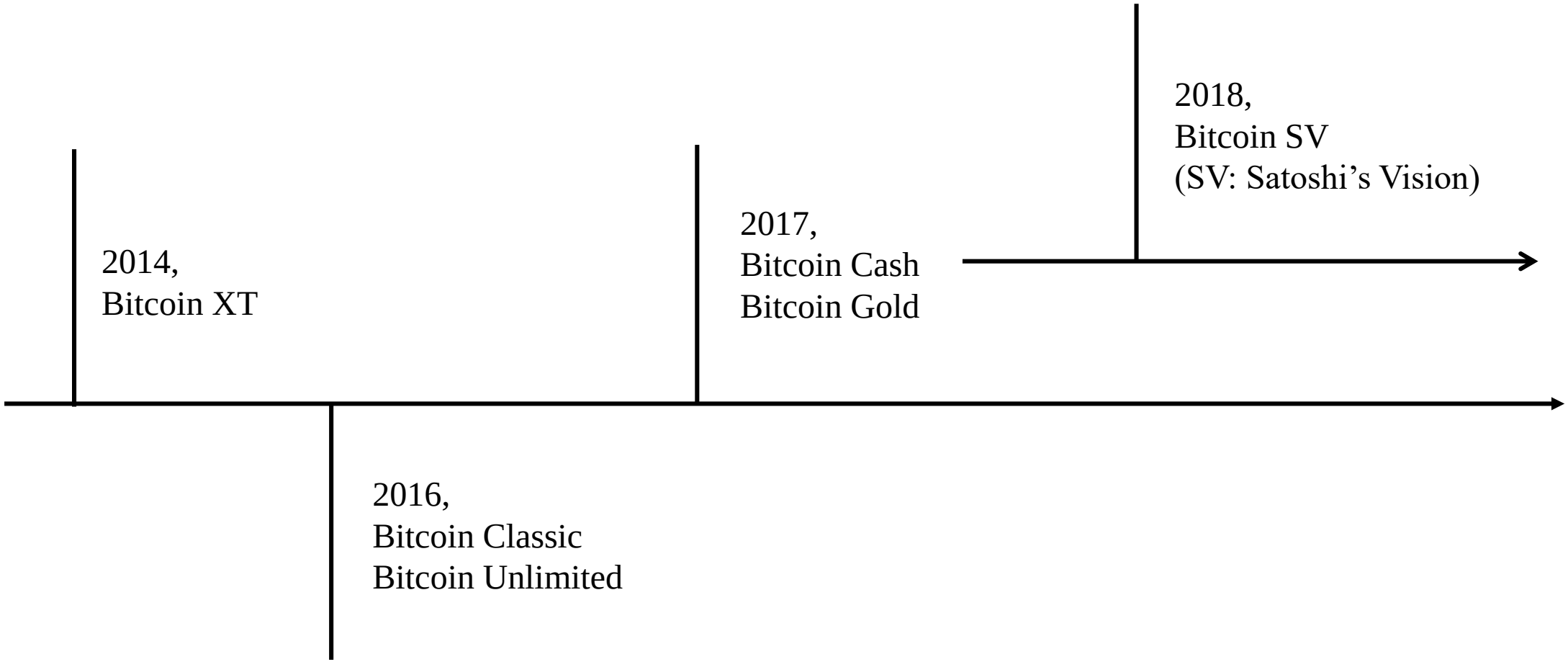
Bitcoin Scaling Issue

- Bitcoin block size is restricted to 1 MB, and each block can at most contain around 2000 transactions. The transaction confirmation speed is inadequate for processing daily transactions.

- Solution 1: increase the block size
- Solution 2: remove some of the data out of blockchain and stored it in external files

- The majority of contentious hard forks are enacted because people want to choose different solutions.

A History of Bitcoin Hard Forks



Source: Investopedia, Wikipedia

Bitcoin XT

In Jun 2014, Mike Hearn proposed BIP64, which is "*a small P2P protocol extension that performs UTXO lookups given a set of outpoints",* and created Bitcoin XT.

In Aug. 2015, BIP101 proposed by Gavin Andresen is implemented in Bitcoin XT. The main goal of BIP 101 is to increase the block size from 1 MB to 8 MB, and double the block size every two years. This is a controversial proposal and it failed eventually.

