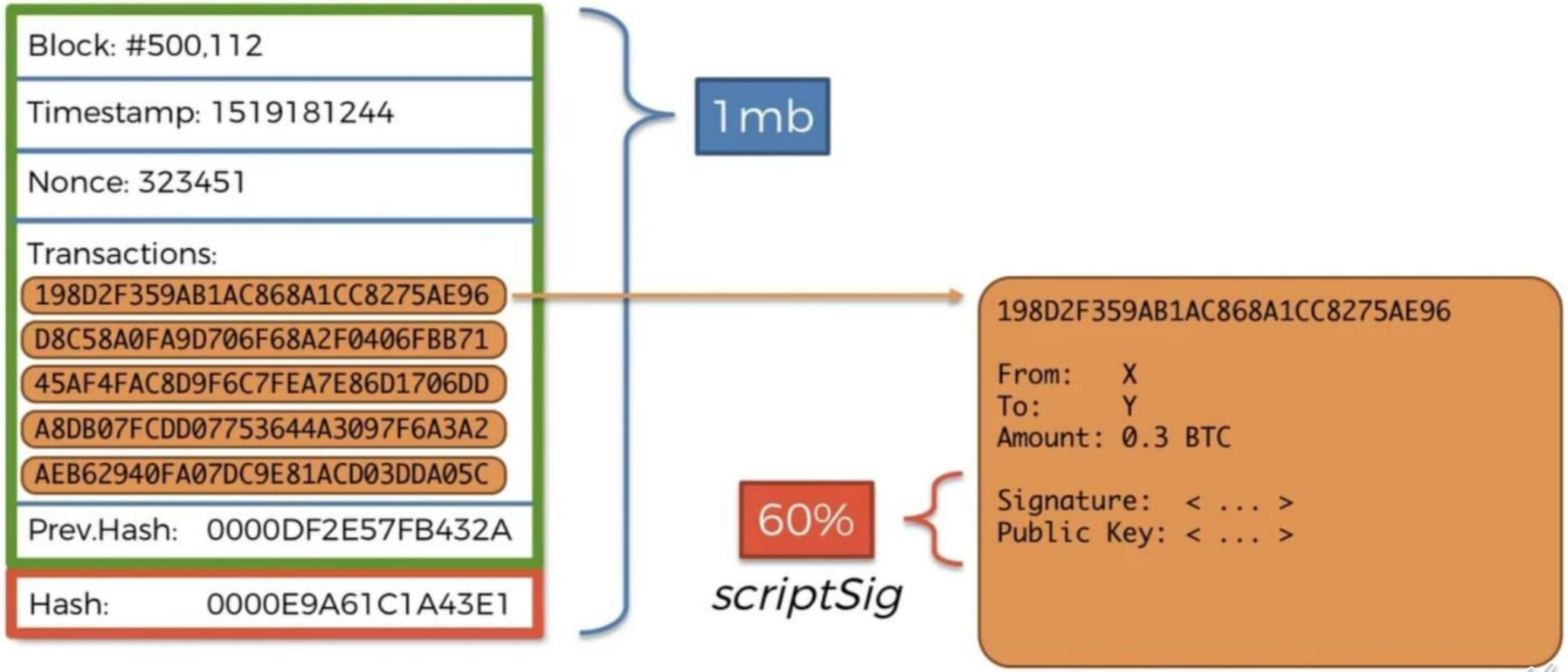
Blockchain and Cryptocurrency

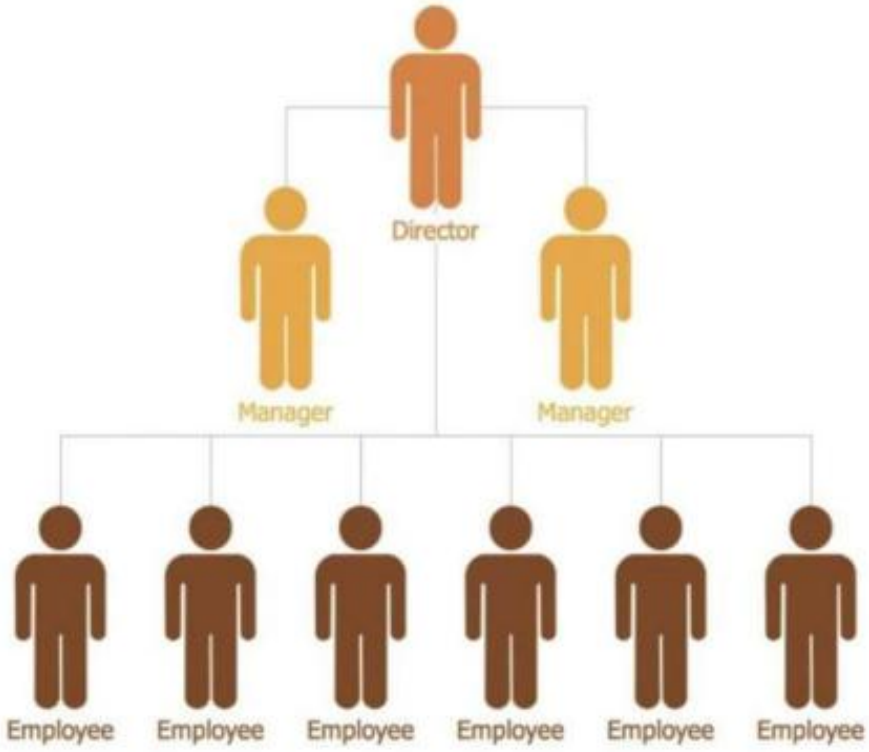
By: Syeda Tayyaba Bukhari

Segregated Witness (SegWit)

