

# Blockchain Workshop

Learn Blockchain by Building One

Presenter: Samaneh Miri  
July 30, 2021

# Outline

- What is a Blockchain?



# Outline

- What is a Blockchain?
- Hash Cryptography



# Outline

- What is a Blockchain?
- Hash Cryptography
- Immutable Ledger





# Outline

- What is a Blockchain?
- Hash Cryptography
- Immutable Ledger
- Distributed P2P Network



# Outline

- What is a Blockchain?
- Hash Cryptography
- Immutable Ledger
- Distributed P2P Network
- Mining



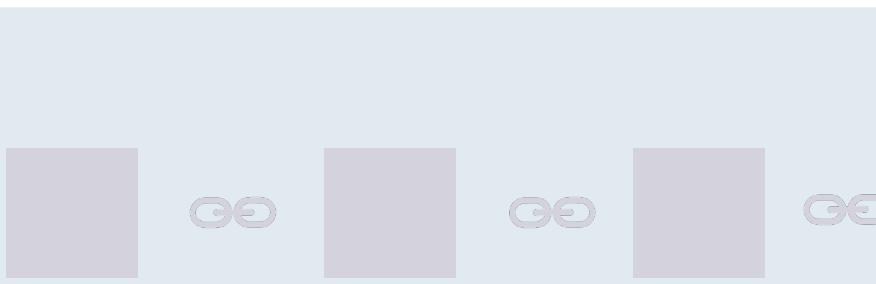
# Outline

- What is a Blockchain?
- Hash Cryptography
- Immutable Ledger
- Distributed P2P Network
- Mining
- Consensus Protocol



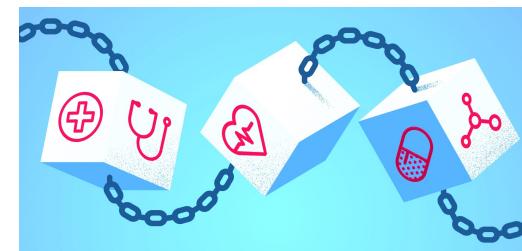
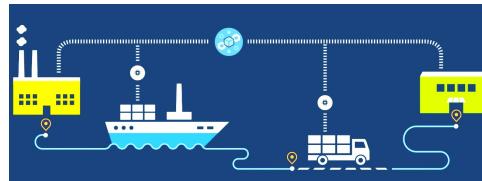
# What is a Blockchain?

A blockchain is a growing list of records, called blocks, that are linked using cryptography (Wikipedia).



# Blockchain Applications

- The blockchain technology first came into the spotlight through bitcoin.
- The technology is not only for cryptocurrencies.
- Features:
  - Immutability
  - Decentralized
  - Enhanced Security
  - Faster Settlement



# What is a Blockchain?



Stuart Haber



W. Scott Stornetta

## How to Time-Stamp a Digital Document\*

Stuart Haber  
stuart@bellcore.com

W. Scott Stornetta  
stornetta@bellcore.com

Year: 1991

Goal: to implement a system where document timestamps could not be tampered with.



# What is a Blockchain?

## Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto  
[satoshi@gmx.com](mailto:satoshi@gmx.com)  
[www.bitcoin.org](http://www.bitcoin.org)

Year introduced: 2008

Year Implemented: 2009

Goal: to timestamp blocks without requiring them to be signed by a trusted party and introducing a difficulty parameter to stabilize rate with which blocks are added to the chain.

# What is a Blockchain?

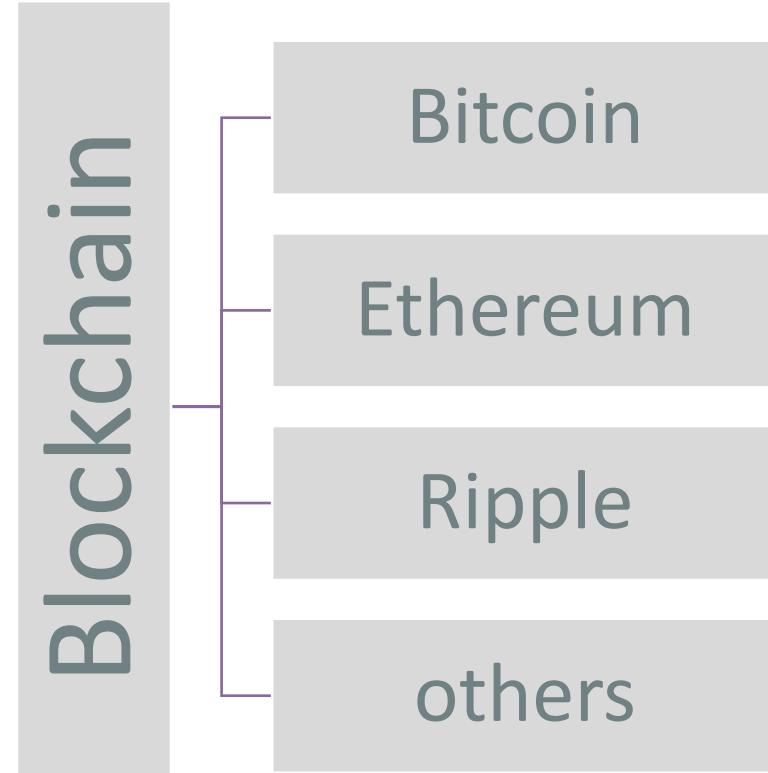
Technology

Blockchain

Protocol

Bitcoin

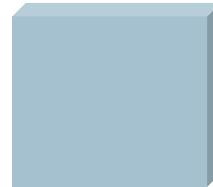
# What is a Blockchain?



# What is a Blockchain?

A blockchain is a growing list of records, called blocks, that are linked using cryptography (Wikipedia).

Block



1. Index:
2. Timestamp:
3. Data:
4. Prev. Hash:
5. Hash:

# What is a Blockchain?

A blockchain is a growing list of records, called blocks, that are linked using cryptography (Wikipedia).

Block



1. Index:
2. Timestamp:
3. Data:
4. Prev. Hash:
5. Hash:

Hash of data is like a fingerprint of a human being.

# What is a Blockchain?

- A sequence of **linked blocks** creates a **chain**.

Genesis Block



Index: 1

Timestamp:

Data:

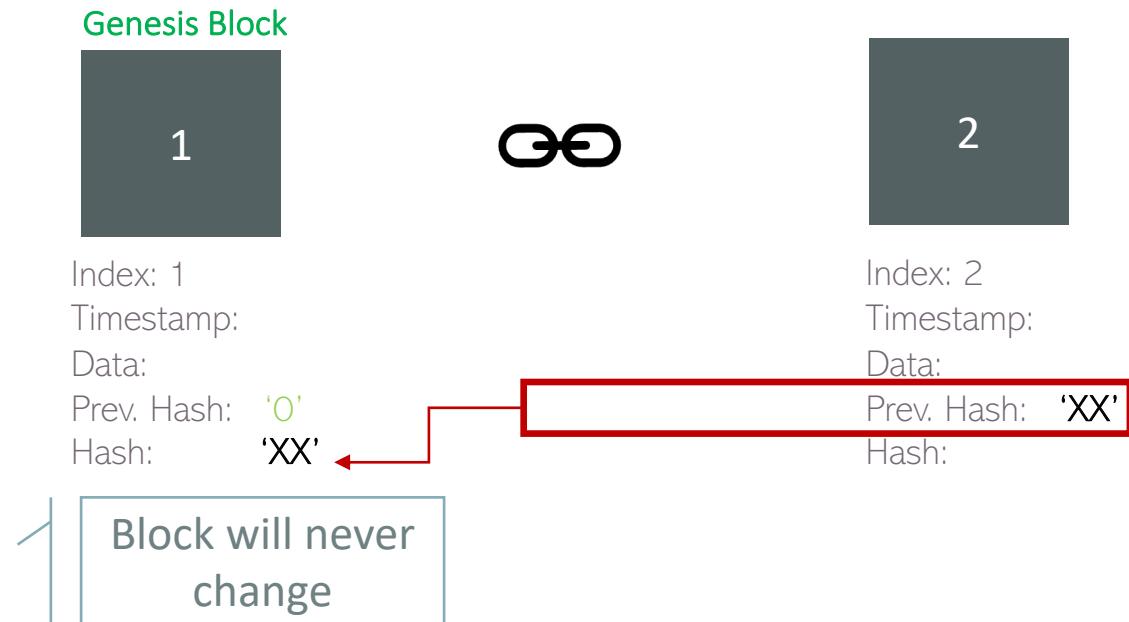
Prev. Hash: '0'