In Jan. 2016, BIP 101 was removed from Bitcoin XT and replaced with a one-time block size increase to 2 MB (BIP109). However, Bitcoin XT has lost popularity.

Bitcoin Classic

- In Jan. 2016, Gavin Andresen proposed to increase the block size to 2MB in BIP109. Then the project Bitcoin Classic is initialized.

- Bitcoin Classic has received support from some Bitcoin companies, developers, investors and miners. However, the wider bitcoin community did not think a hard fork is justified.

- The software's peak use was observed in early 2016 with a steady decline in usage from March 2016 onwards.

Bitcoin Unlimited

- https://www.bitcoinunlimited.info

- This project is not associated with a famous developer, it arose from a single thread on Bitcoin Talk known as "Gold Collapsing Bitcoin Up“.

- This project is inspired by BIP100, which suggests to *“replace the static base block size hard limit with a hard limit set by Coinbase vote, conducted on the same schedule as difficulty retargeting.”*

Bitcoin Cash

- https://bitcoincash.org

- Bitcoin Cash was launched by the Chinese mining pool ViaBTC.

- The Bitcoin Cash hard fork took place on August 1, 2017, after block 478558

- Bitcoin Cash increased the block size to 8 MB, then further increased it to 32 MB in May 2018.

- Why do we care about block size?