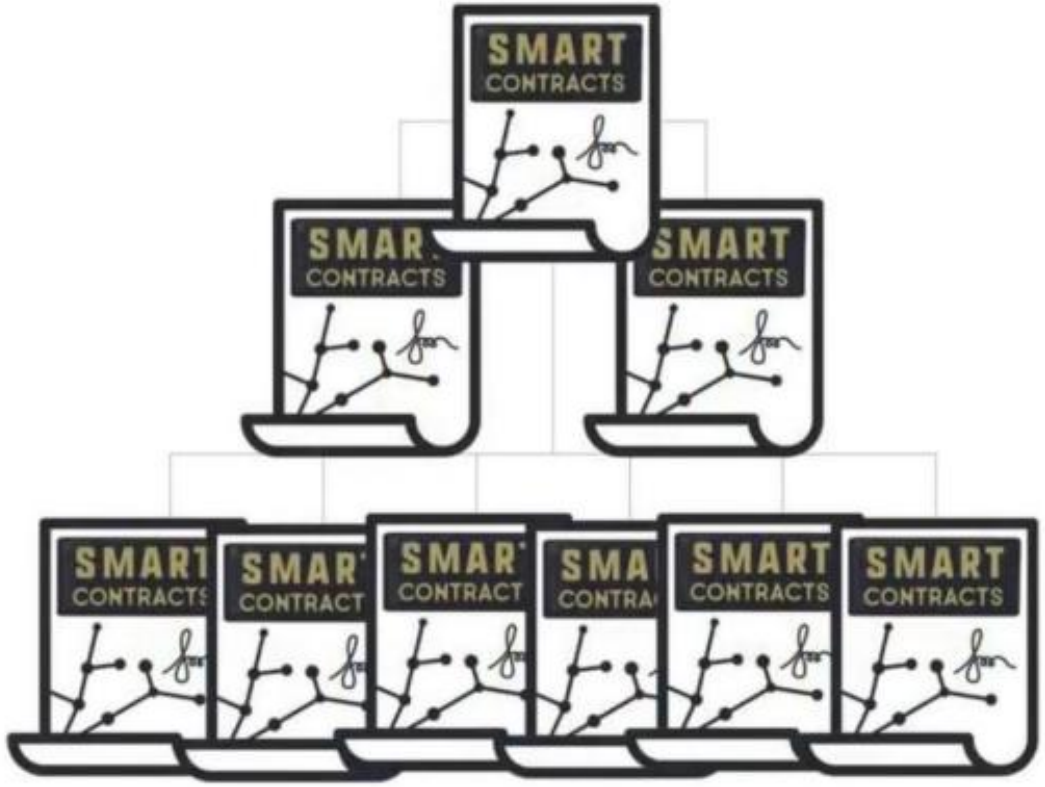

Block: #500,112
Timestamp: 1519181244
Nonce: 323451
Transactions:
198D2F359AB1AC868A1CC8275AE96
D8C58A0FA9D706F68A2F0406FBB71
45AF4FAC8D9F6C7FEA7E86D1706DD
A8DB07FCDD07753644A3097F6A3A2
AEB62940FA07DC9E81ACD03DDA05C
Prev.Hash: 0000DF2E57FB432A
Hash: 0000E9A61C1A43E1
1mb
198D2F359AB1AC868A1CC8275AE96
From: X
To: Y
Amount: 0.3 BTC
Signature: < ... >
Public Key: < ... >
60%
scriptSig

Decentralized Autonomous Organizations (DAOs)

Generic Organization



DAOs



2016
On Ethereum
Investor-directed venture capital fund
Stateless
May 2016 Crowdfunded ~$150,000,000
June 2016 Hacked for ~$50,000,000
Dilemma: *"Code Is Law?"*

DAO Attack

Solution presented was:

Solution: Hard Fork

Solution: Hard Fork

-> Ethereum split into 2 parts

-> ETH and ETC

ETH(Ethereum): Money returned to owner/DAO

ETC(Ethereum Classic): Money remains on child account and will be transferred to hacker’s account after decided time limit

Remember: Problem was in DAO code not in Ethereum

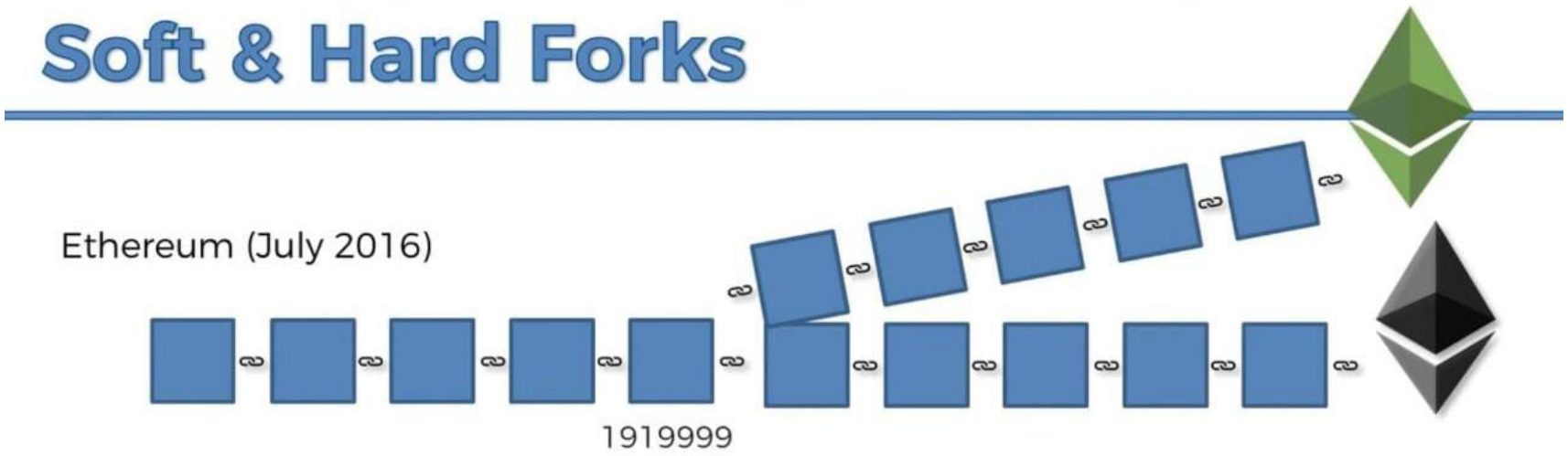
Must read Blog:

The Ether Thief

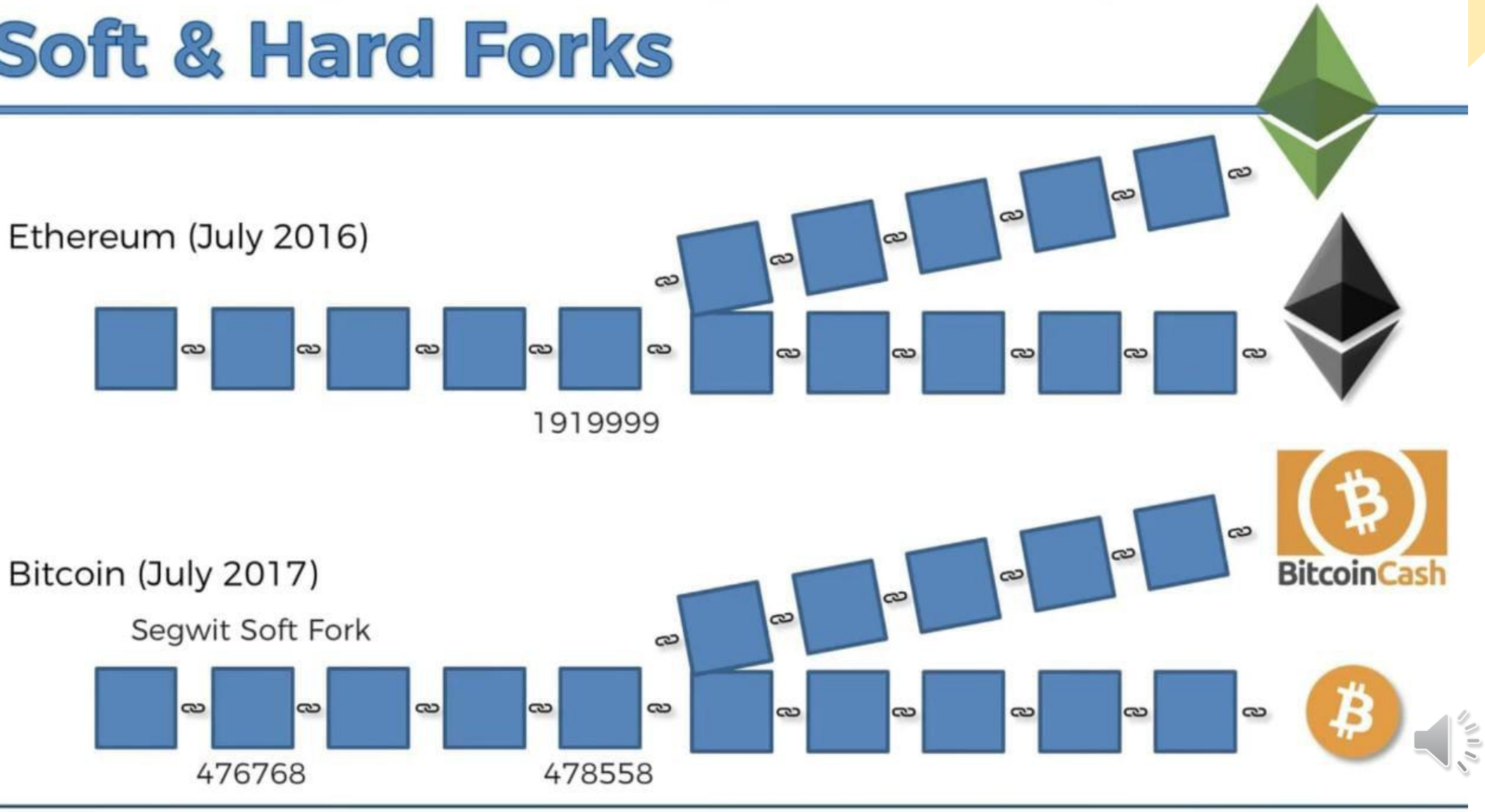
https://www.bloomberg.com/features/2017-the-ether-thief/