Hash:

Block will never  
change

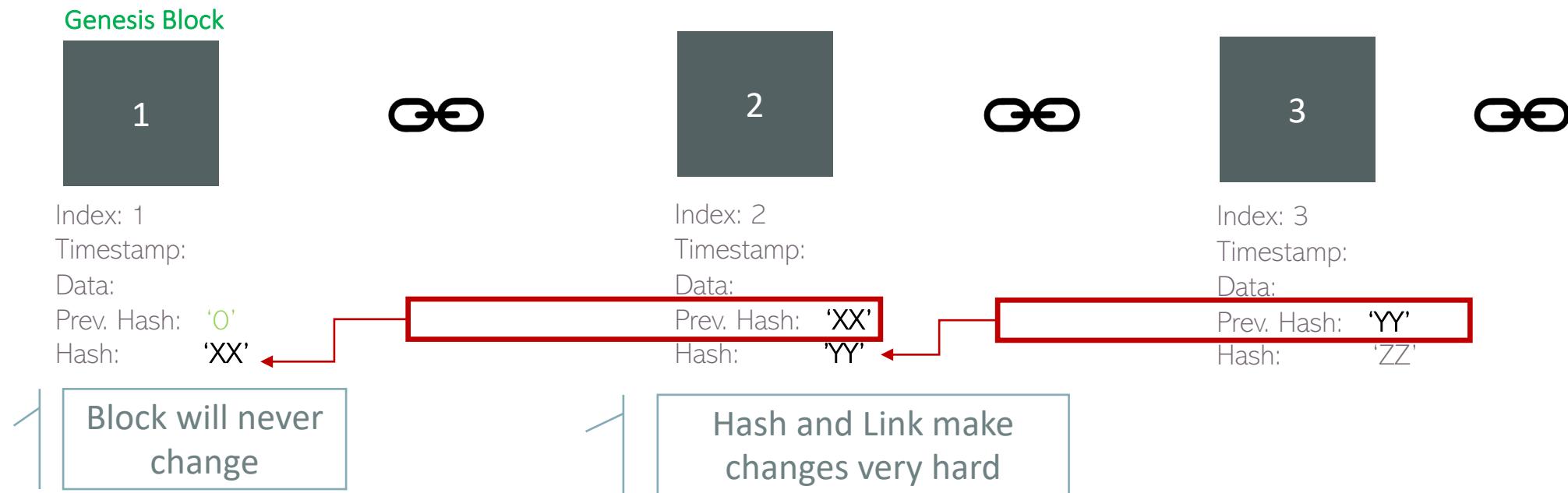
# What is a Blockchain?

- A sequence of **linked blocks** creates a **chain**.



# What is a Blockchain?

- A sequence of **linked blocks** creates a **chain**.





Hash Cryptography

Immutable Ledger

Distributed P2P Network

Mining

Consensus Protocol

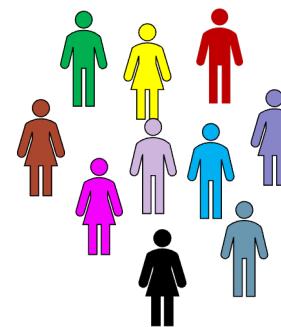


# Hash Cryptography

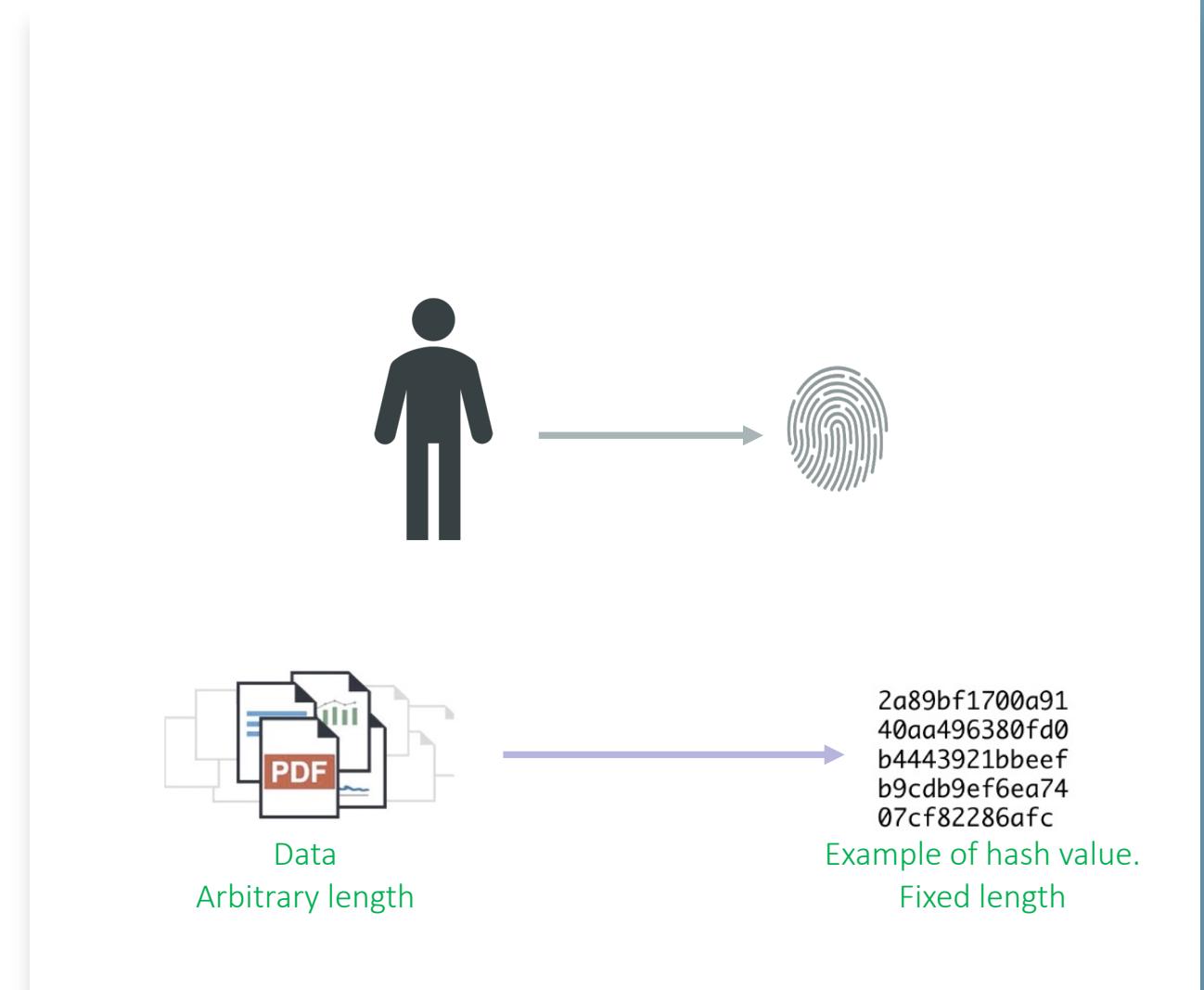
A hash function is a function which takes an arbitrary length input and produces **a fixed length** “fingerprint” string.

# Hash Value

Different people have different fingerprints.



# Hash Value



# SHA256

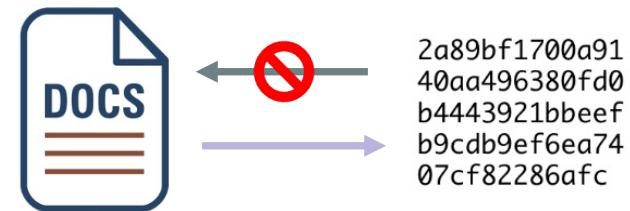
- Several cryptocurrencies use Secure Hash Function (SHA) family for verifying transactions or proof of work.
- Bitcoin uses SHA256.
- SHA256 is always 256 bits long, equivalent to 64 bytes in hexadecimal string format.



