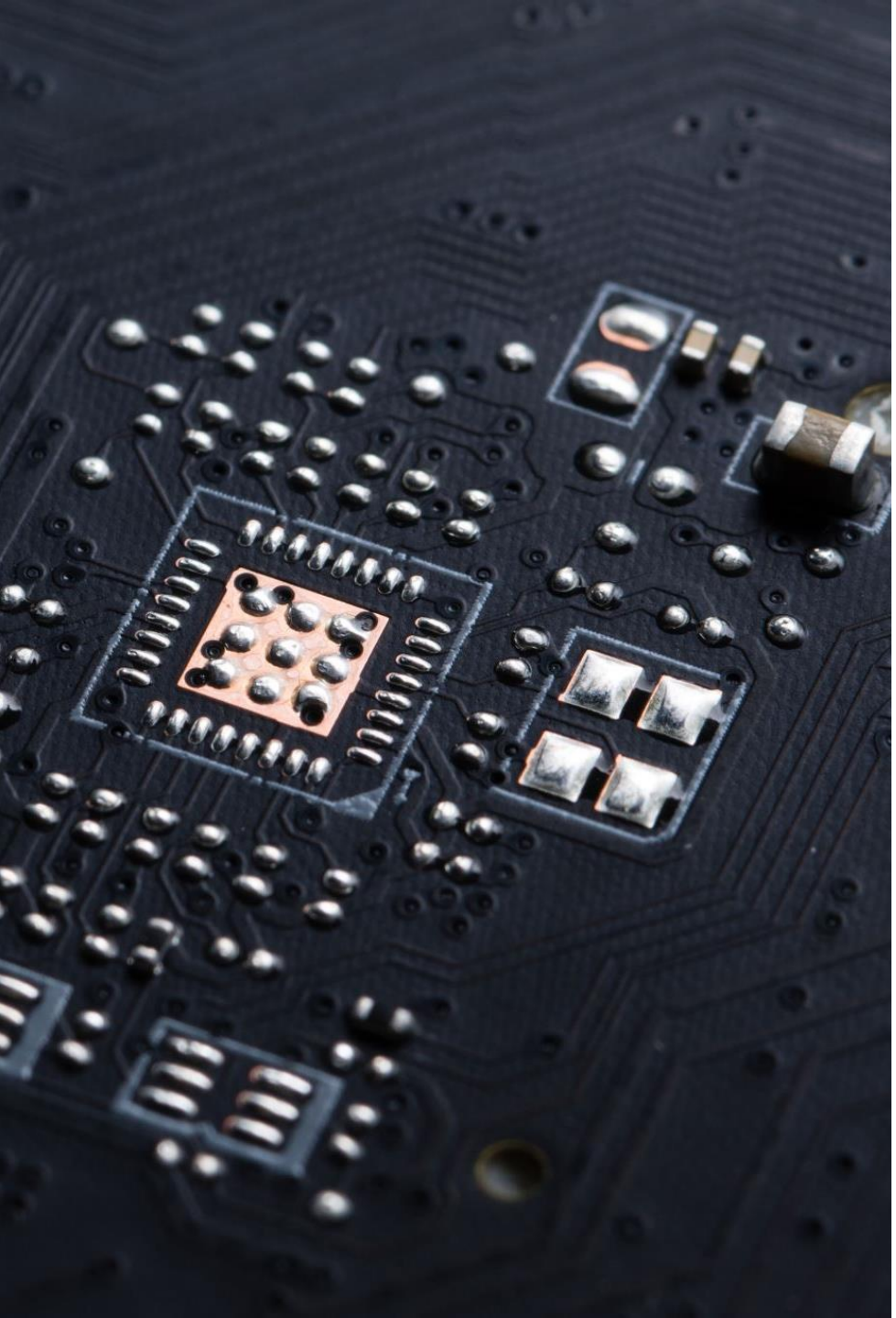
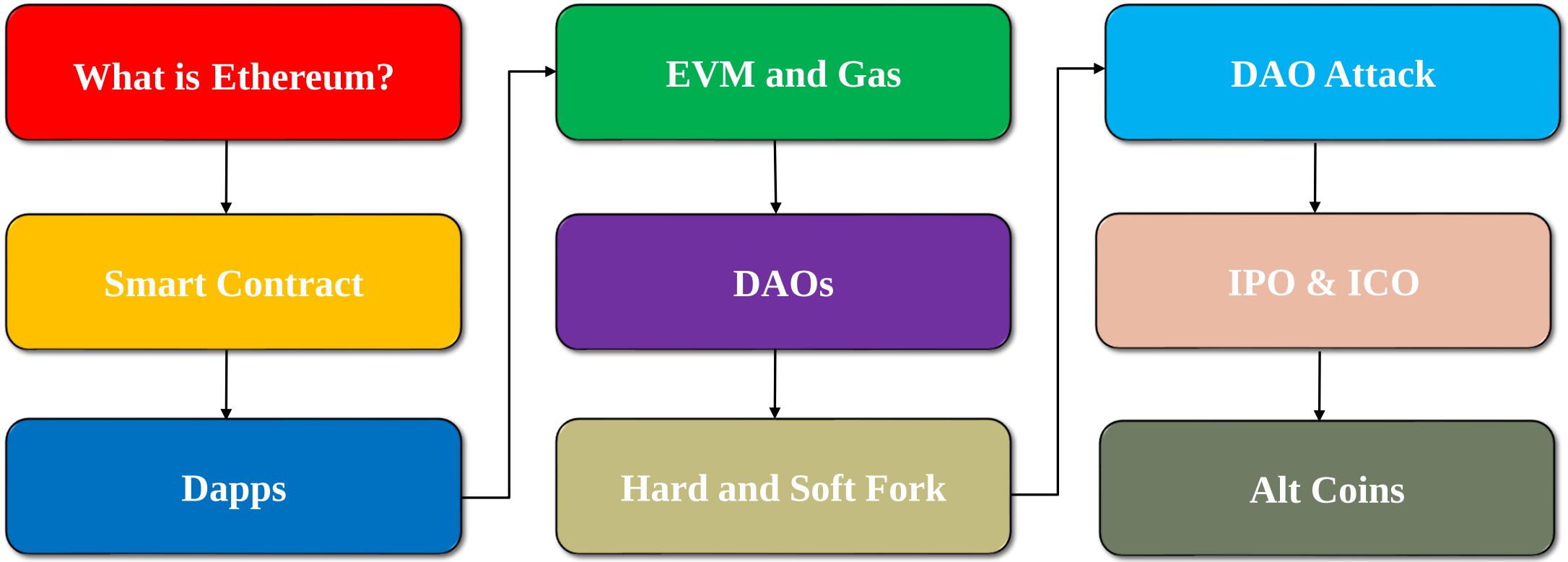
Blockchain

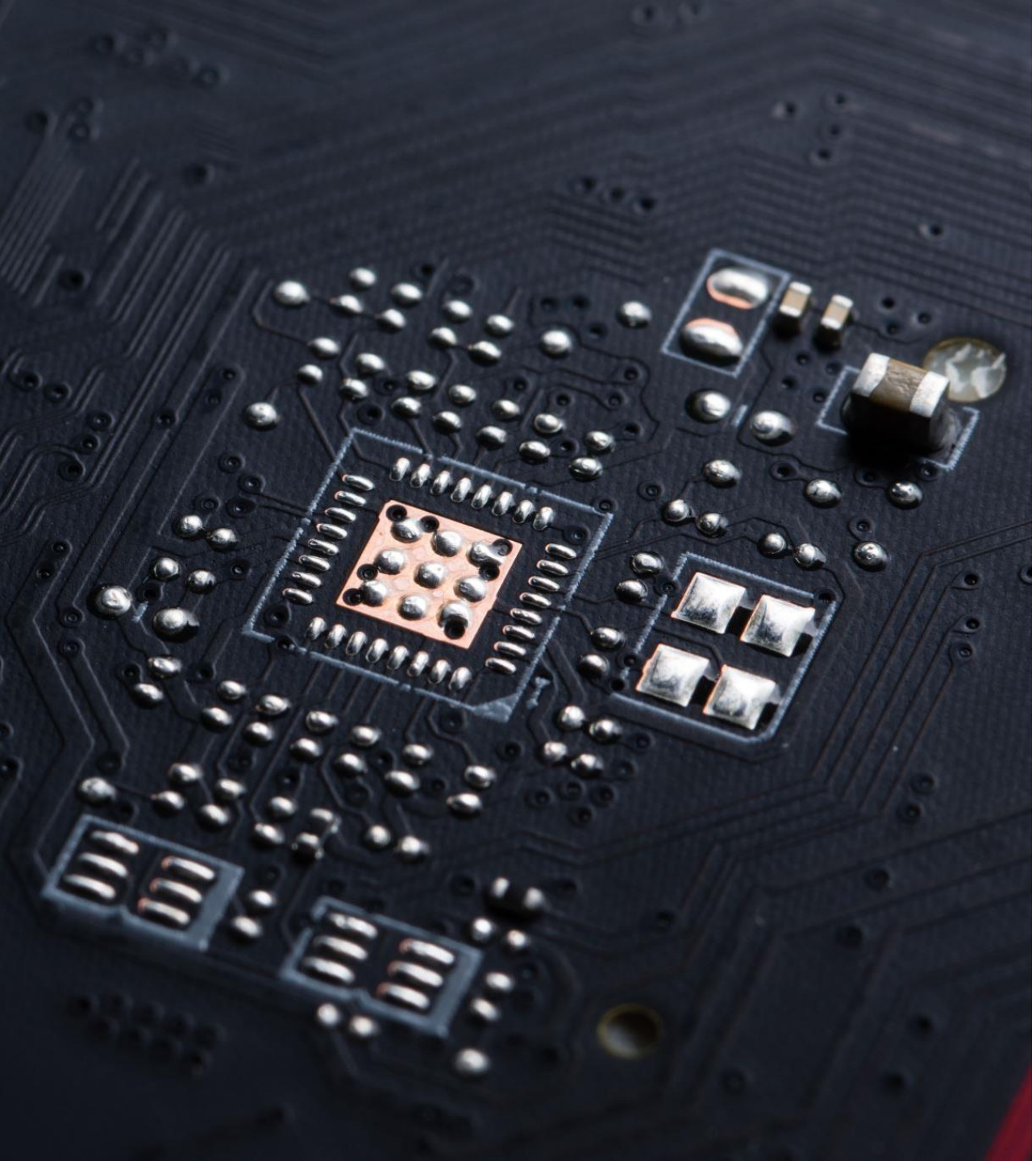
Dr. Bahar Ali
Assistant Professor (CS), National University Of Computer and Emerging Sciences, Peshawar.