Soft & Hard Forks

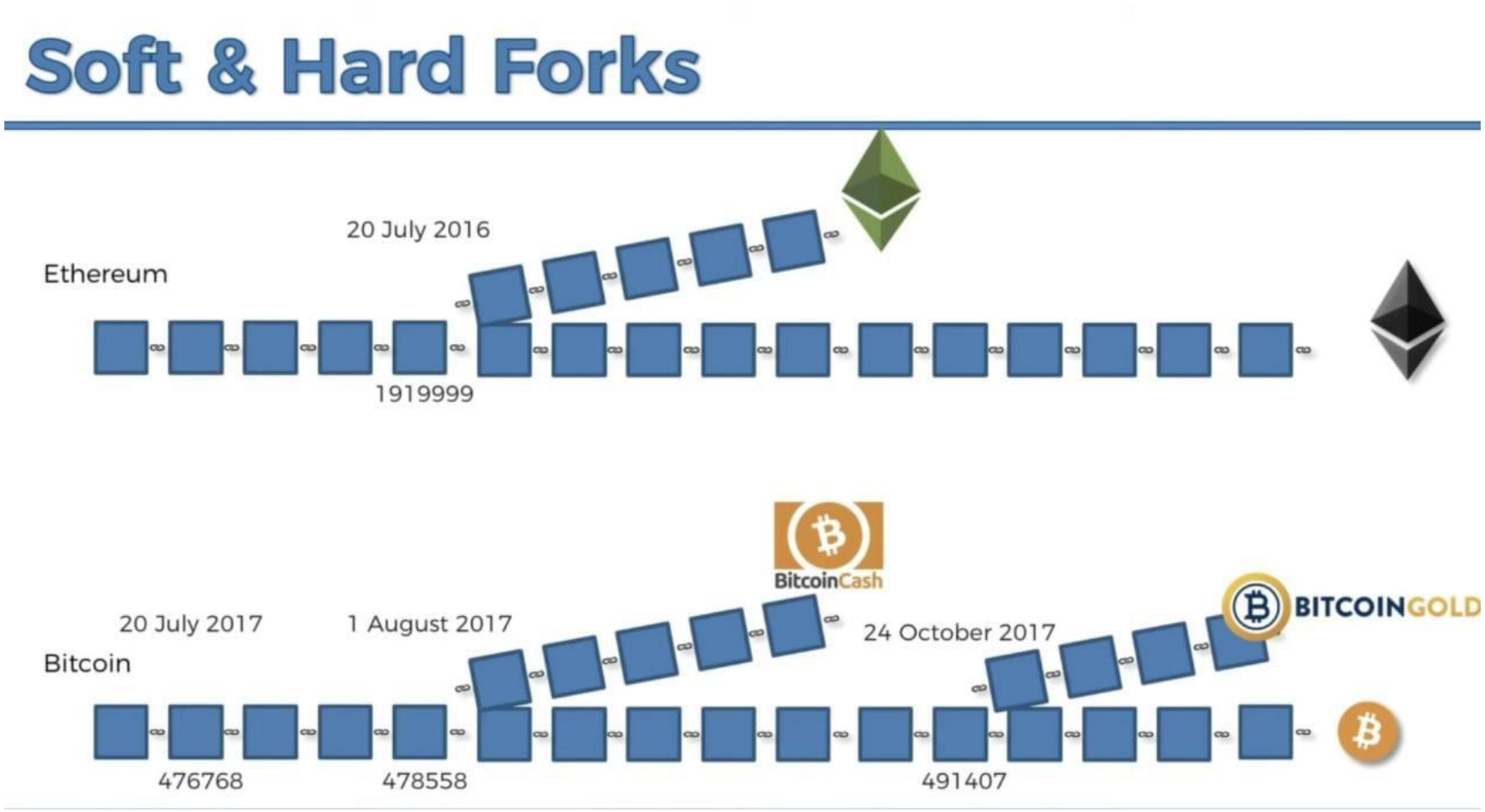
Hard Fork produced ETH and ETC



Soft & Hard Forks



20 July 2016 --- Hard Fork on Ethereum to change rules of smart contract due to DAO attack
20 July 2017 --- Soft Fork on Bitcoin to upgrade Bitcoin with Segwit Witness feature
1 August 2017 --- Hard Fork on Bitcoin to increase the Block size up-to 8MB from 1 MB
24 October 2017 --- Hard Fork on Bitcoin to make ASIC resistant network.