<https://demoblockchain.org/hash>

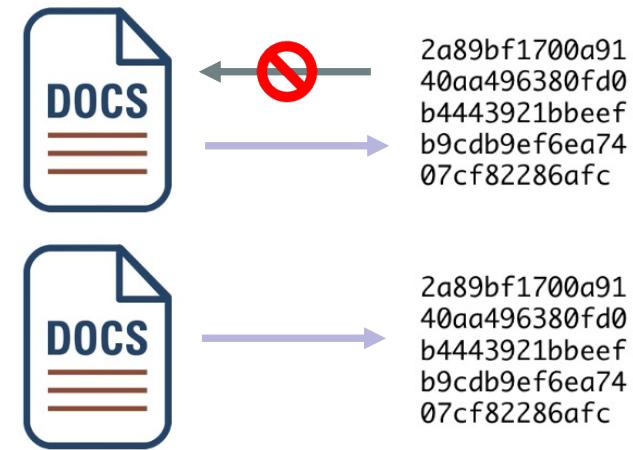
# SHA256 Hash: Characteristics

- One-way



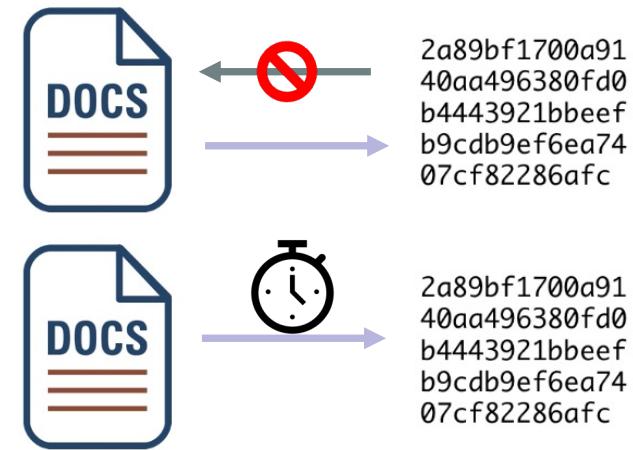
# SHA256 Hash: Characteristics

- One-way
- Deterministic



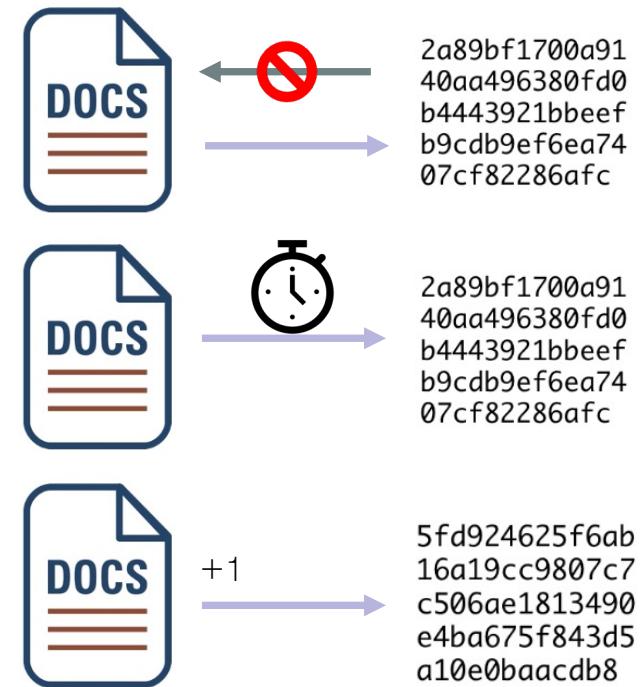
# SHA256 Hash: Characteristics

- One-way
- Deterministic
- Fast Computation



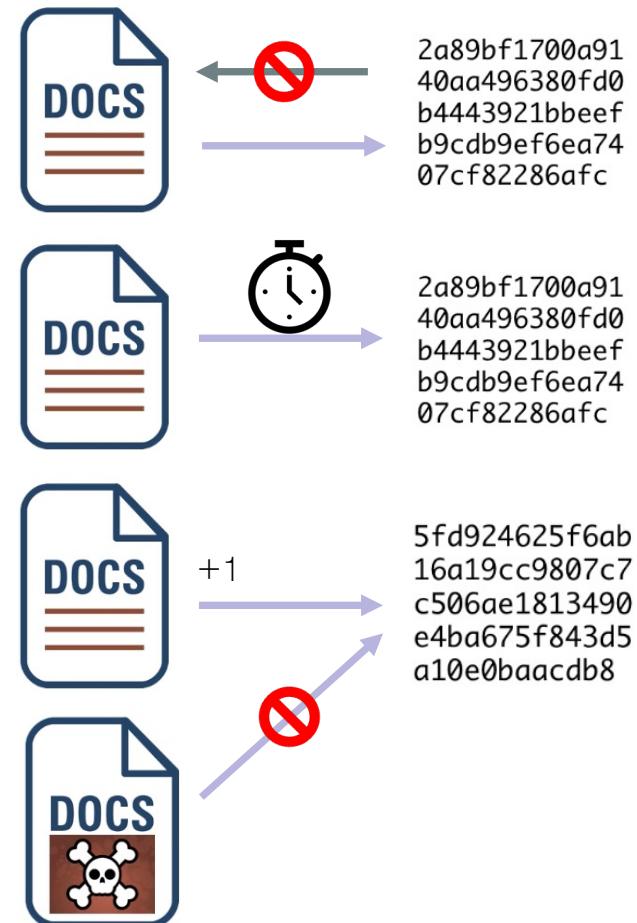
# SHA256 Hash: Characteristics

- One-way
- Deterministic
- Fast Computation
- Avalanche Effect



# SHA256 Hash: Characteristics

- One-way
- Deterministic
- Fast Computation
- Avalanche Effect
- Must withstand collision