Ethereum

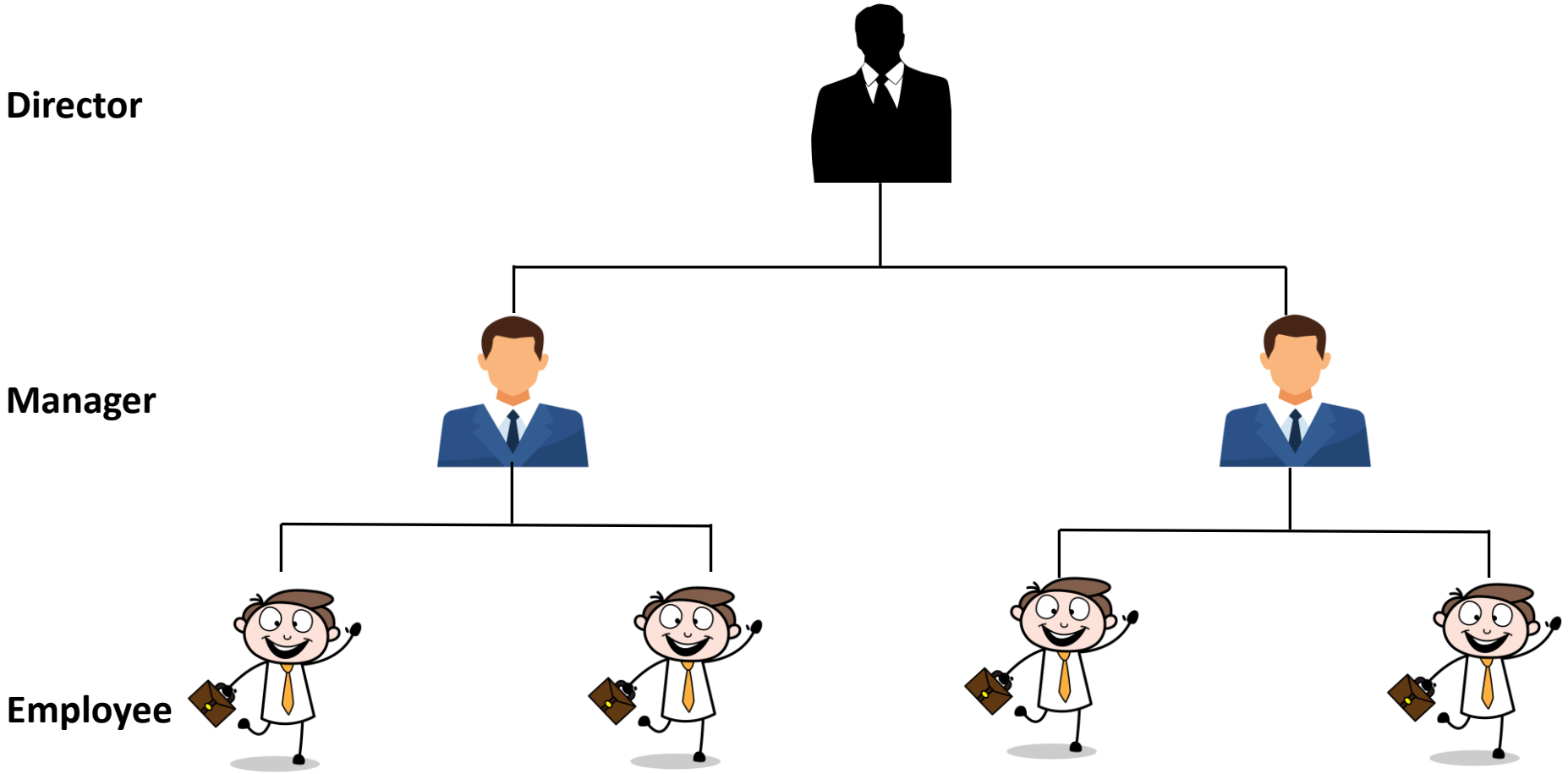
Contents – Module C





Decentralized Autonomous Organization (DAOs)

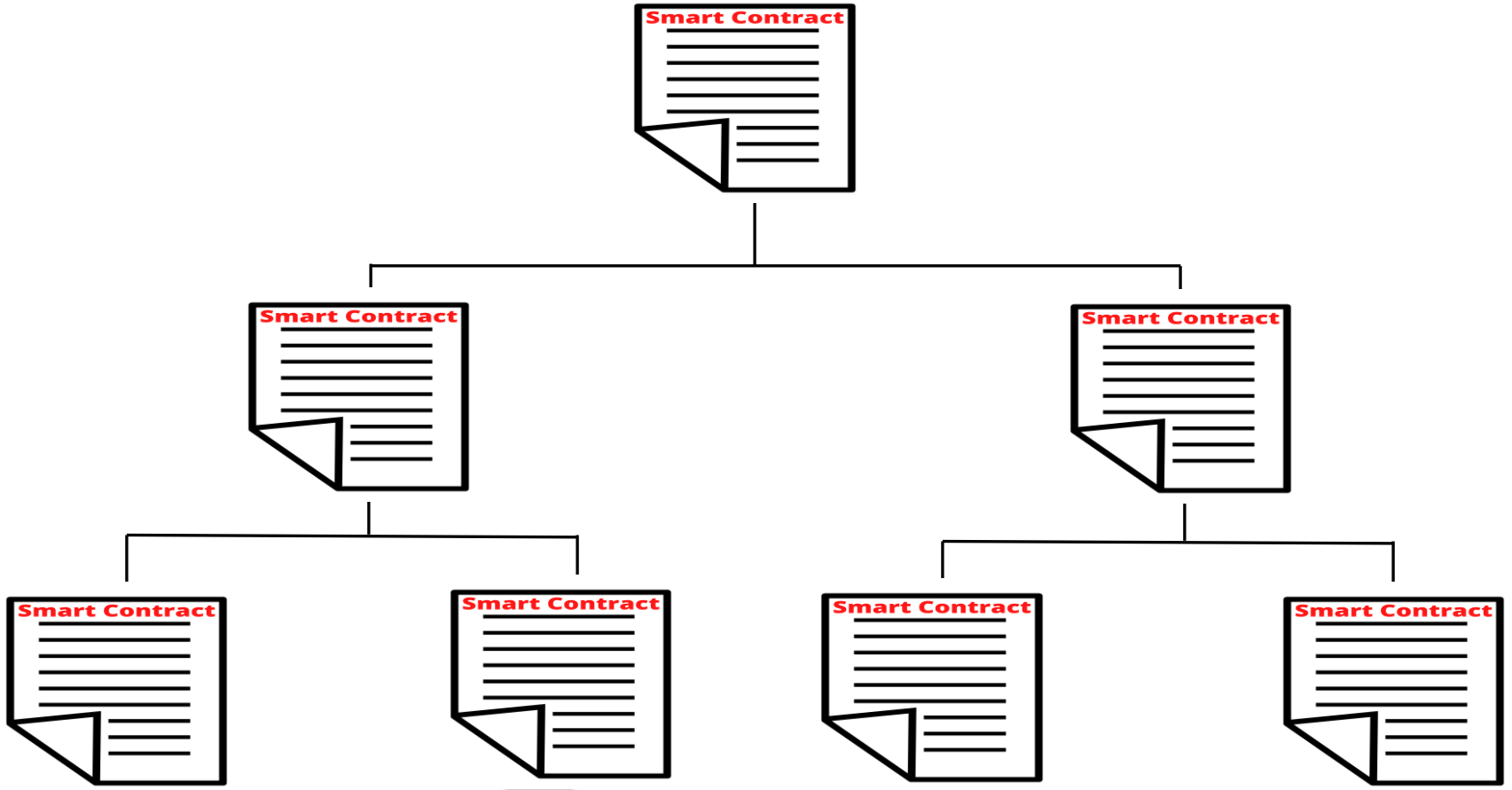
Traditional Organization



Traditional Organization

- In a traditional organization, every employee has their own role
- However, the company is mainly controlled by the director/ owner
- The organization has some tasks of repetitive nature like doubts of customers, which can be solved by a chatbot etc., and need no human interactions. However, if involve human, then expenses are increased
- **The solution for this is DAOs**

Decentralized Autonomous Organization (DAOs)



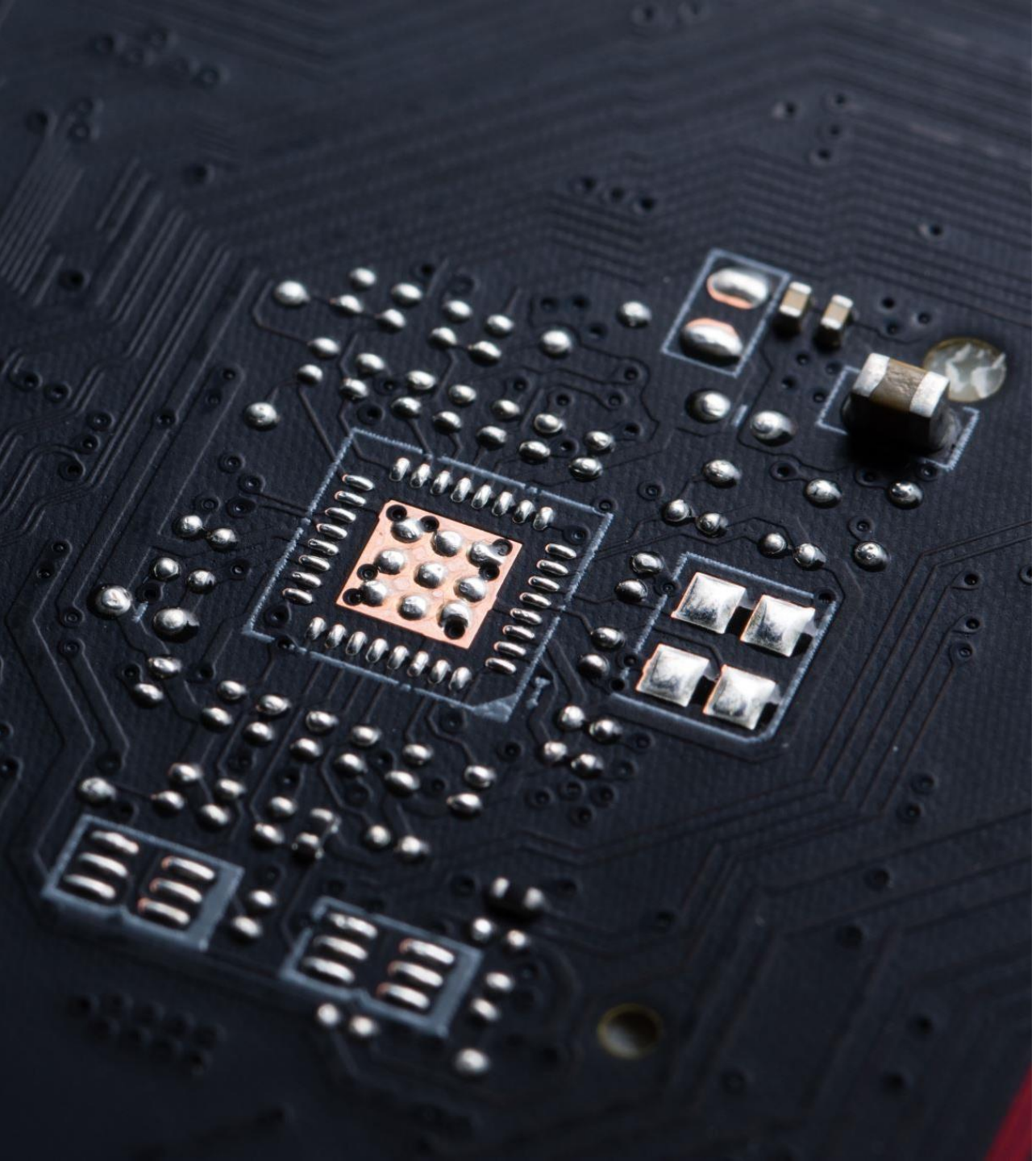
Decentralized Autonomous Organization (DAOs)

- A DAO is a community-led entity with no central authority.
- It is fully autonomous and transparent
- Smart contracts lay the foundational rules, execute the agreed-upon decisions, proposals, voting, and even the very code itself can be publicly audited
- A smart contract is written which can solve the repetitive tasks automatically
- works just like an organization that is why called DAOs

DAO vs Organization

DAO	A traditional organization
Fully democratized.	Usually hierarchical.
Voting required .	Voting may or may not require.
No trusted intermediary to count vote.	Outcome of voting must be handled manually.
Services offered are handled automatically.	Requires human handling, or centrally controlled automation.
All activity is transparent and fully public.	Activity is typically private, and limited to the public.