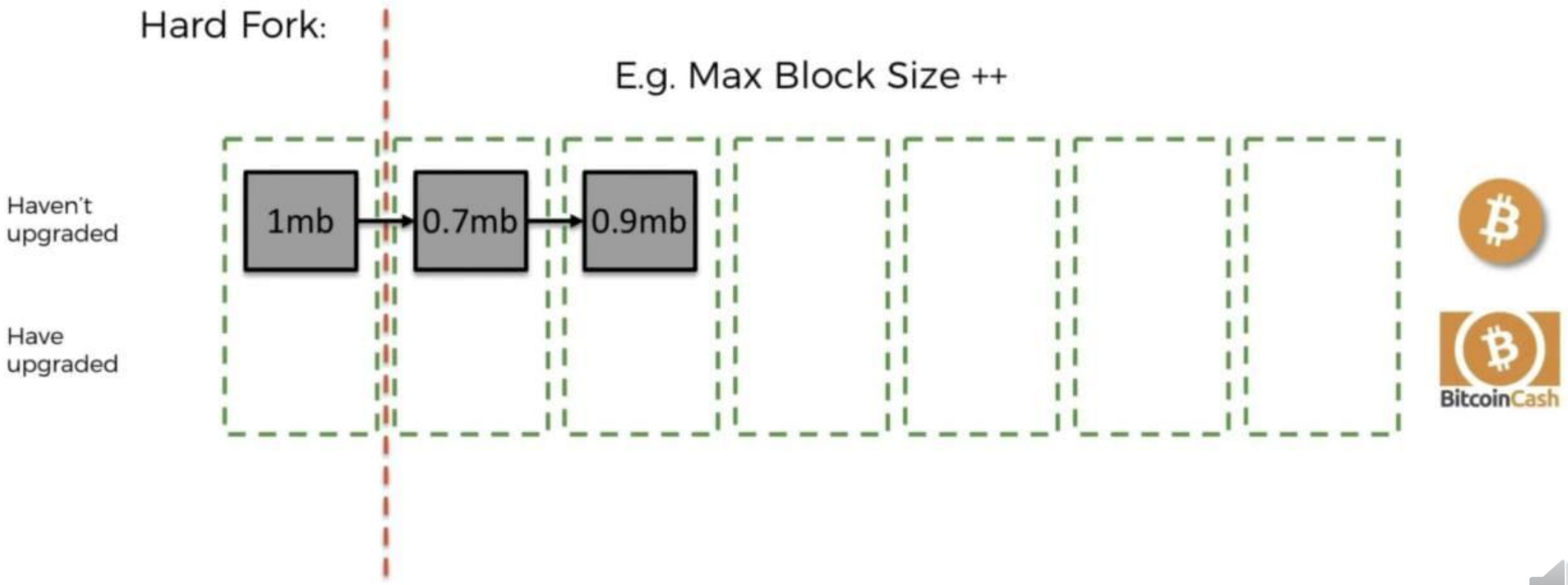
Soft & Hard Forks

Hard Forks = Loosen Rules

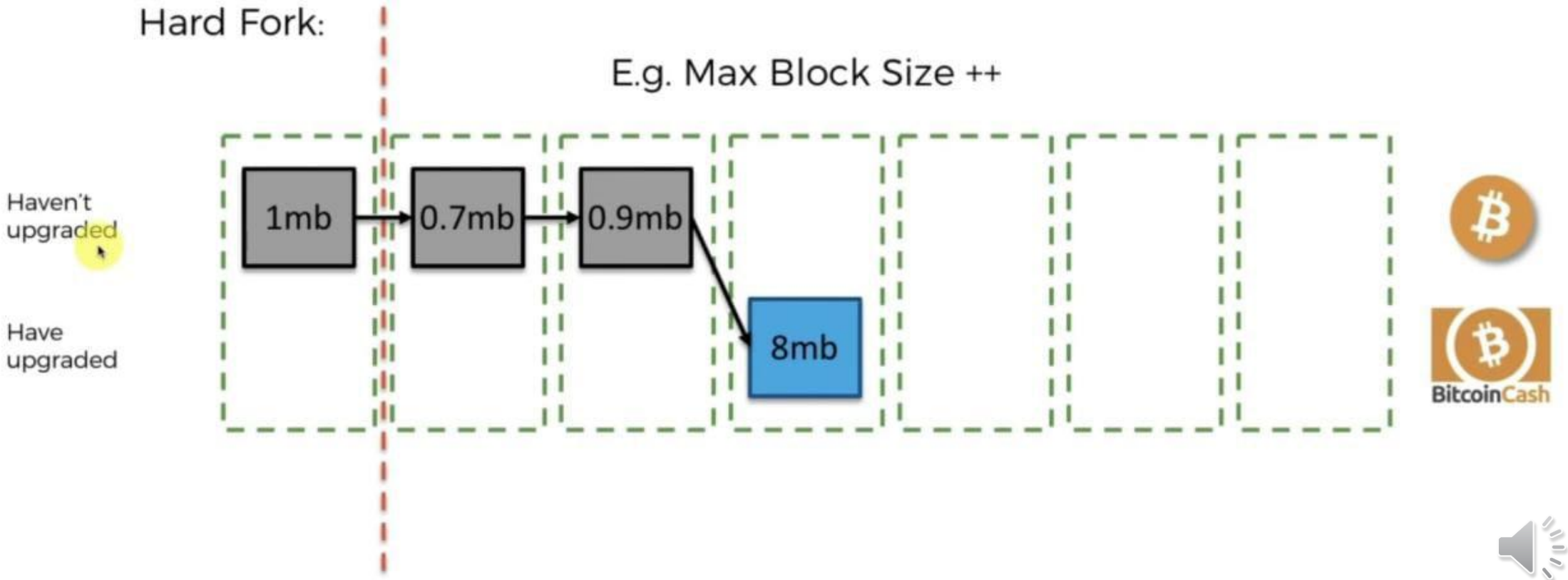
Soft Forks = Tighten Rules

Hard Fork

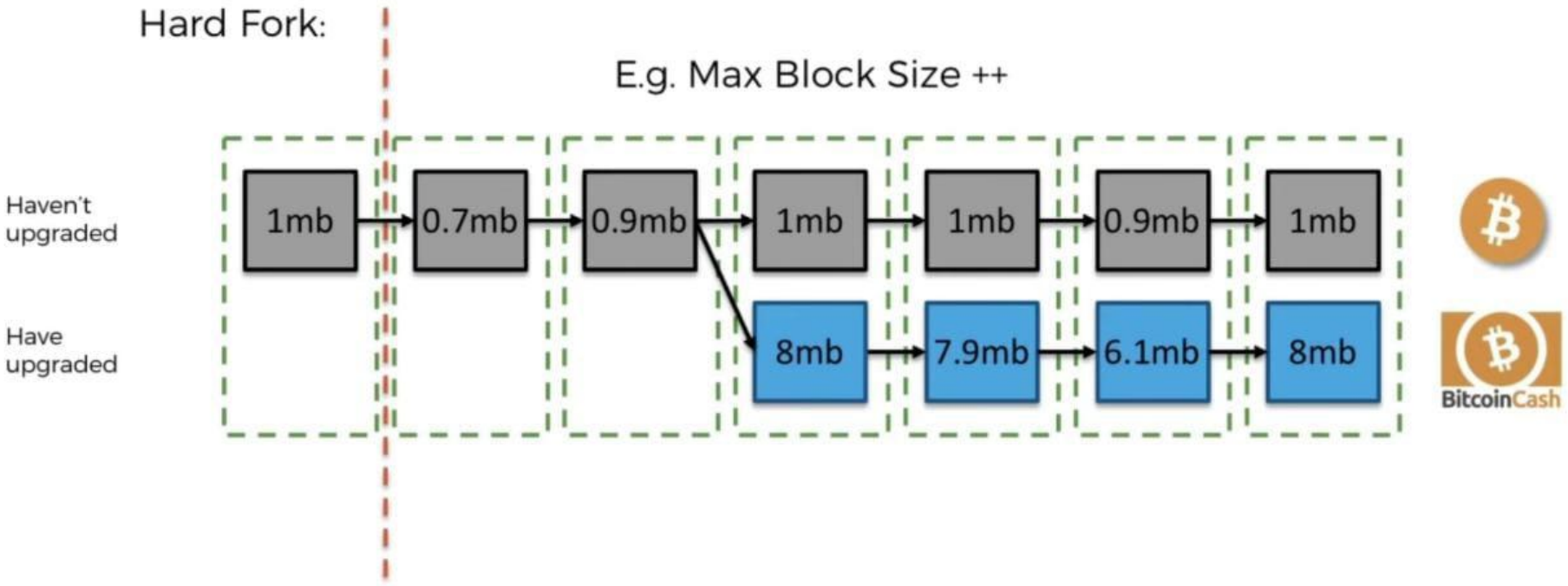