Bitcoin Gold

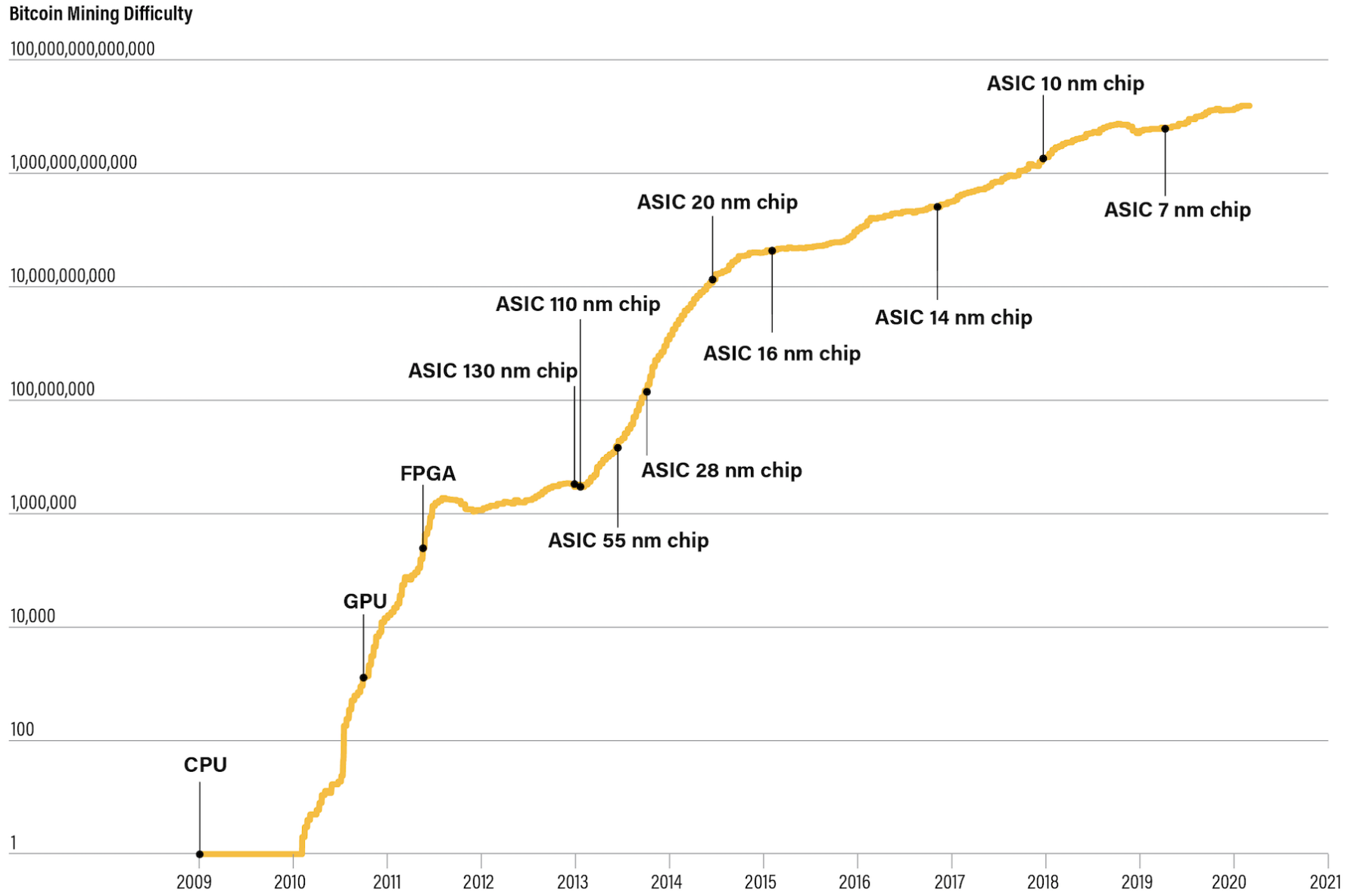
- https://bitcoingold.org

- The Bitcoin Gold fork from the original Bitcoin blockchain took place on October 24, 2017 at block height 491407.

- Bitcoin Gold modified the mining algorithm (Equihash, a memory-hard Proof-of-Work algorithm) to make it ASIC-resistant.

- Why do we care about being ASIC-resistant?

Bitcoin Mining Equipment Evolution



Source: CoinDesk

Altcoins

Altcoin is used to referee to all cryptocurrencies except bitcoin. Some famous altcoins are:

- Ether

Ether is the coin used on Ethereum platform, it the second largest cryptocurrency in the world.

- Litecoin

One of the first altcoins, released in 2011. The block time was set to be four times faster than bitcoin’s. The algorithm is ASIC-resistant.

- Dogecoin

Released in 2013, dogecoin was originally created out of a joke, and it got popularized by Elon Musk in 2021.

Segregated Witness (SegWit) & SegWit2X

- SegWit and SegWit2X together are a two-stage process known as the "New York Agreement“.

- SegWit is a soft-fork that focus on removing part of data out of blockchain

- SegWit2X is a hard-fork that focus on increasing the block size, it never got implemented.

Soft Fork: Segregated Witness (SegWit)

- Defined by BIP141, BIP143, BIP144, and BIP145, SegWit is an upgrade to the bitcoin consensus rules and network protocol.

- “Witness” means a solution that satisfies a cryptographic condition imposed on an UTXO, for example, the signature generated by the corresponding private key is one type of witness.

- SegWit means separating the signature or unlocking script from the on-chain data.

SegWit

Transaction input w/o SegWit

```
[...]
“Vin” : [
"txid": "0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2",
"vout": 0,
       "scriptSig": “<Bob’s scriptSig>”,
]
[...]
```

Transaction input with SegWit

```
[...]
“Vin” : [
"txid": "0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2",
"vout": 0,
       "scriptSig": “”,
]
[...]
“witness”: “<Bob’s witness data>”
[...]
```

Multi-sig transaction input w/o SegWit

```
[...]
“Vin” : [
"txid": "abcdef12345...",
"vout": 0,
       "scriptSig": “<SigA> <SigB> <2 PubA PubB PubC PubD PubE 5 CHECKMULTI-
SIG>”,
]
```

Multi-sig transaction input with SegWit

```
[...]
“Vin” : [
"txid": "abcdef12345...",
"vout": 0,
       "scriptSig": “”,
]
[...]
“witness”: “<SigA> <SigB> <2 PubA PubB PubC PubD PubE 5 CHECKMULTISIG>”
[...]
```

Why SegWit?

- Network and Storage Scaling

The witness data is usually a large portion of a transaction. Removing the witness data outside the transaction can improve bitcoin’s scalability.

- Transaction Malleability

Without including the witness data, transaction hash becomes immutable, which can prevent malleability attacks.

- Signature Verification Optimization
- Offline Signing Improvement
- Script Versioning

Soft Fork: Taproot

- Taproot is proposed in BIP341 in Jan. 2021, and got implemented in Nov. 2021.