Decentralized Autonomous Organization (DAOs)

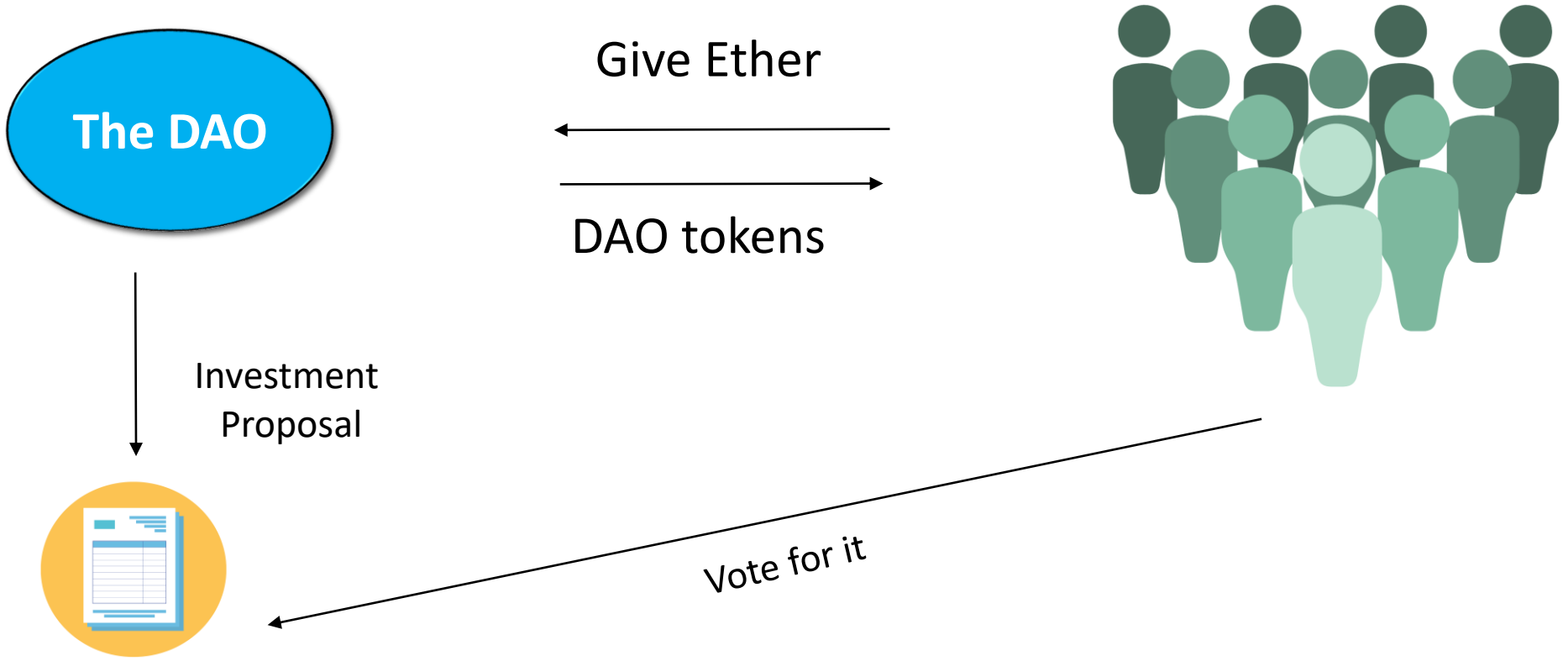


The DAO attack

The DAO

- The concept of a DAO was first ideated in 2015 by a German start-up Slock.it
- **The DAO** organization was established based on **a DAO** concept
- They wanted to make a DAO of a venture capital firm investing in any startup
- People invest ethers and buy DAO tokens and using the tokens people can vote for the investment proposals
- Raised more than $150 million from more than 11,000 investors, making it one of the largest crowdfunding campaigns in history at the time.

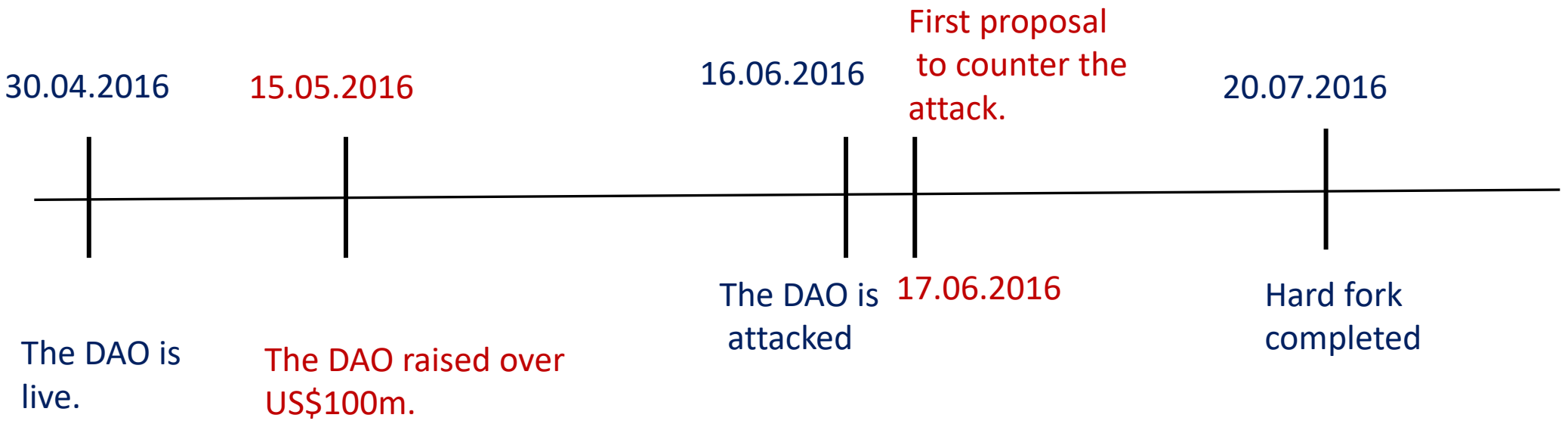
The DAO


The DAO
Give Ether
DAO tokens
Investment
Proposal
Vote for it

The DAO Attack

- After raising $150 million through a token sale, **The DAO** was hacked due to vulnerabilities in its code base (**Recursive Call Bug**)
- The problem was in the code of a smart contract, due to which the hacker withdraw $60 million
- The Ethereum community decided to solve this problem (30 days to stop)
- One proposal is accepted, where a Hard Fork was used
- The Ethereum network was divided into two parts i.e., **Ethereum Classic (Old)** and **Ethereum**