Soft & Hard Forks



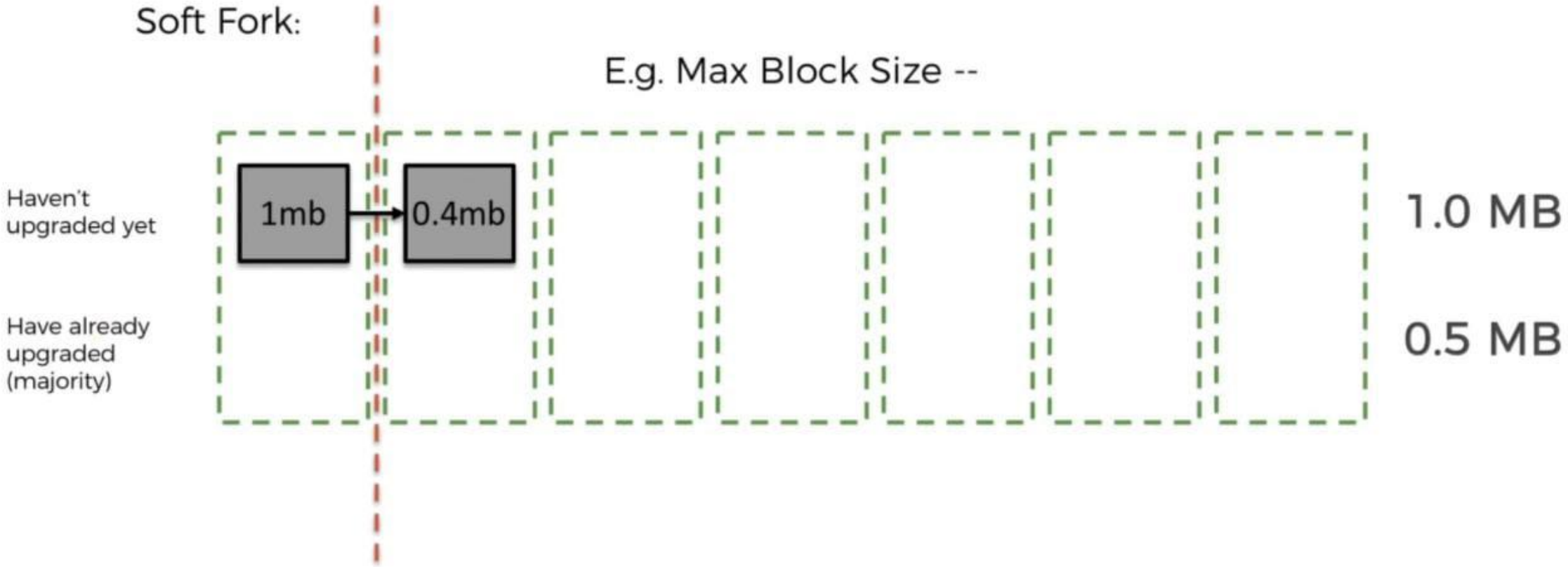
Soft & Hard Forks



Not Backward Compatible

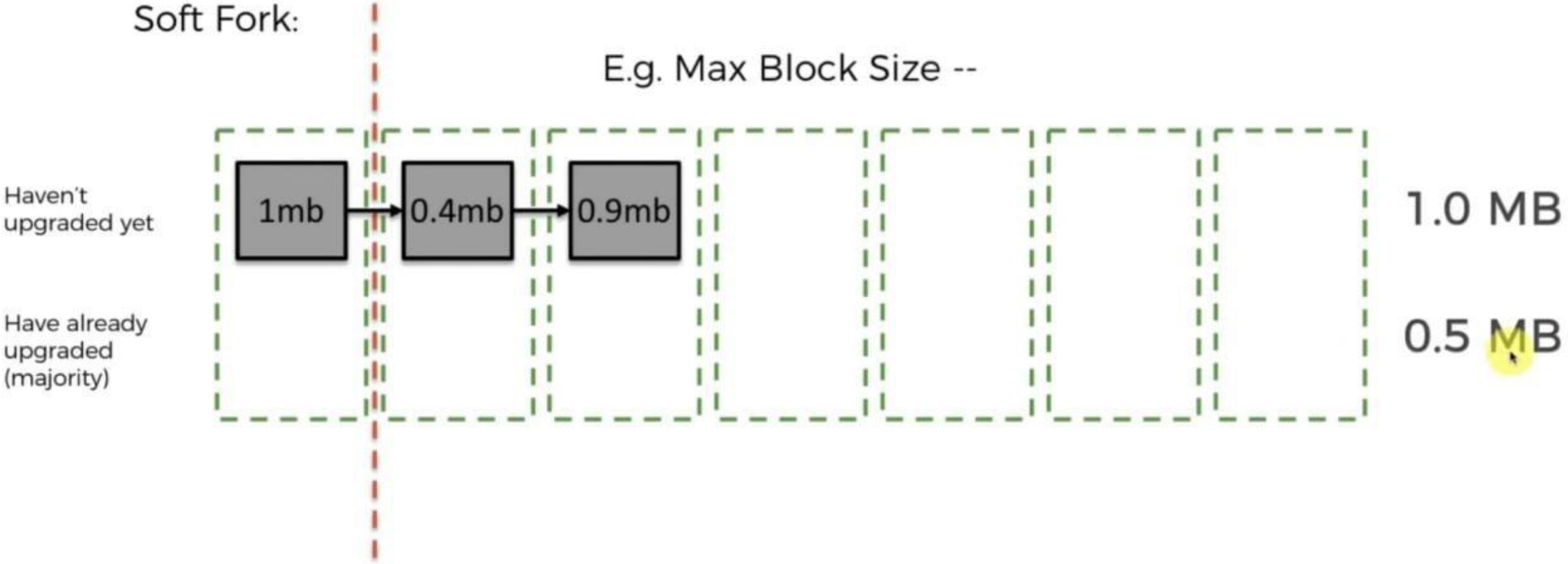


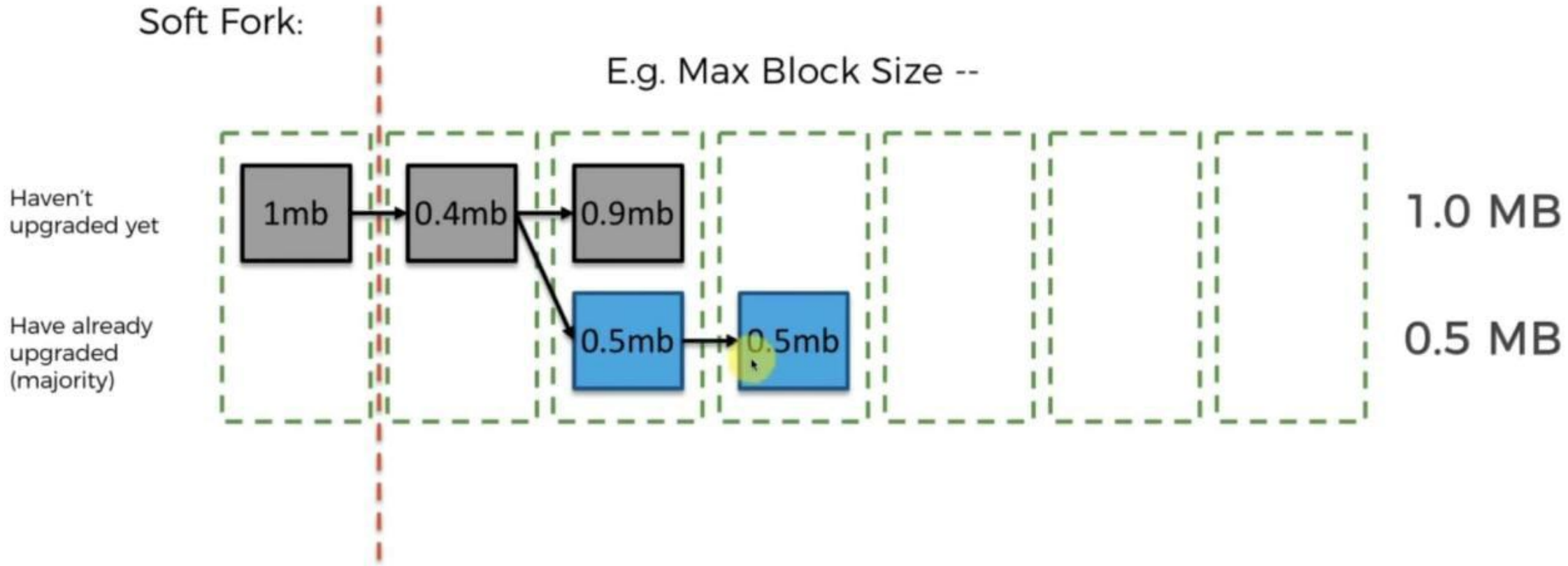