- Use Schnorr Signature to simplify the signature verification process in multi-sig transactions.

- Make single-sig transactions and multi-sig transactions indistinguishable.

Part VI: Cryptocurrency Fundamentals: Consensus

Byzantine Generals Problem

Suppose a group of generals have besieged a city and they have to agree on either attaching or retreating. Generals can only communicate through messages, then they have a communication problem:

(1) Messages can get delayed, destroyed or lost

(2) One or more generals may act maliciously and send out fraudulent messages.

Think of these generals as nodes in the blockchain system, then we still need to solve this Byzantine Generals Problem in nowadays.

Byzantine Fault Tolerance

- Byzantine Fault Tolerance is a system's ability to continue operating even if some of its nodes fail or act maliciously.

- The consensus algorithm is how a blockchain achieves Byzantine Fault Tolerance.

- Byzantine Fault Tolerance Intro

Consensus Algorithm

Consensus: a voting protocol for making decisions.

- Proof-based consensus

Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), etc.

- Voting-based consensus

Practical Byzantine Fault Tolerance

Proof-of-Work

- Allocate the validation rights through the hashing power competition
- PoW takes the workload as the safeguard.
- PoW is susceptible to 51% attack.
- PoW wastes a lot of computing power and natural resources.

Consensus Attack -- Proof of Work

- 51% Attack

If one entity controls a majority (51%) of the total network's hashing power, it has the ability to invalidate confirmed blocks and double-spend its own transactions.

Solution: wait longer to confirm your transaction

- Deny Service Attack

An attacker with a majority of the mining power can simply ignore specific transactions, for example transactions that involve a certain address.

Proof-of-Stake

PoS algorithms use several methods to select who will validate the next block:

(1) The size of the stake

The more tokens staked, the higher the chance of being chosen to validate.

(2) The age of the tokens staked

The longer the tokens have been unspent, the higher the chance of being chosen to validate. Once that stake is used to verify a block, its age is reset to zero.

(3) Random Selection

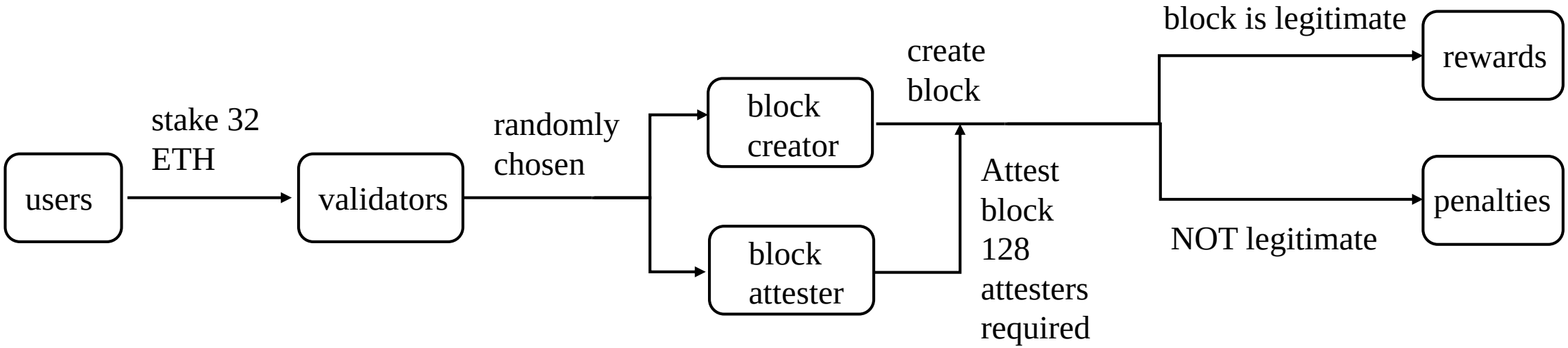
Proof-of-Stake in Ethereum 2.0

- Shard chain: mainly addresses the scalability concern. There are 64 shard chains in the Ethereum network.

- Beacon chain: coordinates the information between different shard chains and manages validators.

- Validator: the nodes in the Ethereum network who want to confirm transactions. Users need to stake 32 ETH to become validators.