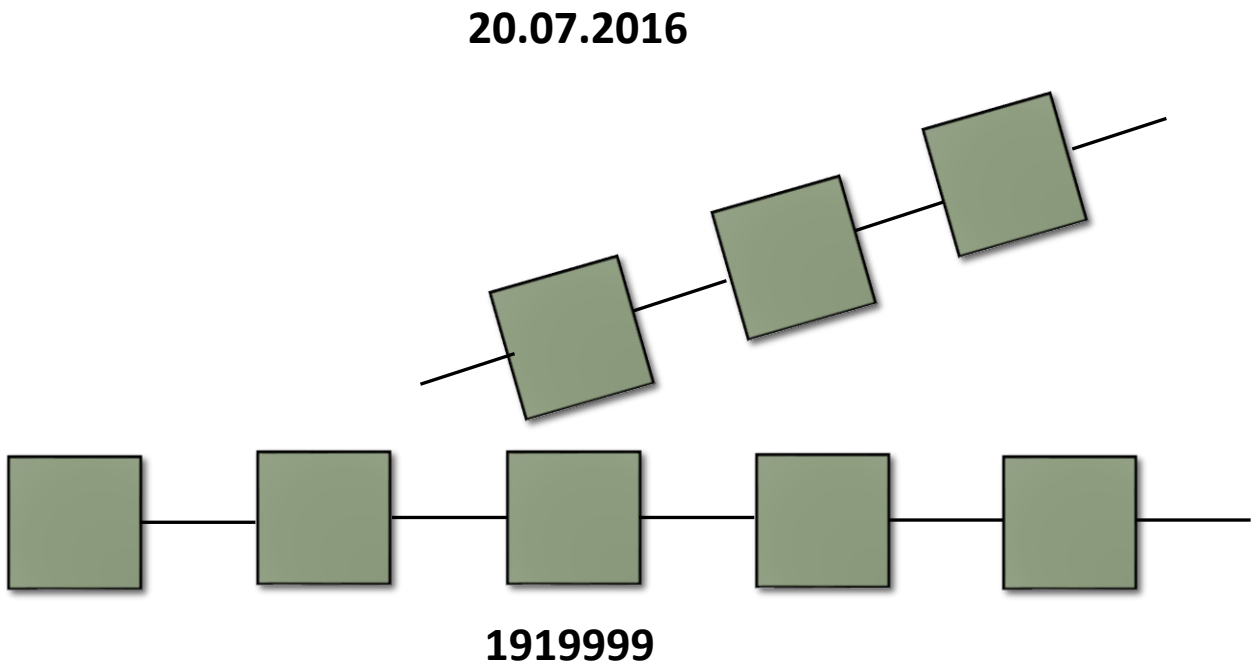
The DAO Attack



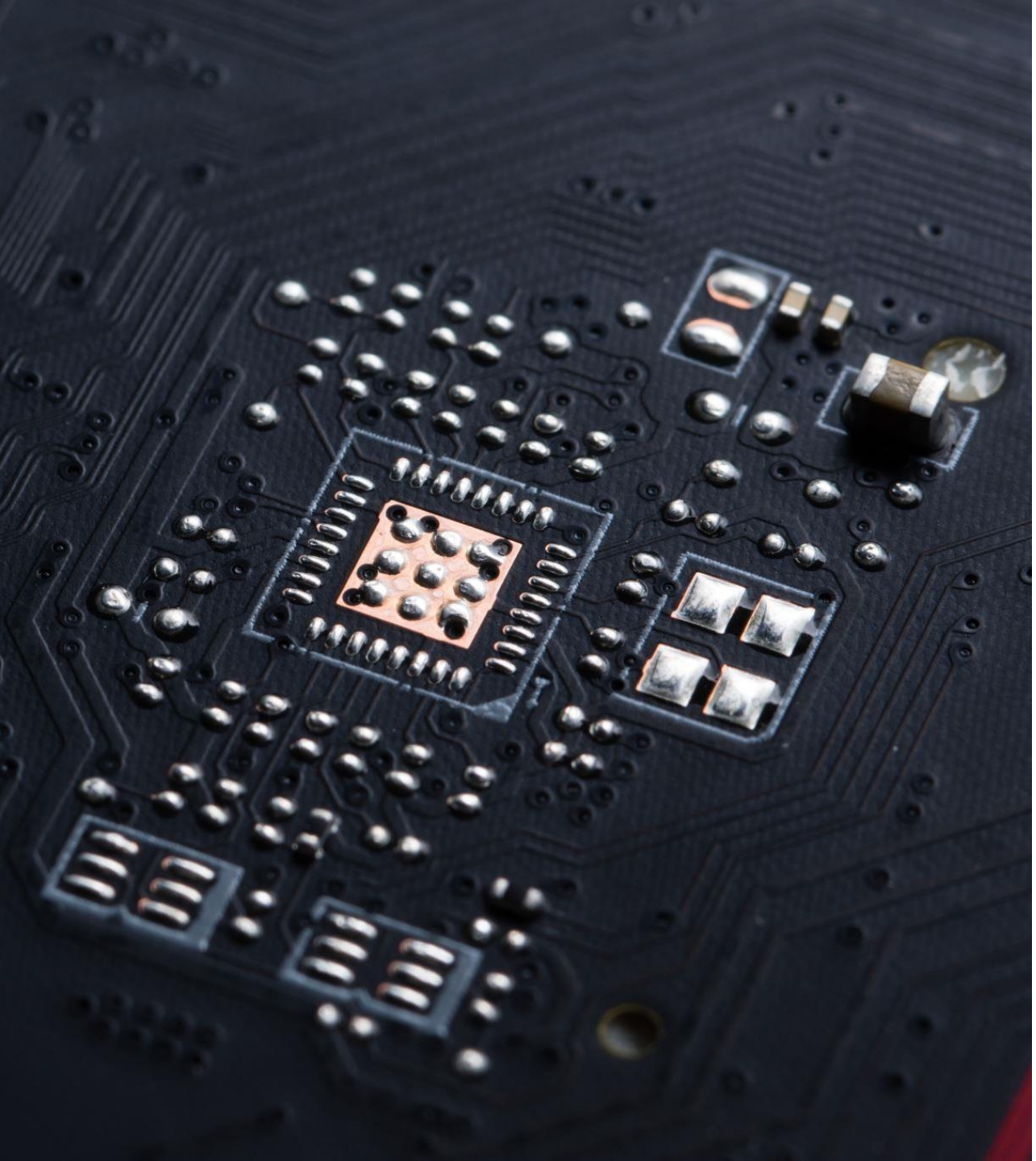
The DAO Attack

- Two communities are created based on two different opinions
- **Ethereum Classic (Old):**
  - They wanted not to change the smart contract as it was against the rules of a Blockchain
- **Ethereum:**
  - The community of the new network wanted to change a smart contract so that the amount will be recovered from the hackers

The DAO Attack

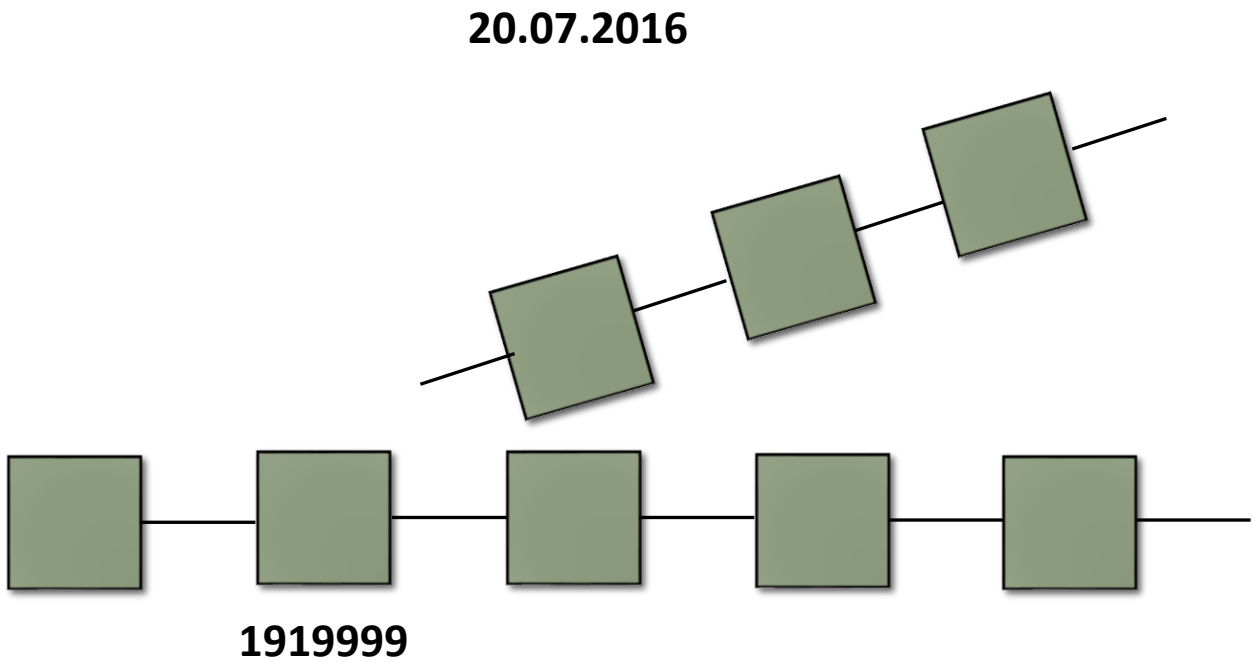


ethereum
classic



Hard Fork

Hard Fork



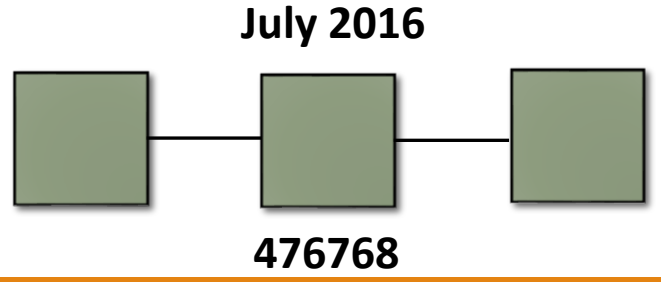
ethereum
classic

Hard Fork

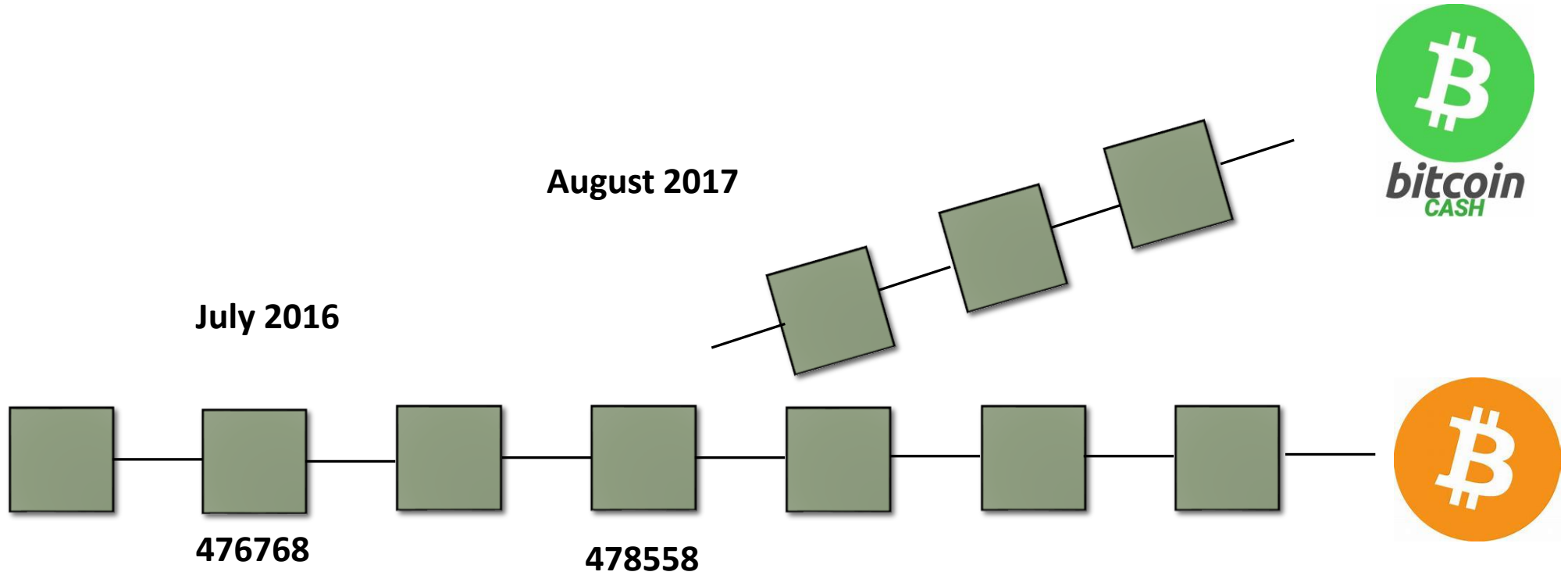
- During a hard fork, software implementing a protocol and its mining procedures is upgraded.
- Once a user upgrades their software, that version rejects all transactions from older software, effectively creating a new branch of the blockchain.
- However, those users who retain the old software continue to process transactions.

Hard Fork

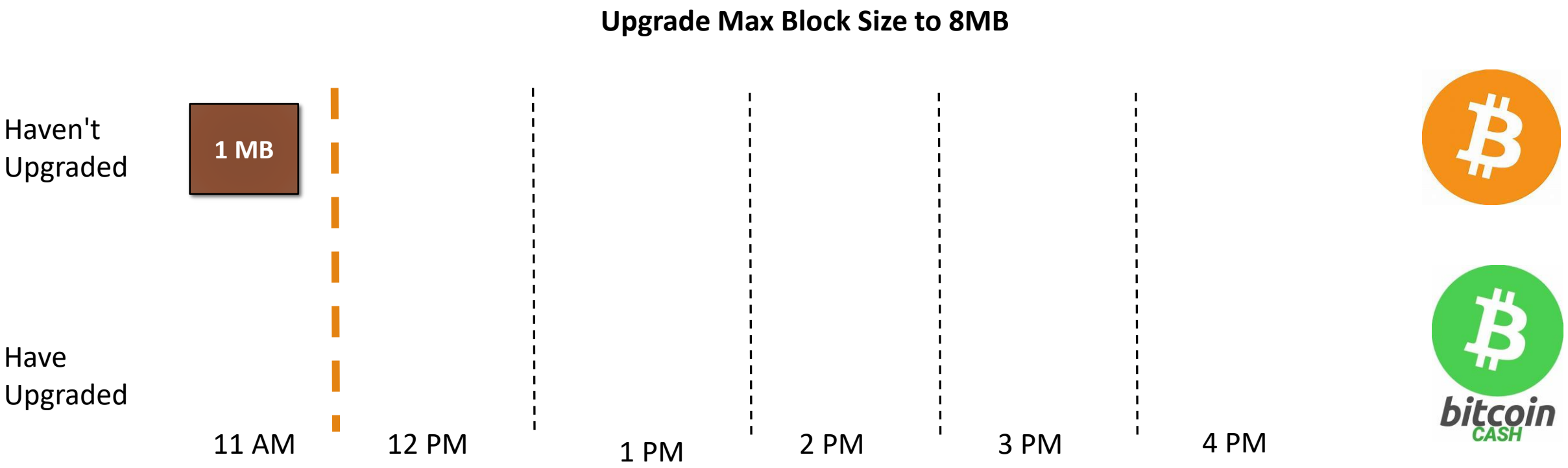
- A hard fork was used in the case of bitcoin
- As in the case of **SegregatedWitness,** where the public key and signature are separated from the transaction
- A month later one community rejected it and called it a temporary solution, according to them, the permanent solution is to increase the block size.
- A new community was named **Bitcoin Cash**
- I.e., Political parties are divided into competitors