Soft Fork

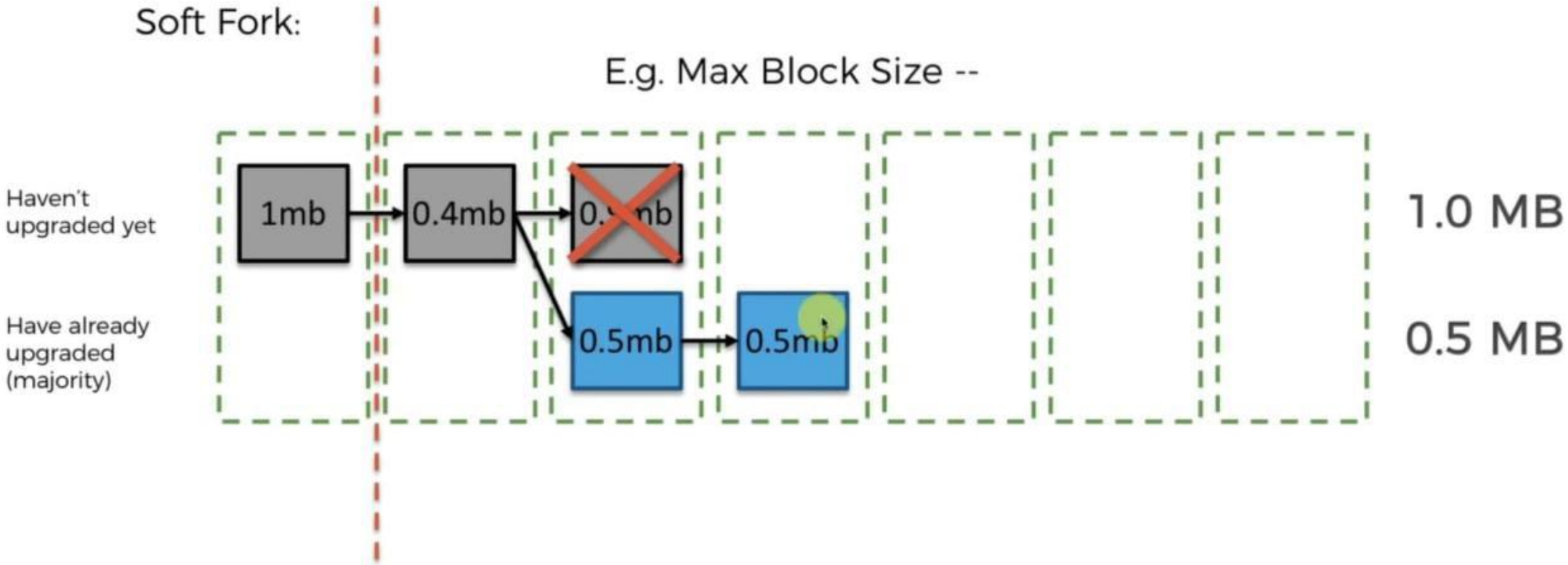

Soft Fork:
E.g. Max Block Size --
Haven't upgraded yet
1mb
0.4mb
1.0 MB
Have already upgraded (majority)
0.5 MB

Soft Fork:

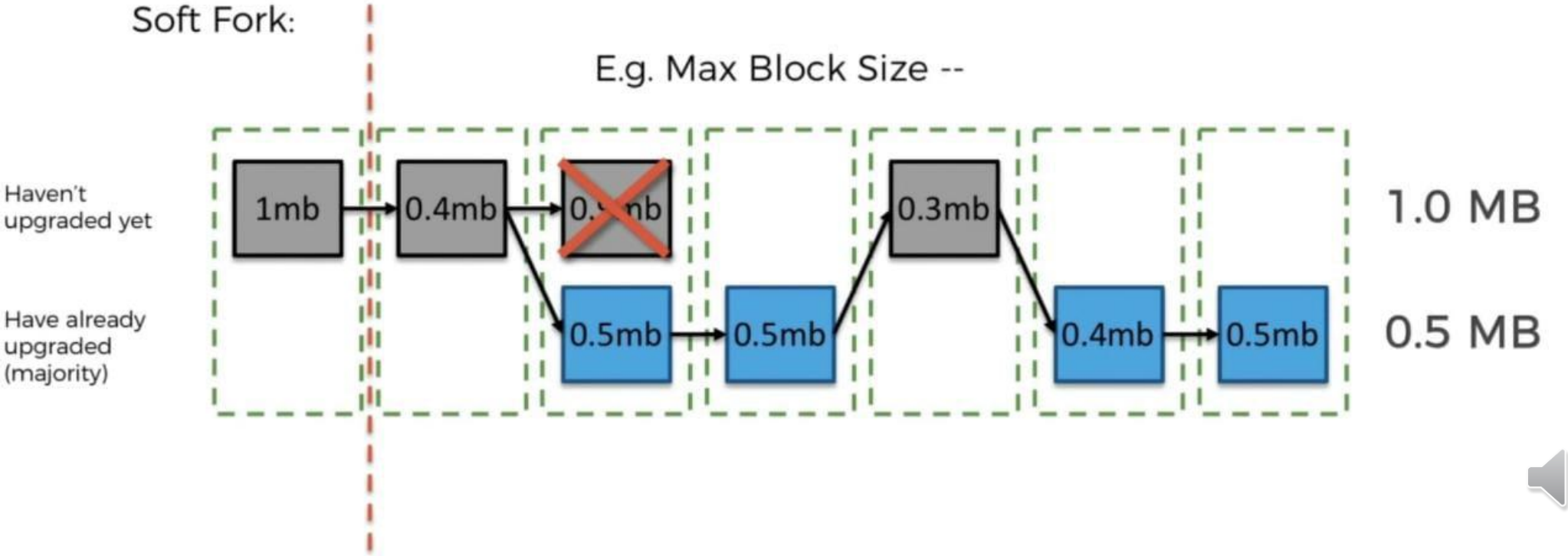
E.g. Max Block Size --



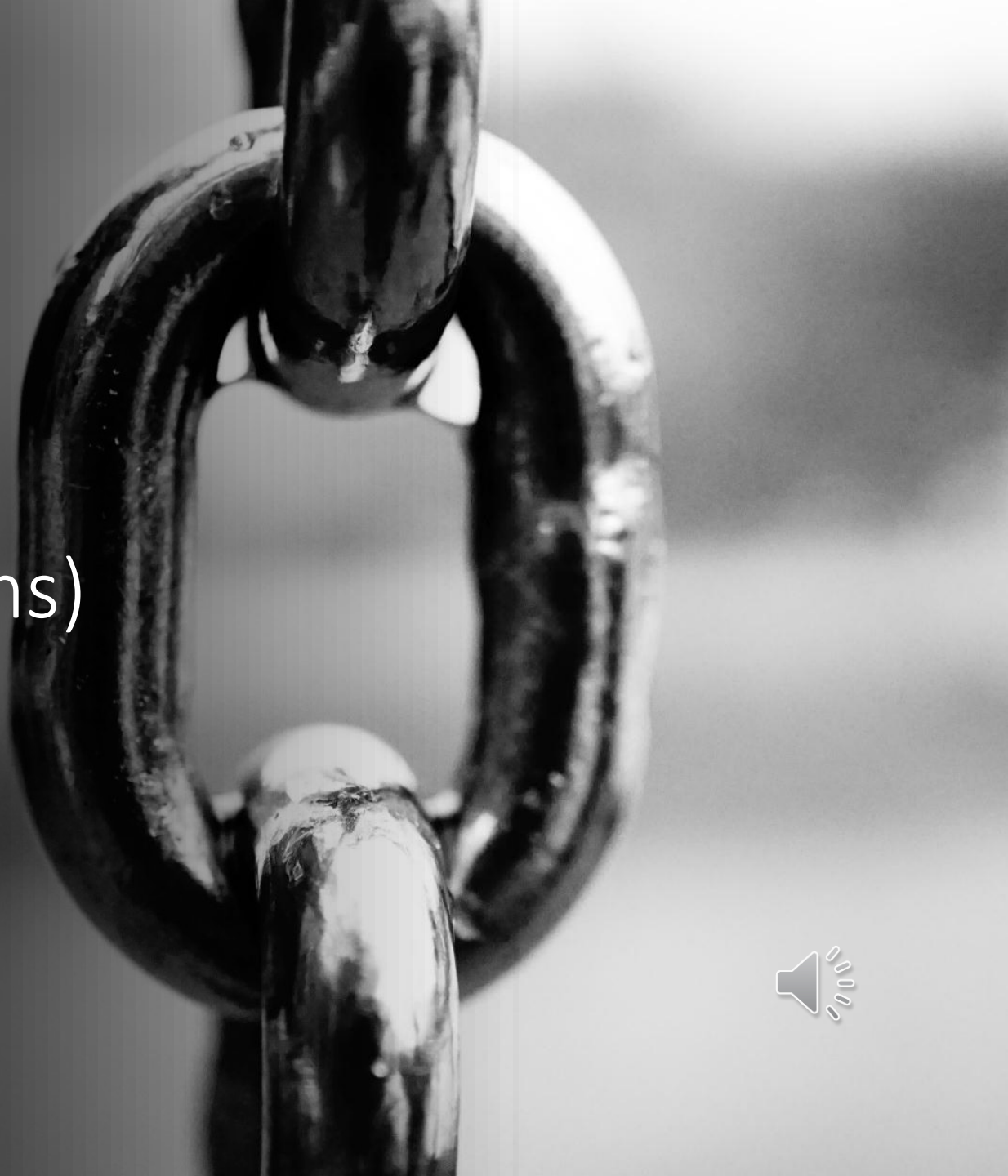

Soft Fork:
E.g. Max Block Size --
Haven't upgraded yet
Have already upgraded (majority)
1mb
0.4mb
0.9mb
0.5mb
0.5mb
1.0 MB
0.5 MB


Soft Fork:
E.g. Max Block Size --
Haven't upgraded yet
Have already upgraded (majority)
1mb
0.4mb
0.5mb
0.5mb
0.5mb
1.0 MB
0.5 MB

Backward Compatible



Proofs(Consensus Algorithms) in Blockchain



PoW – Proof-of-Work

Proof-of-Work

- Miners has to solve a crypto puzzle
- Miner who solved the puzzle first, will get the mining reward.
- There is a lot of power consumption in PoW
- Higher you have the hash rate or hashing power, higher the chance to mine the block
- Miners are also group together to increase the hashing power and distribute the mining reward, called mining pools

Energie usage ⏫

Mining pools -> centralization 😡

Drawback of PoW

PoS – Proof-of-Stake

PoS – Proof-of-Stake

Instead of Miners, PoS has **Validators**

Validators are responsible for minting/forging the block(s)

To become a validator, a node has to deposit certain amount of coins into the network as **Stake**

We can think it like a security deposit

PoS – Proof-of-Stake

Size of Stake determines the chances of validator to be chosen to forge the next block

No electricity wastage, No mining pools,

Brings Disadvantages too (favors rich nodes, 51% attack(less chances than PoW))

Casper – Proof-of-Stake system by Ethereum – Deployed on Ethereum testnet

Cardano project is developing proof-of-stake Algorithm, Ouroboros

Delegated Proof-of-Stake

Proof-of-Authority

Proof of **Burn**

A consensus algorithm in which miners burn coins in order to get right to update the blockchain/ or mine a block

Verifiers also need to burn the coins in order to validate the transactions

Acknowledgement and Source:

- https://www.udemy.com/course/build-your-blockchain-az/