# Blockchain Components

Hash Cryptography

Immutable Ledger

Distributed P2P Network

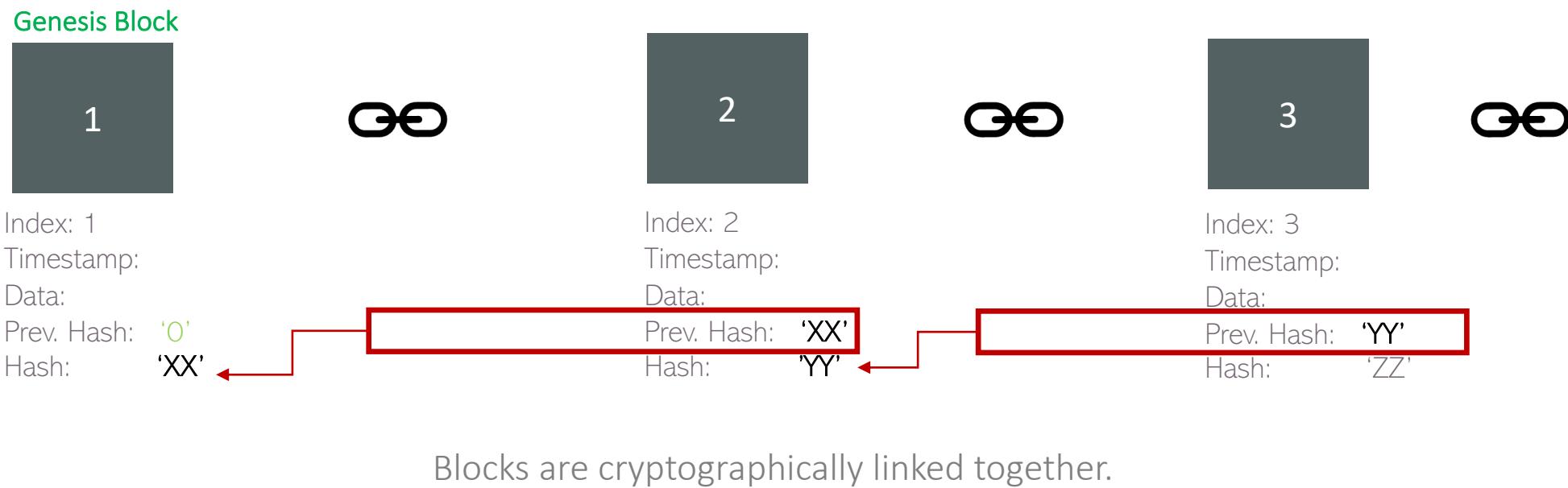
Mining

Consensus Protocol

# Immutable Ledger

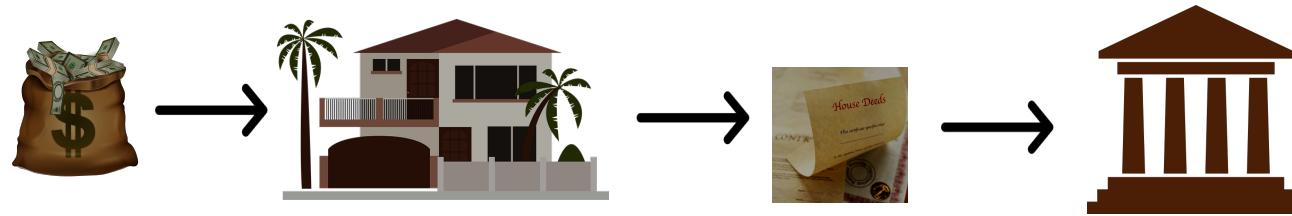
An Immutable Ledger is a record that cannot be changed.

# Immutable Ledger



# Immutable Ledger

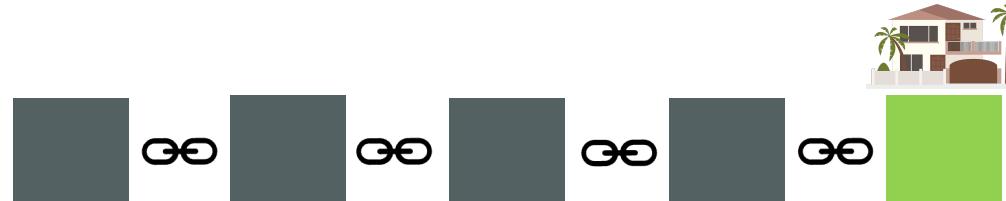
- Buying a house: from payment to a deed registration



- Traditional ledger

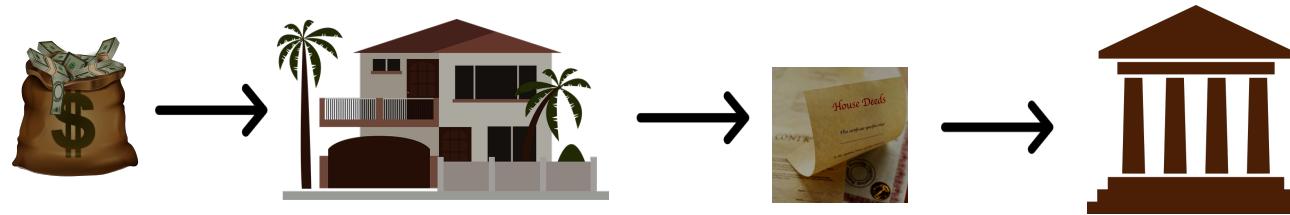


- Blockchain



# Immutable Ledger

- Buying a house: from payment to a deed registration



- Traditional ledger

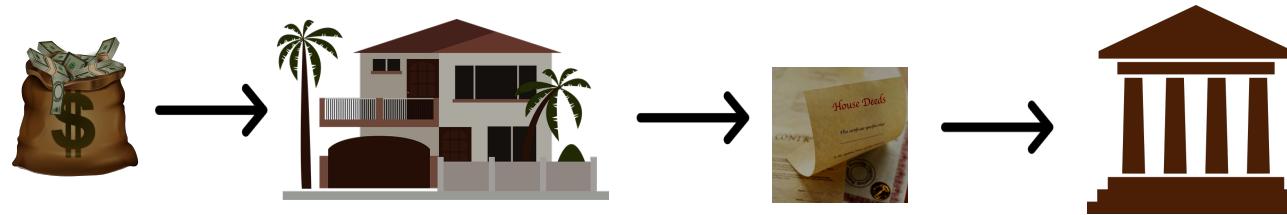


- Blockchain



# Immutable Ledger

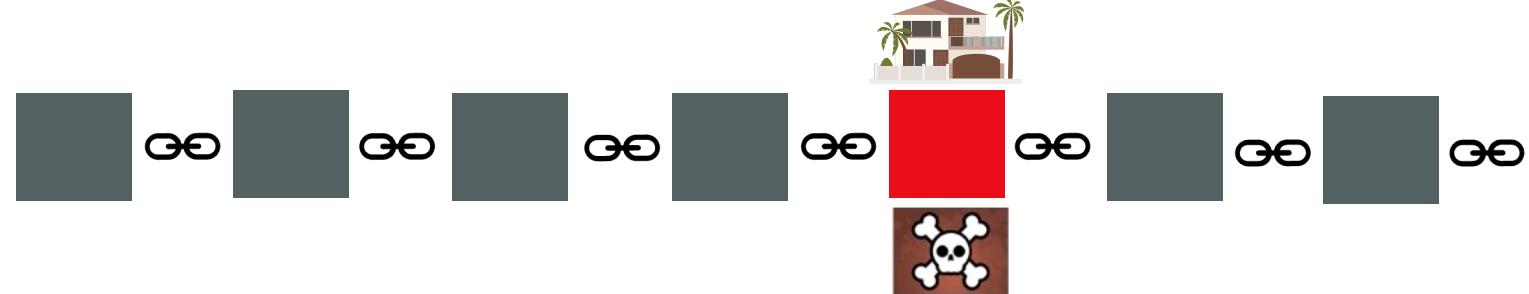
- Buying a house: from payment to a deed registration



- Traditional ledger

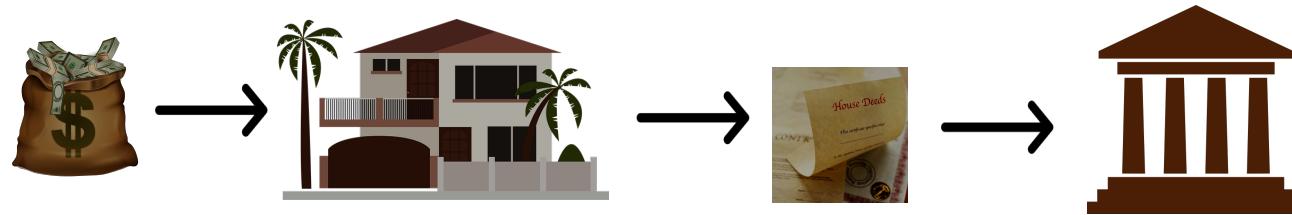


- Blockchain



# Immutable Ledger

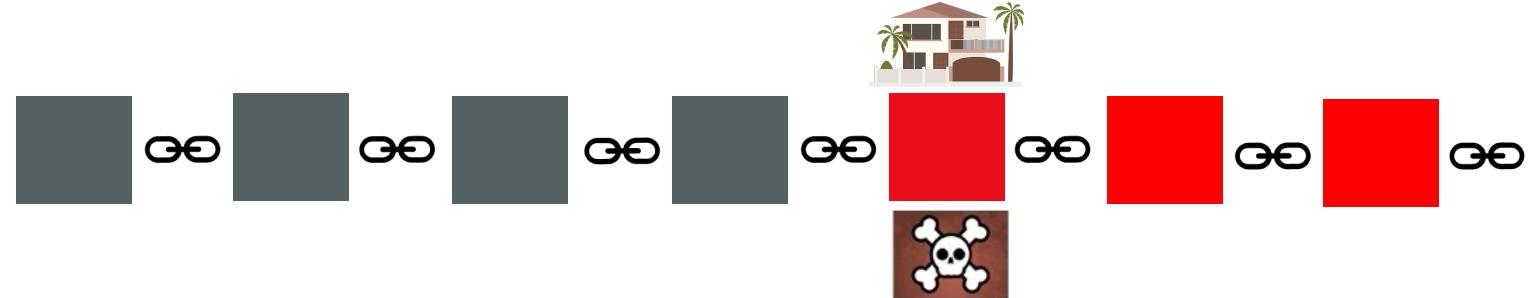
- Buying a house: from payment to a deed registration