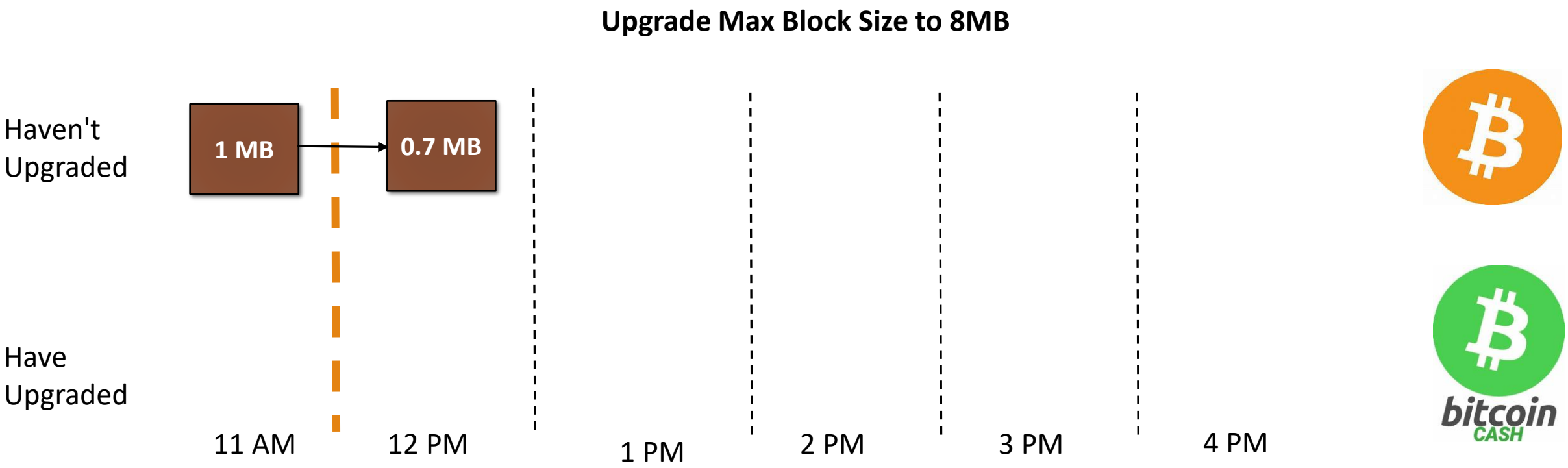
Hard Fork



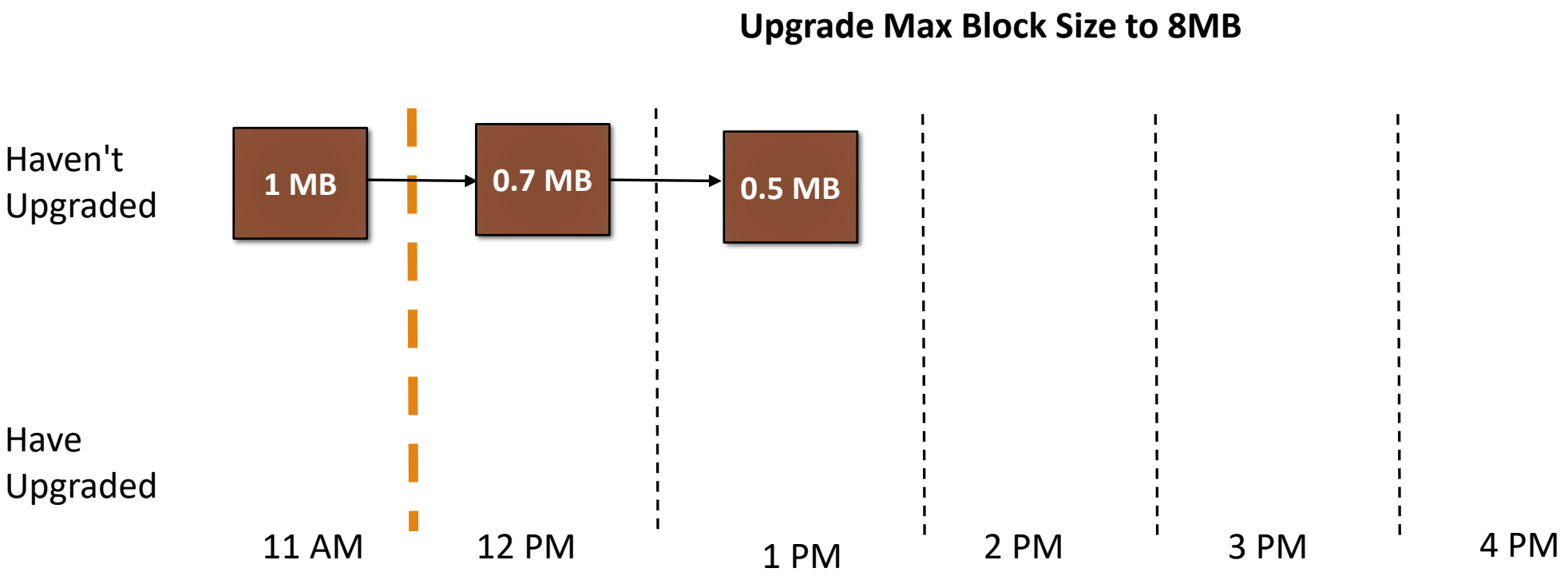
Hard Fork


Upgrade Max Block Size to 8MB
Haven't Upgraded
Have Upgraded
1 MB
11 AM
12 PM
1 PM
2 PM
3 PM
4 PM
bitcoin CASH

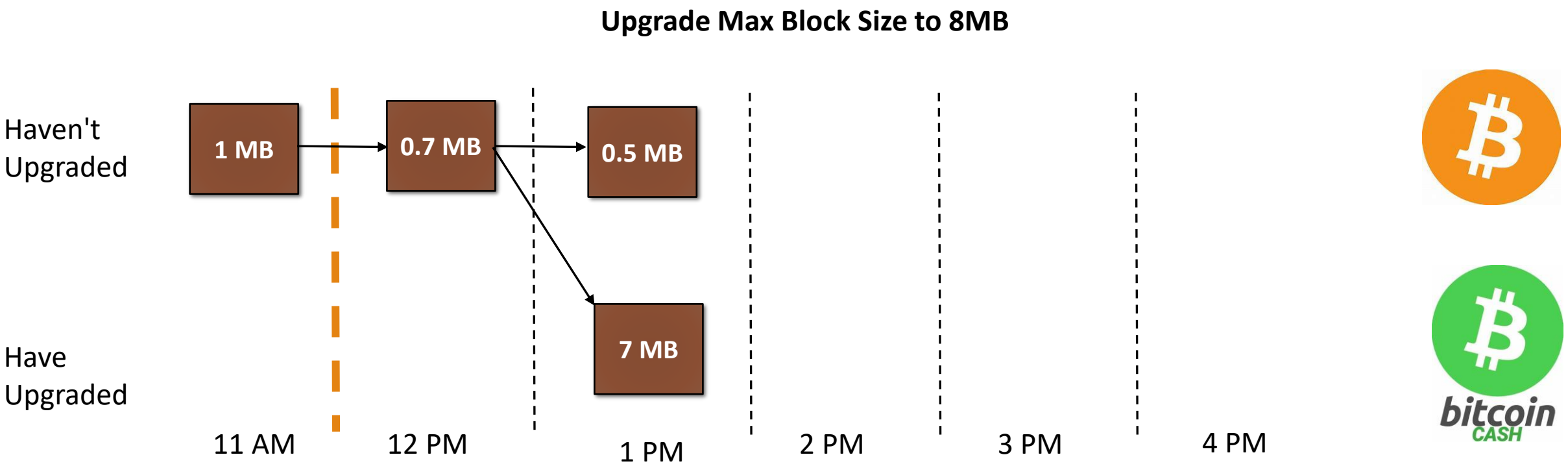
Hard Fork


Upgrade Max Block Size to 8MB
Haven't Upgraded
Have Upgraded
1 MB
0.7 MB
11 AM
12 PM
1 PM
2 PM
3 PM
4 PM
bitcoin
CASH

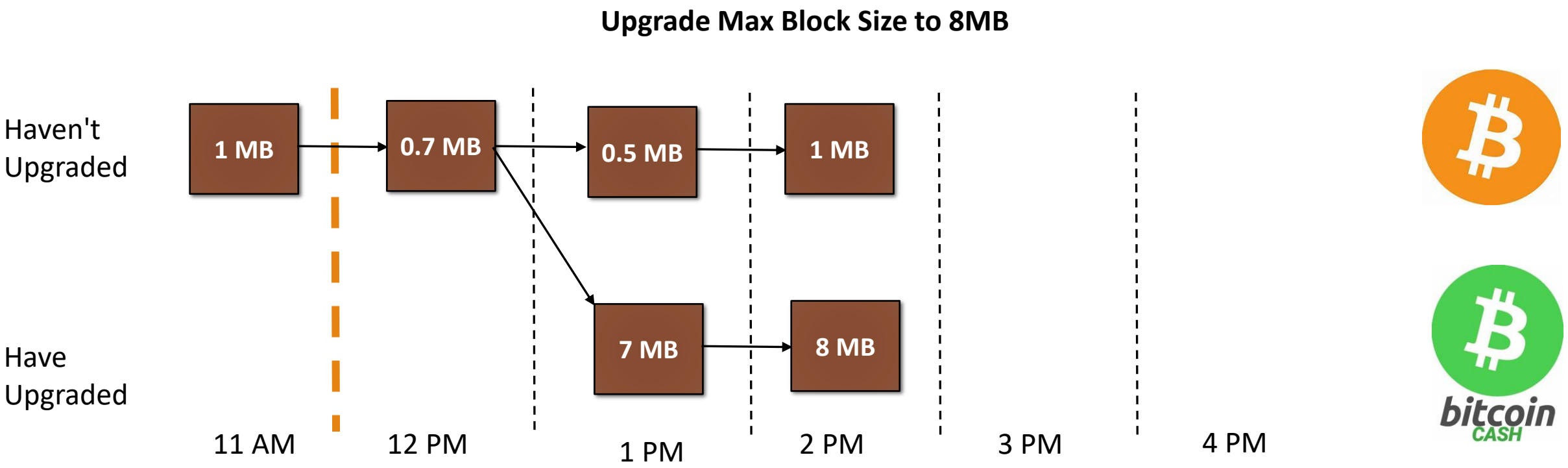
Hard Fork


Upgrade Max Block Size to 8MB
Haven't Upgraded
Have Upgraded
1 MB
0.7 MB
0.5 MB
11 AM
12 PM
1 PM
2 PM
3 PM
4 PM