Proof-of-Stake in Ethereum 2.0



Resource: [Ethereum Whitepaper]

Proof-of-Stake in Ethereum 2.0

(1) Pros

- Better energy efficiency
- Lower barriers to entry (hardware requirement is low)
- Stronger immunity to centralization

(2) Cons

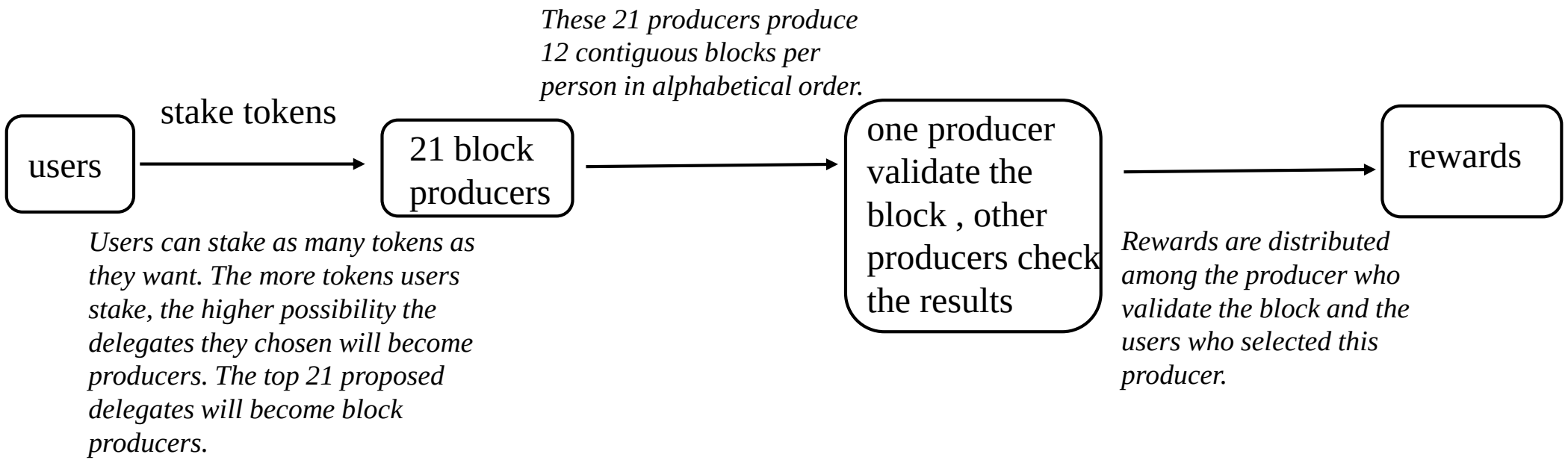
Compared with Proof-of-Work, Proof-of-Stake is less battle-tested in the real world.

Q: Does 51% attack still exist in proof-of-stake?

Delegated Proof of Stake

- In DPoS, users do not directly become validators, they vote for delegates to become validators.
- Users vote on delegates by pooling their tokens into a staking pool and linking those tokens to a particular delegate.
- These delegates are usually called as witnesses or block producers.

Delegated Proof of Stake in EOS



Resource: [EOS Whitepaper]

Practical Byzantine Fault Tolerance

- The client sends a request to the primary(leader) node.
- The primary(leader) node broadcasts the request to the all the secondary(backup) nodes.
- The nodes(primary and secondaries) perform the service requested and then send back a reply to the client.
- The request is served successfully when the client receives ‘m+1’ replies from different nodes in the network with the same result, where m is the maximum number of faulty nodes allowed.

Proof-based or Voting-based consensus?

- Proof-based consensuses are widely used in **permissionless** networks. There is no control on the nodes. Nodes can join or leave the network as their wish.

- Voting-based consensuses are usually used in **permissioned** networks. In a permissioned network, all the nodes are identified, and the designer knows how many validators at most can be compromised.

- Proof-based consensuses are less efficient than voting-based consensuses.

Bitcoin Transaction Data

You can access the whole history of bitcoin transactions by hosting a bitcoin full node.

....or, you can rely on third-party services.

(1) blockchain.com

(2) cryptocompare.com

(3) Google Cloud