- Traditional ledger



- Blockchain



# Blockchain Components

Hash Cryptography

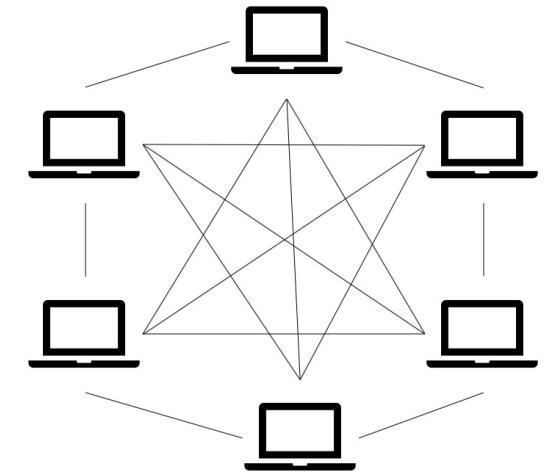
Immutable Ledger

Distributed P2P Network

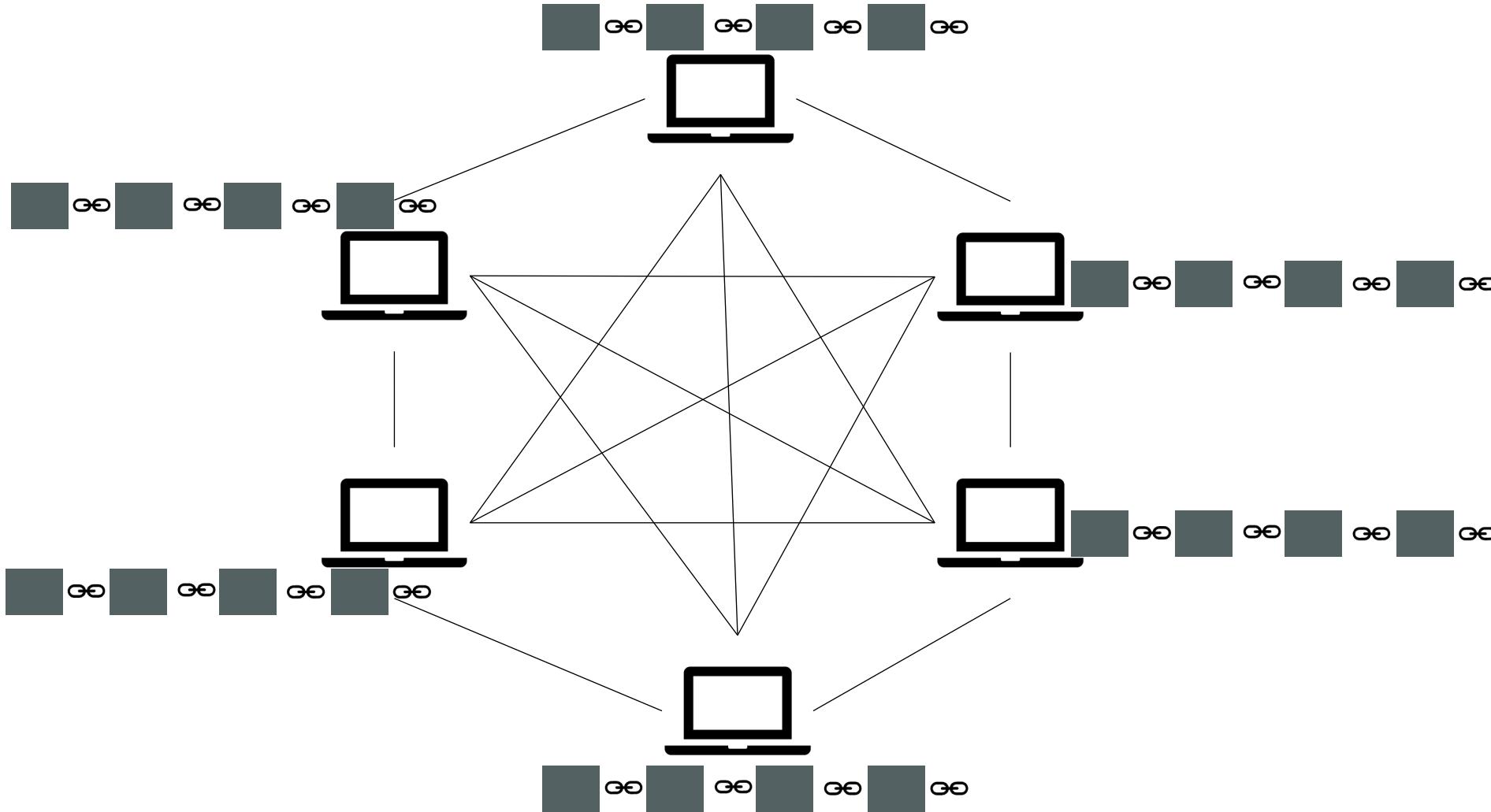
Mining

Consensus Protocol

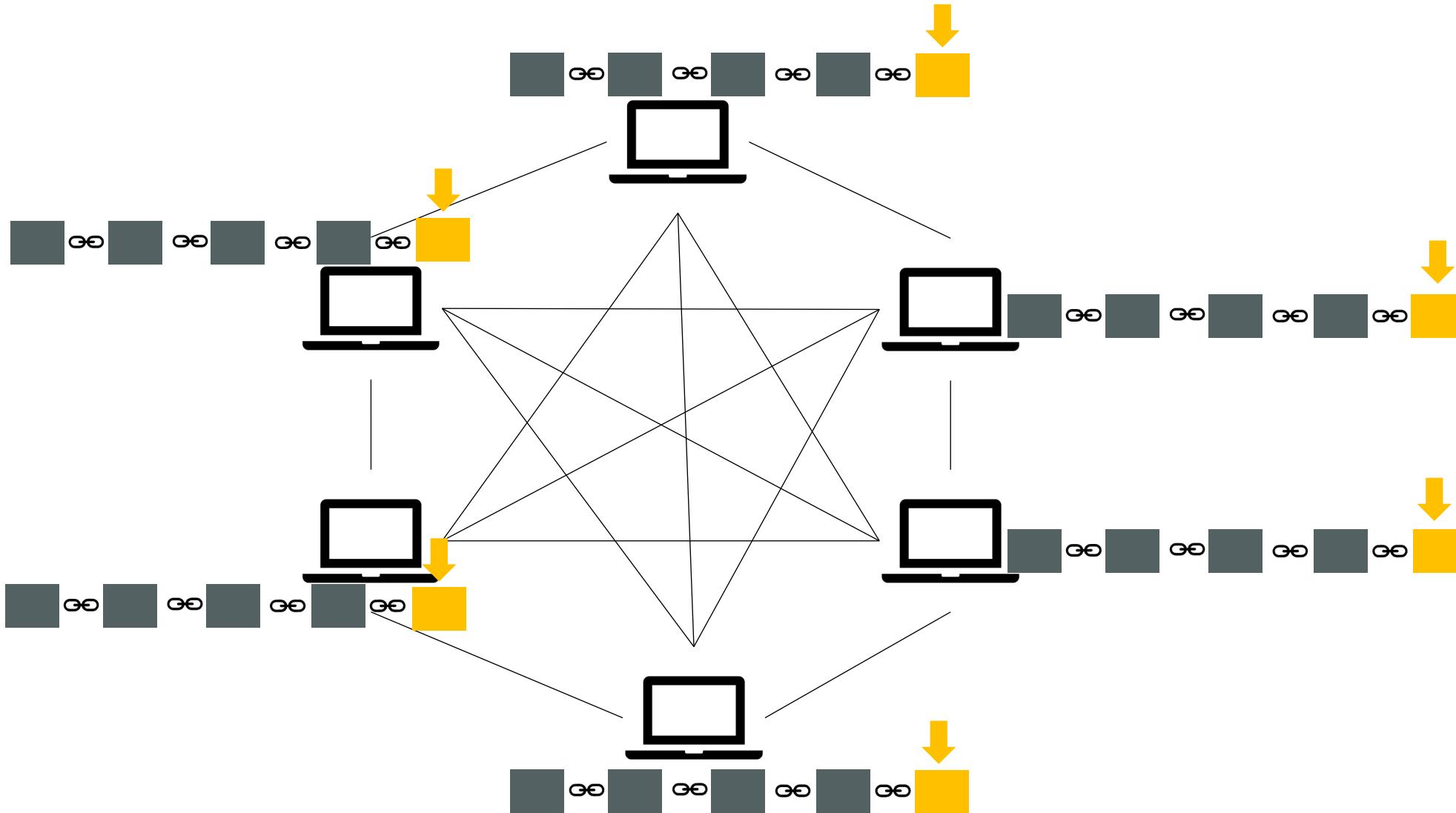