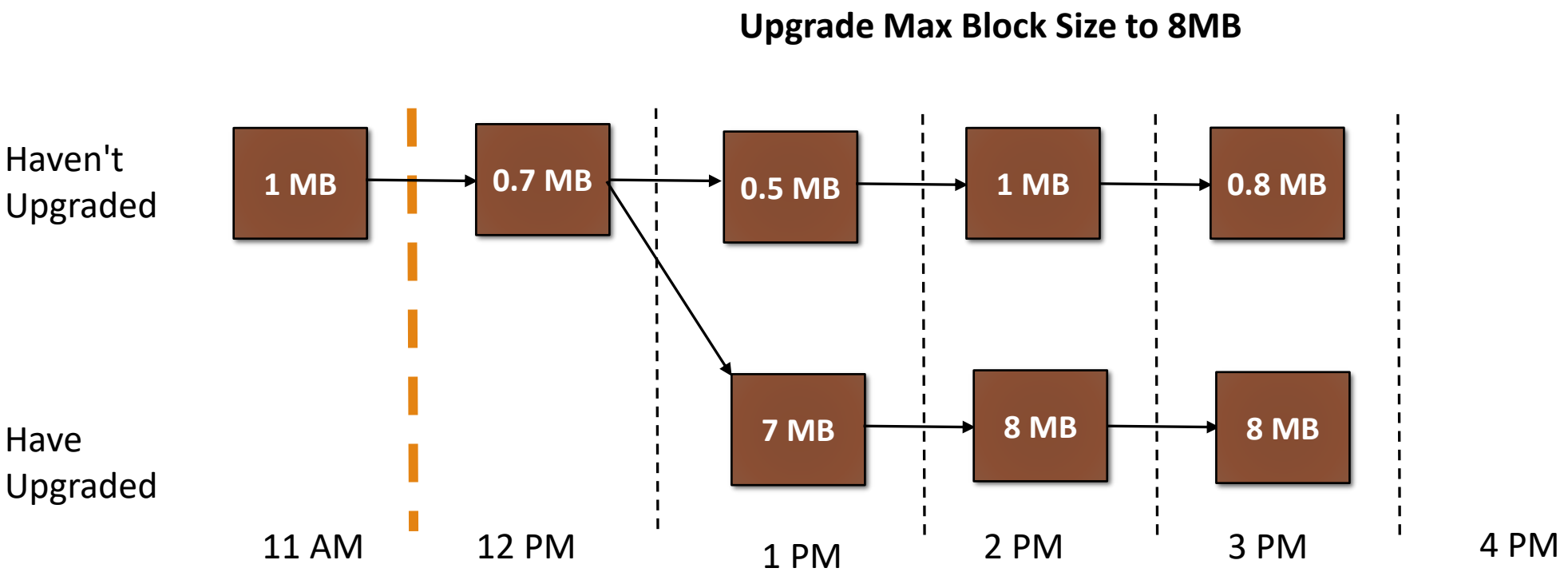
Hard Fork


Upgrade Max Block Size to 8MB
Haven't Upgraded
Have Upgraded
1 MB
0.7 MB
0.5 MB
7 MB
11 AM
12 PM
1 PM
2 PM
3 PM
4 PM

Hard Fork

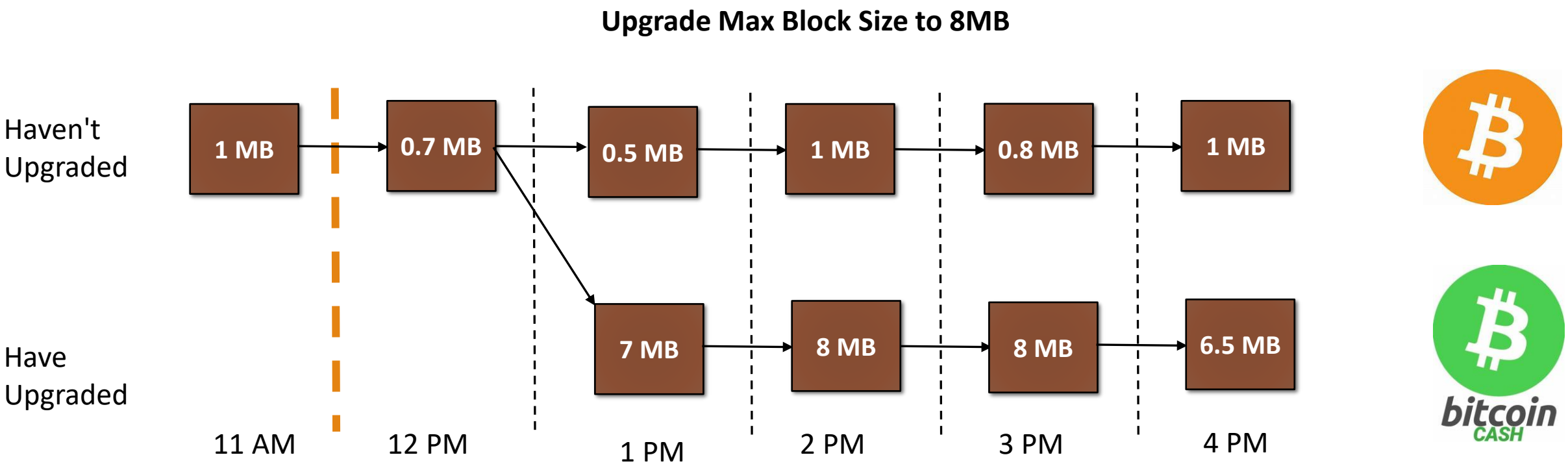

Upgrade Max Block Size to 8MB
Haven't Upgraded
Have Upgraded
1 MB
0.7 MB
0.5 MB
1 MB
7 MB
8 MB
11 AM
12 PM
1 PM
2 PM
3 PM
4 PM

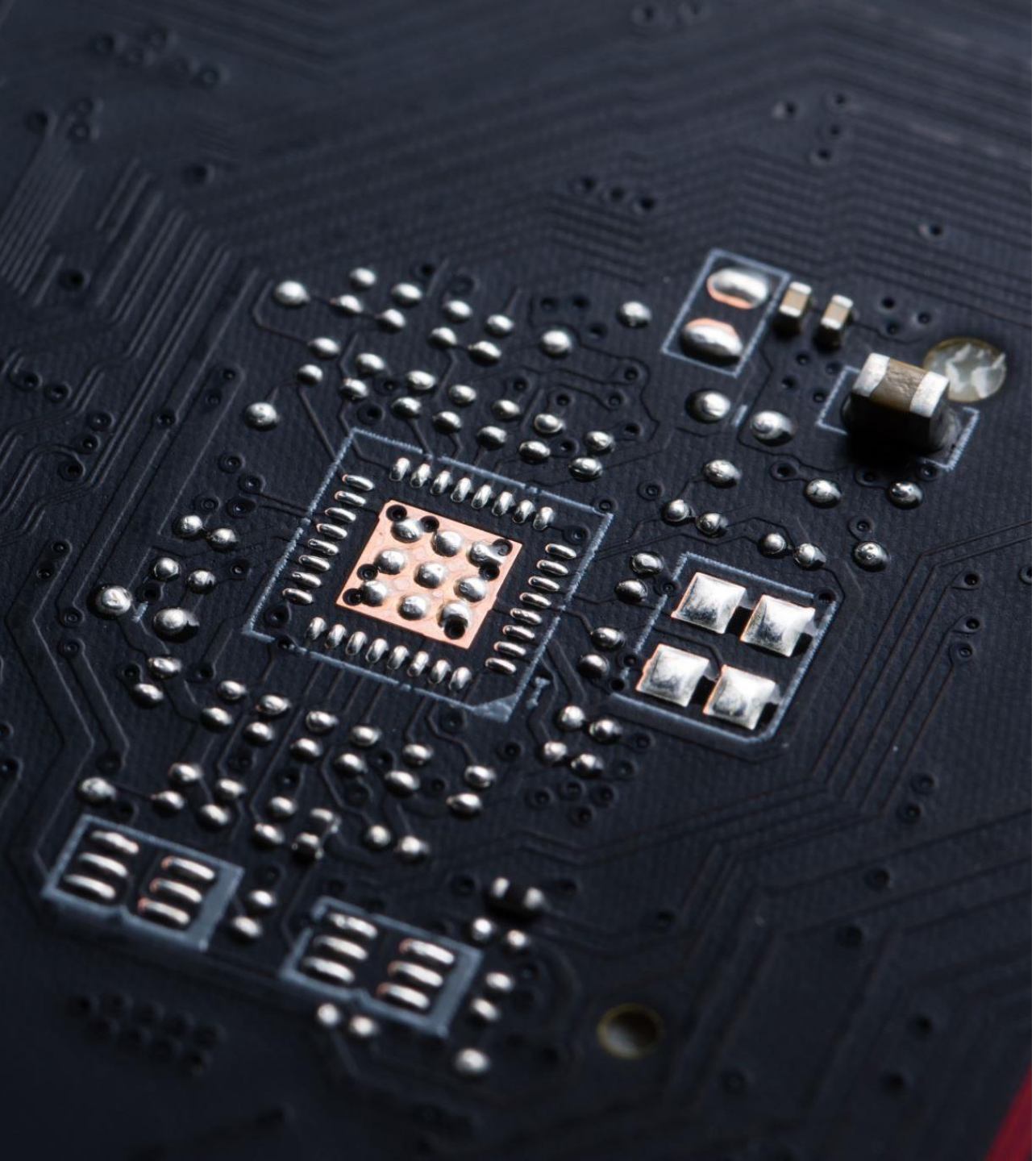
Hard Fork


Upgrade Max Block Size to 8MB
Haven't Upgraded
Have Upgraded
1 MB
0.7 MB
0.5 MB
1 MB
0.8 MB
7 MB
8 MB
8 MB
11 AM
12 PM
1 PM
2 PM
3 PM
4 PM

bitcoin
CASH

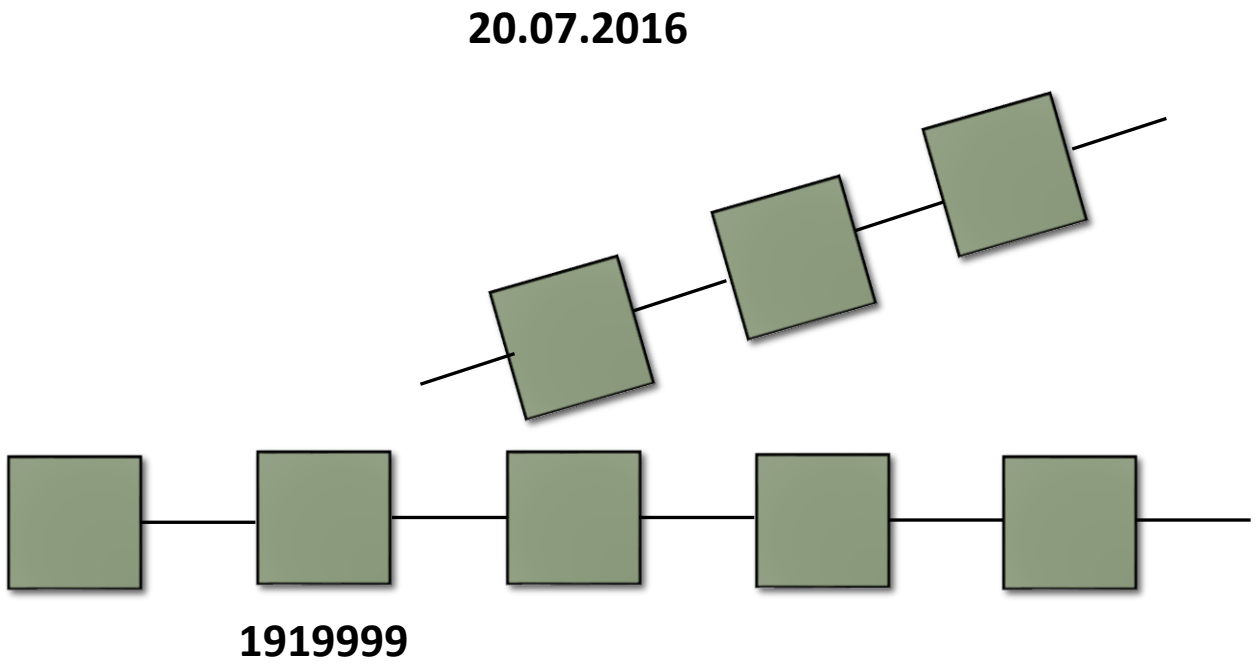
Hard Fork


Upgrade Max Block Size to 8MB
Haven't Upgraded
Have Upgraded
1 MB
0.7 MB
0.5 MB
1 MB
0.8 MB
1 MB
7 MB
8 MB
8 MB
6.5 MB
11 AM
12 PM
1 PM
2 PM
3 PM
4 PM
bitcoin CASH



Soft Fork

Hard Fork



ethereum
classic

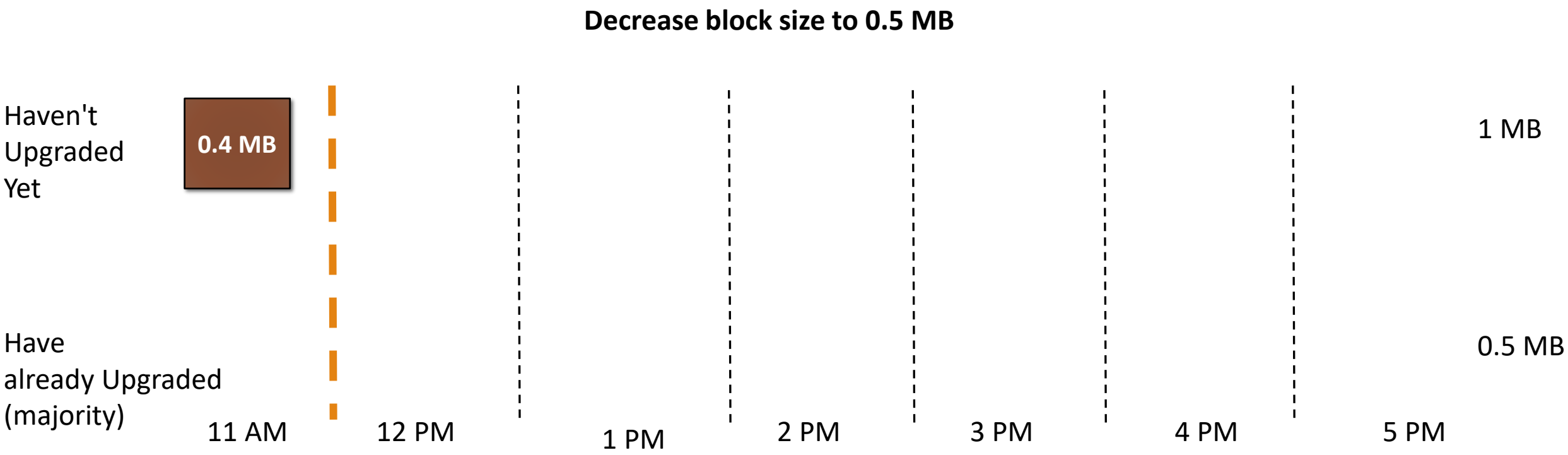
Soft Fork

- Soft forks are a change to the protocol, but the end product remains unchanged.

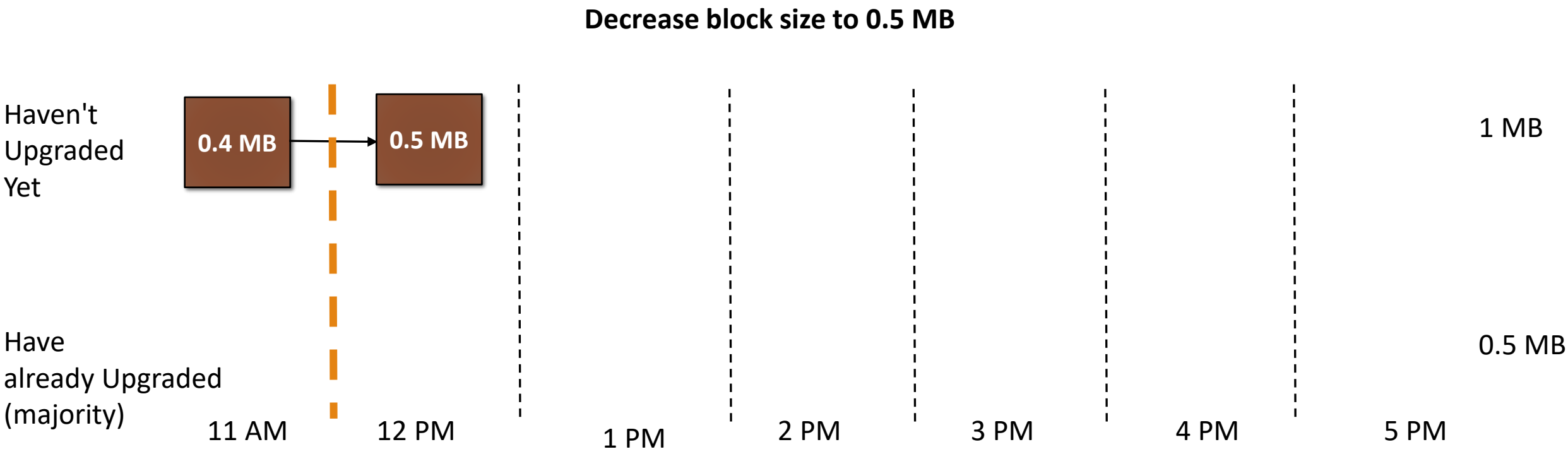
- A soft fork is a *backward-compatible* upgrade, meaning that the upgraded nodes can still communicate with the non-upgraded ones.

- Old nodes(not upgraded nodes) could still validate blocks and transactions (the formatting didn’t break the rules), but they just wouldn’t understand them.

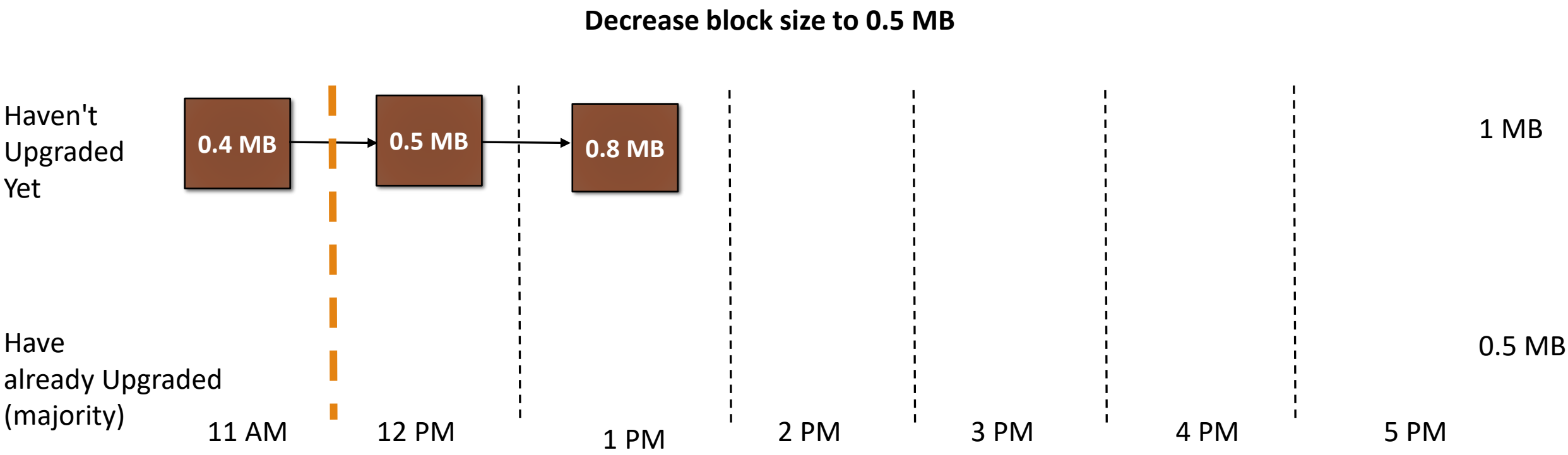
Soft Fork


Decrease block size to 0.5 MB
Haven't Upgraded Yet
Have already Upgraded (majority)
0.4 MB
1 MB
0.5 MB
11 AM
12 PM
1 PM
2 PM
3 PM
4 PM
5 PM

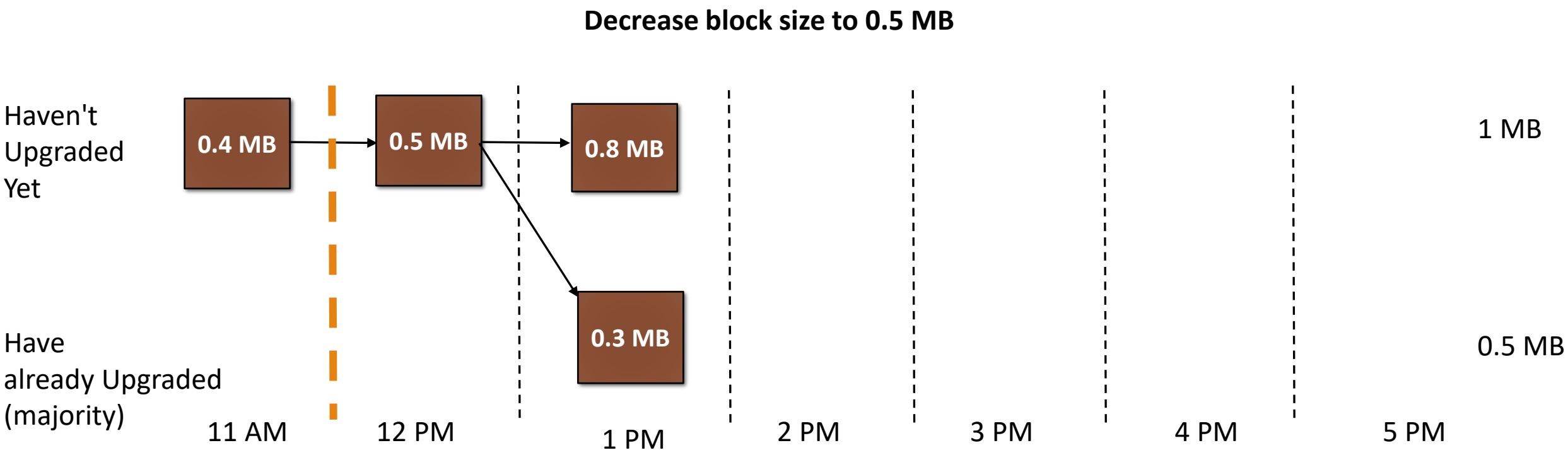
Soft Fork


Decrease block size to 0.5 MB
Haven't Upgraded Yet
Have already Upgraded (majority)
0.4 MB
0.5 MB
1 MB
0.5 MB
11 AM
12 PM
1 PM
2 PM
3 PM
4 PM
5 PM