# Distributed P2P Network



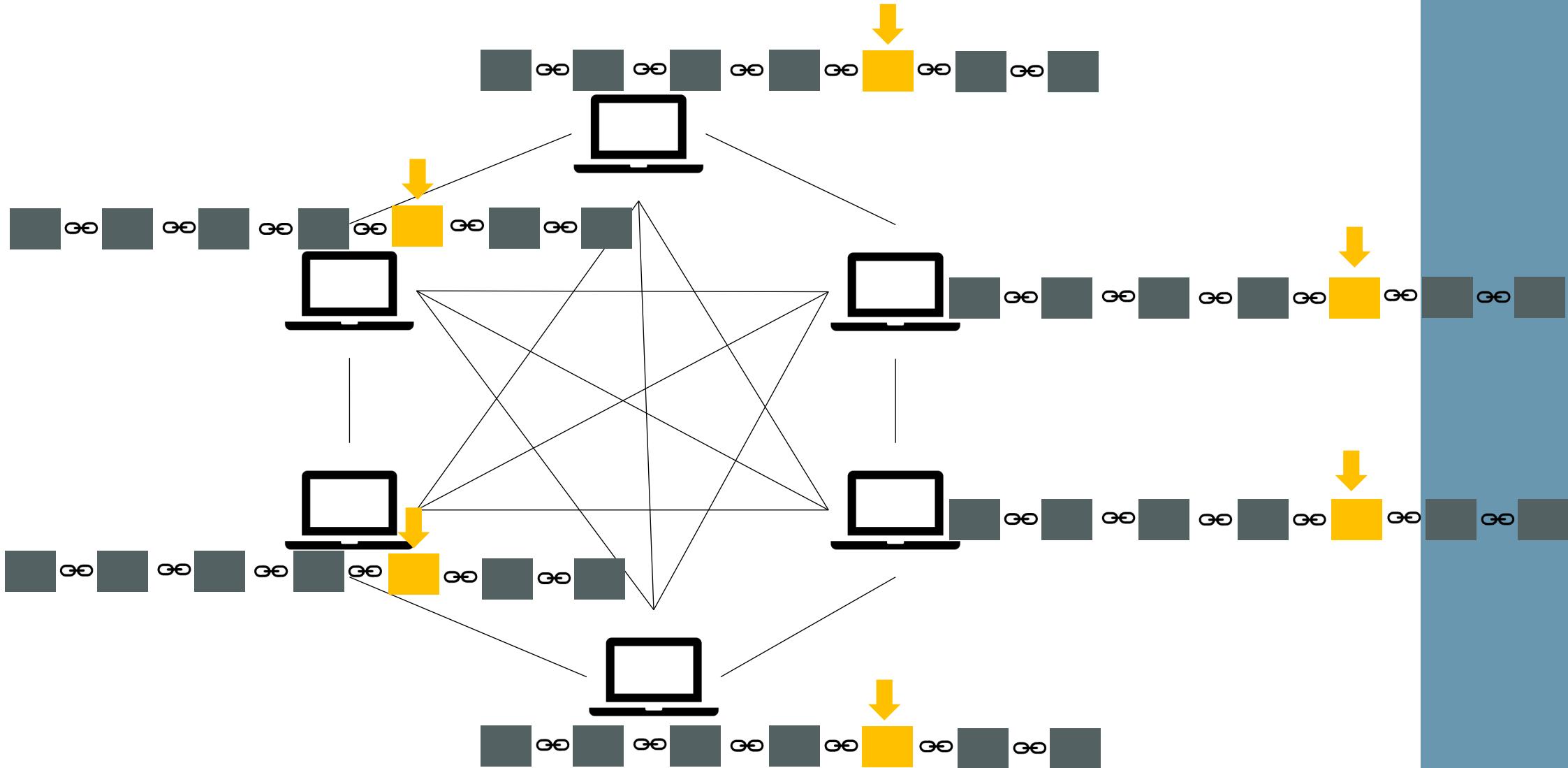
# Distributed P2P Network



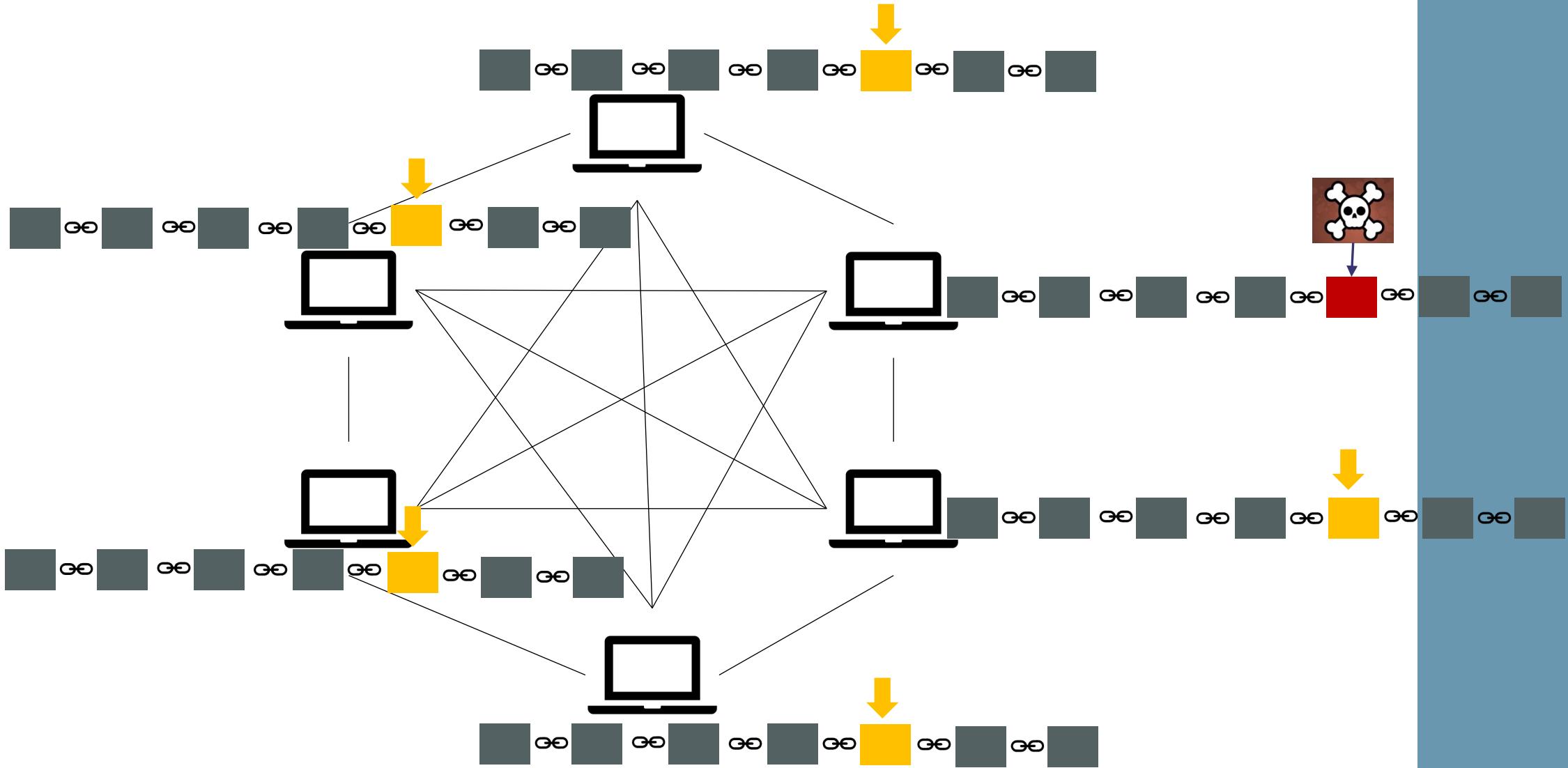
# Distributed P2P Network



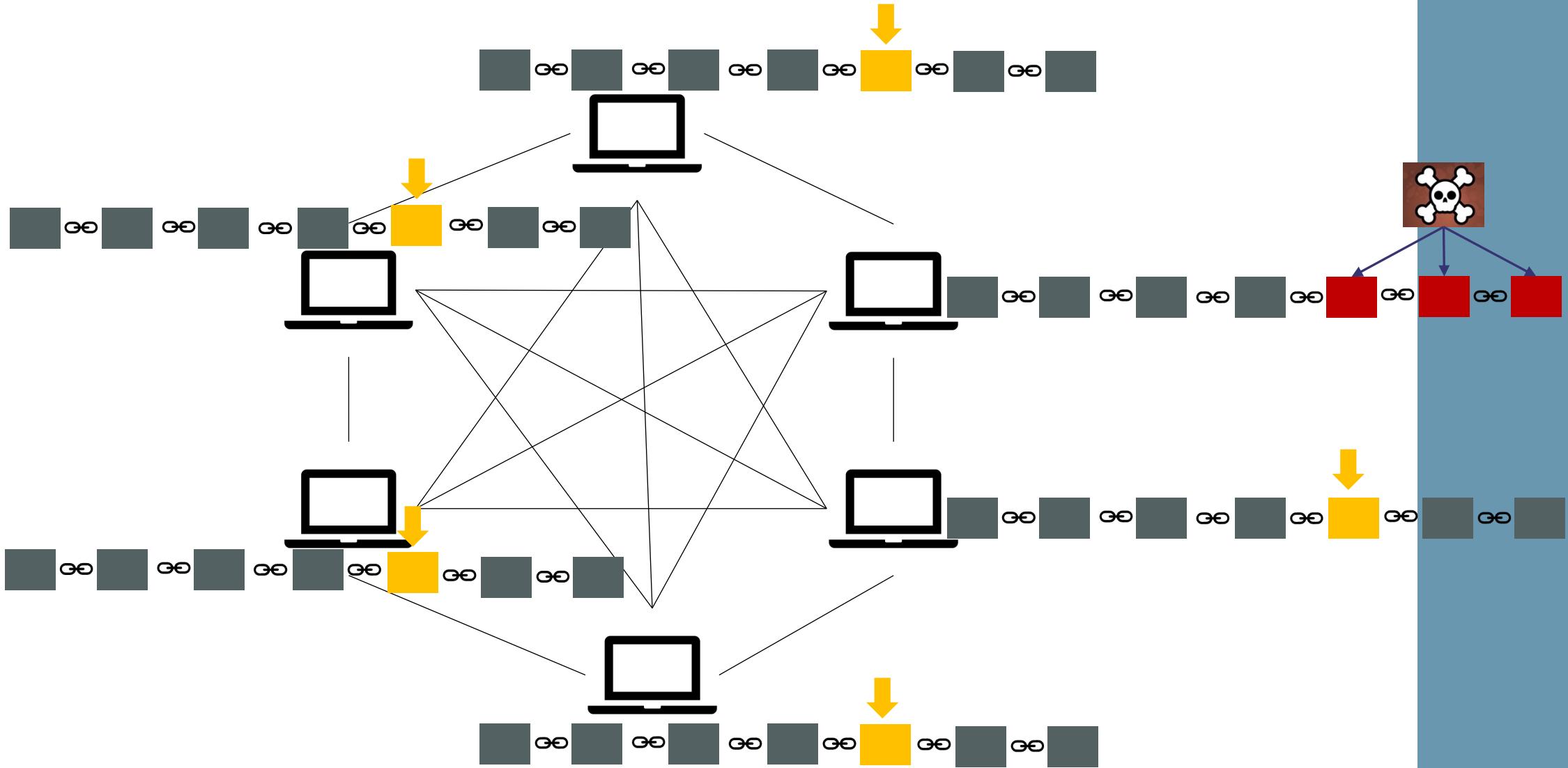
# Distributed P2P Network



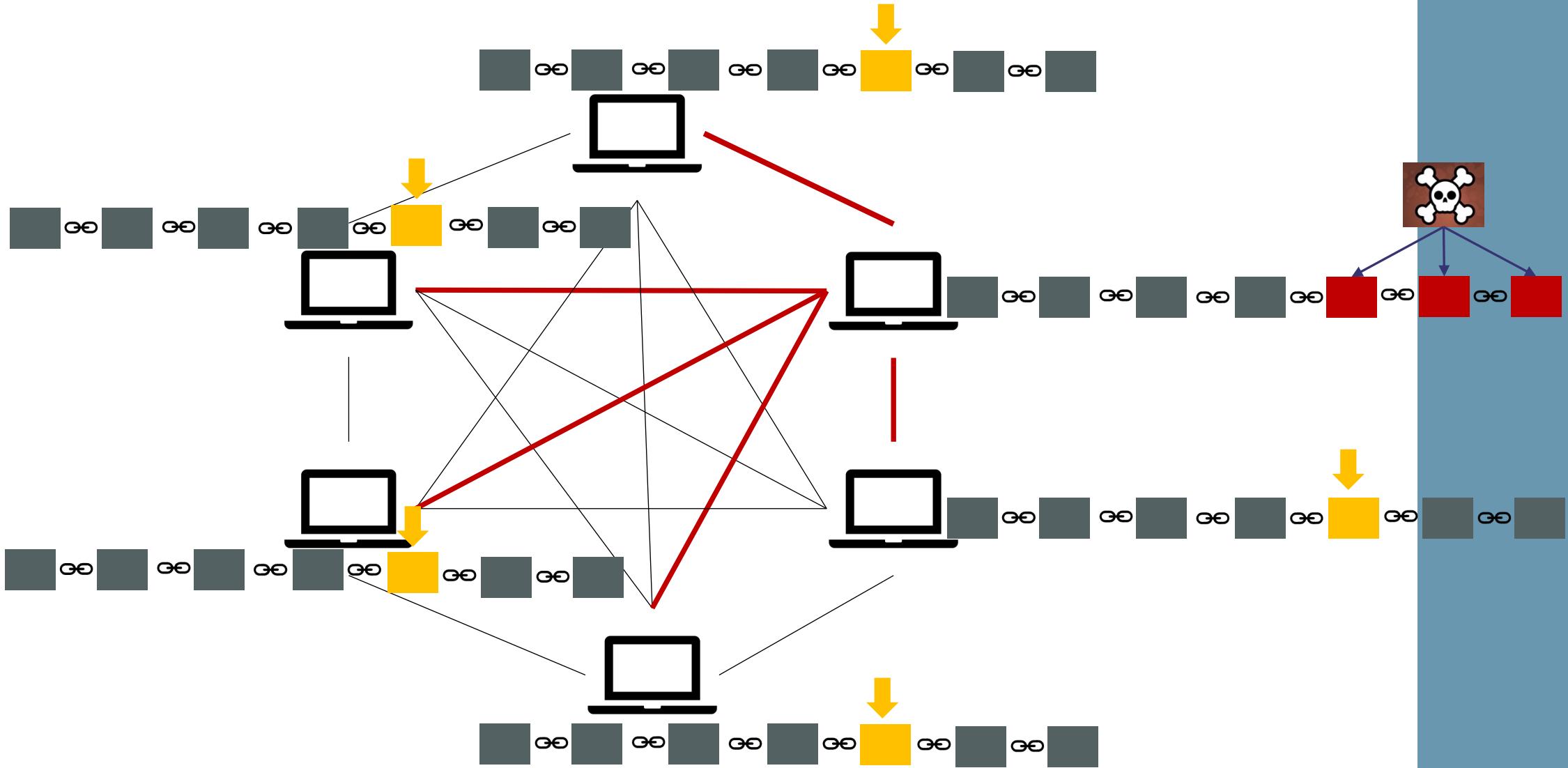