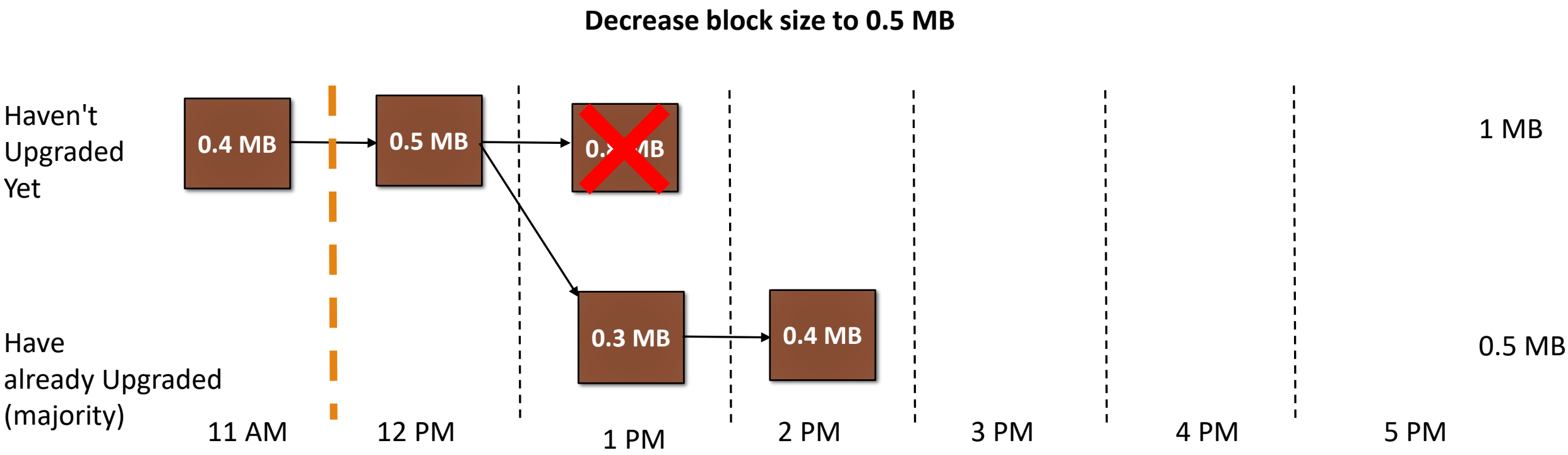
Soft Fork


Decrease block size to 0.5 MB
Haven't Upgraded Yet
Have already Upgraded (majority)
0.4 MB
0.5 MB
0.8 MB
1 MB
0.5 MB
11 AM
12 PM
1 PM
2 PM
3 PM
4 PM
5 PM

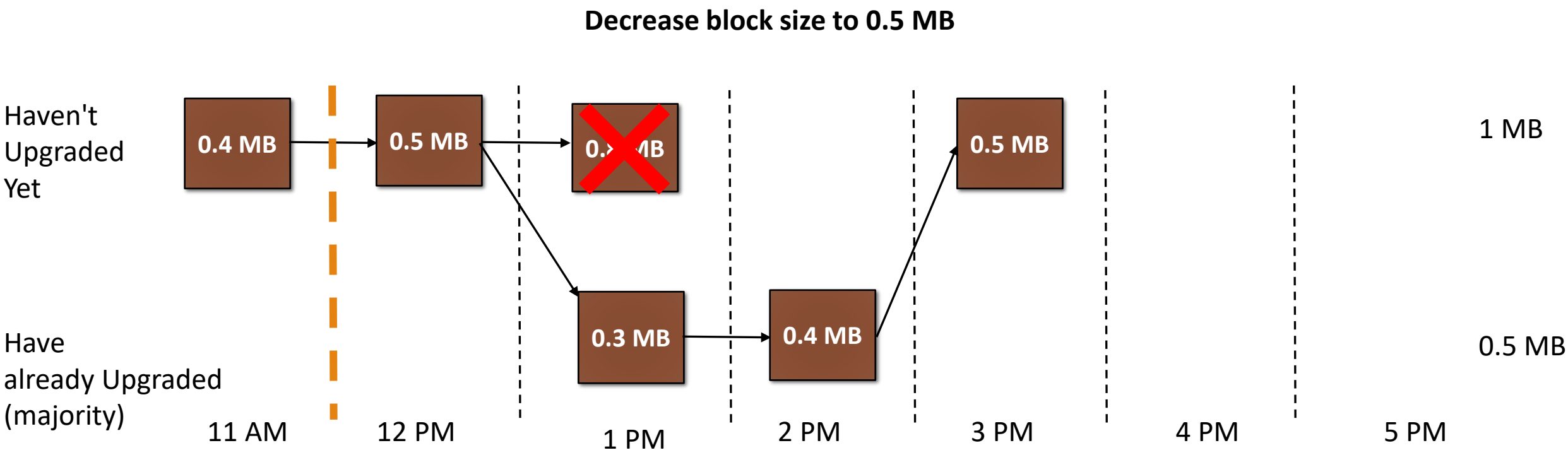
Soft Fork


Decrease block size to 0.5 MB
Haven't Upgraded Yet
Have already Upgraded (majority)
0.4 MB
0.5 MB
0.8 MB
0.3 MB
1 MB
0.5 MB
11 AM
12 PM
1 PM
2 PM
3 PM
4 PM
5 PM

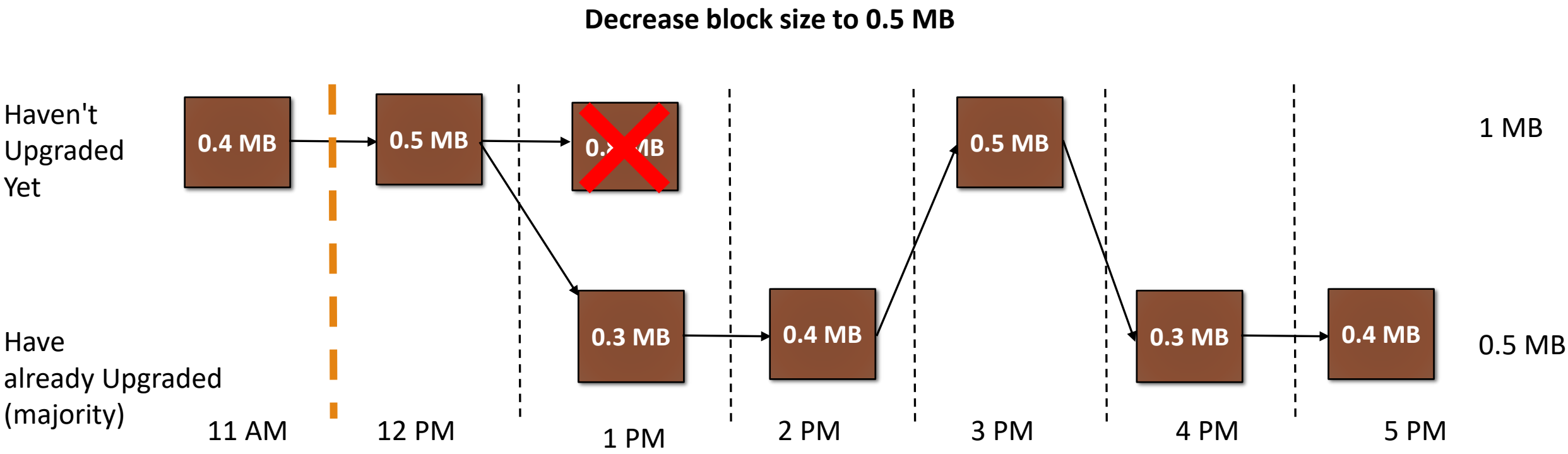
Soft Fork


Decrease block size to 0.5 MB
Haven't Upgraded Yet
Have already Upgraded (majority)
0.4 MB
0.5 MB
0.3 MB
0.4 MB
1 MB
0.5 MB
11 AM
12 PM
1 PM
2 PM
3 PM
4 PM
5 PM

Soft Fork


Decrease block size to 0.5 MB
Haven't Upgraded Yet
Have already Upgraded (majority)
0.4 MB
0.5 MB
0.3 MB
0.4 MB
0.5 MB
1 MB
0.5 MB
11 AM
12 PM
1 PM
2 PM
3 PM
4 PM
5 PM

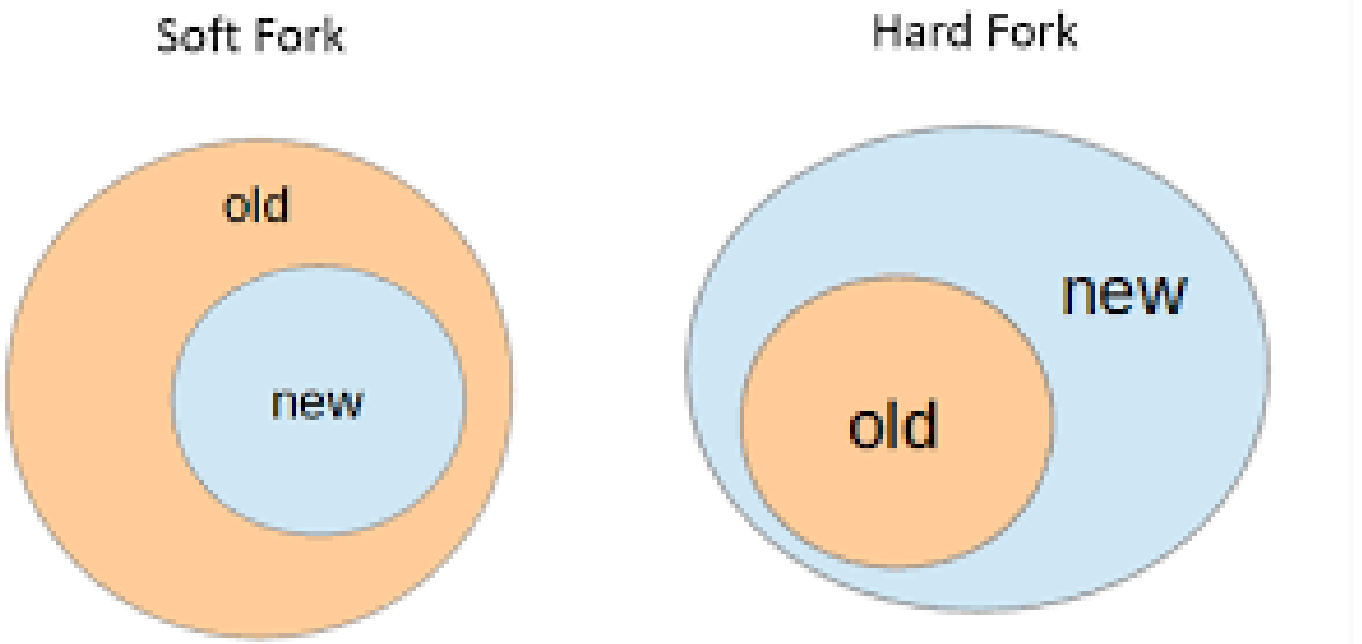
Soft Fork


Decrease block size to 0.5 MB
Haven't Upgraded Yet
Have already Upgraded (majority)
0.4 MB
0.5 MB
0.3 MB
0.4 MB
0.5 MB
0.3 MB
0.4 MB
1 MB
0.5 MB
11 AM
12 PM
1 PM
2 PM
3 PM
4 PM
5 PM

Soft Fork

- There is a link between the two, thus both communities will participate in the mining
- However, due to the majority, the longest chain wins
- I.e., **Computer Games**, games are upgraded, still the old version runs properly
- The new features will not be in the old game. However, to get new features, the old one will also be upgraded

Soft Fork vs. Hard Fork



ICO's

Initial Public Offering (IPO)

Jeff Bezos
Founder of Amazon

Initial Capital

Shares

Services & Products

Profit

Cash

Shares

Initial Public Offering (IPO)

- An IPO is a public offering in which shares of a company are sold to investors
- A company issues shares to the public for the first time

IPO Difficulties

- Preparation for the IPO is expensive, complex, and time-consuming
- It can require the hiring of lawyers, investment bankers, and accountants
- It requires a lot of legal work and documentation
- A majority shareholder controls the company

Initial Coin Offering (ICO)

Initial Capital

Shares

Services & Products

Profit

Token

Cash(Bitcoin/Ether)

Initial Coin Offering (ICO)

- ICO is an unregulated means for funds raising in a cryptocurrency venture
- Investors pay (Bitcoins/ Ether) and in return they get token
- These tokens later will be able to buy things and for trading

ICO Benefits:

- Unlike IPOs investors in ICOs are not entitled to hold a stake in the company and participate in internal management decisions, thus do not have any control over the company
- ICOs do not require legal work and documentation