# Distributed P2P Network



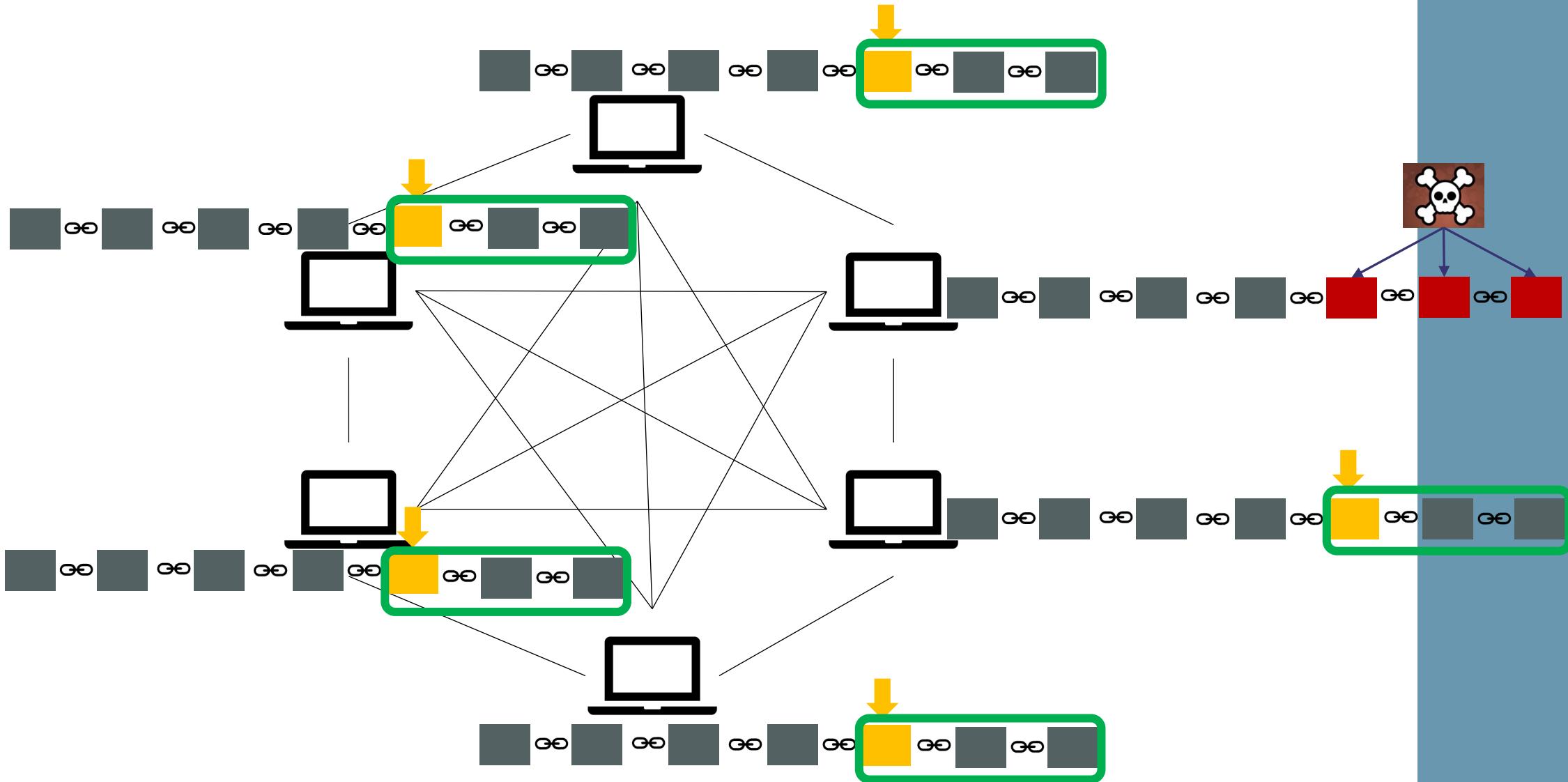
# Distributed P2P Network



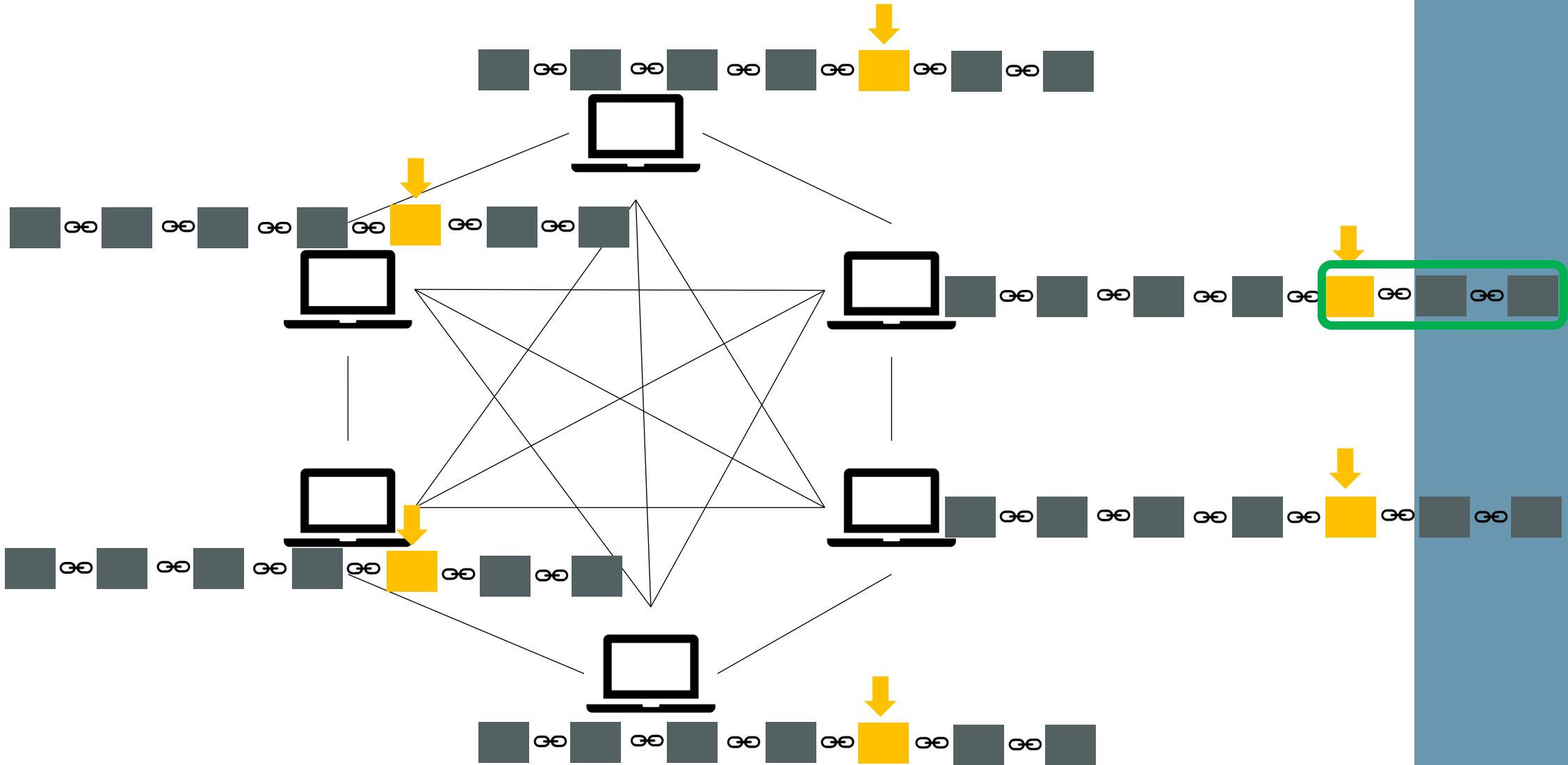
# Distributed P2P Network



# Distributed P2P Network



# Distributed P2P Network



# Blockchain Components

Hash Cryptography

Immutable Ledger

Distributed P2P Network

Mining

Consensus Protocol

# Mining

Mining is all about miners using their time and processing power to solve cryptographically hard puzzles.

# How Mining Works



Block #3

Data:

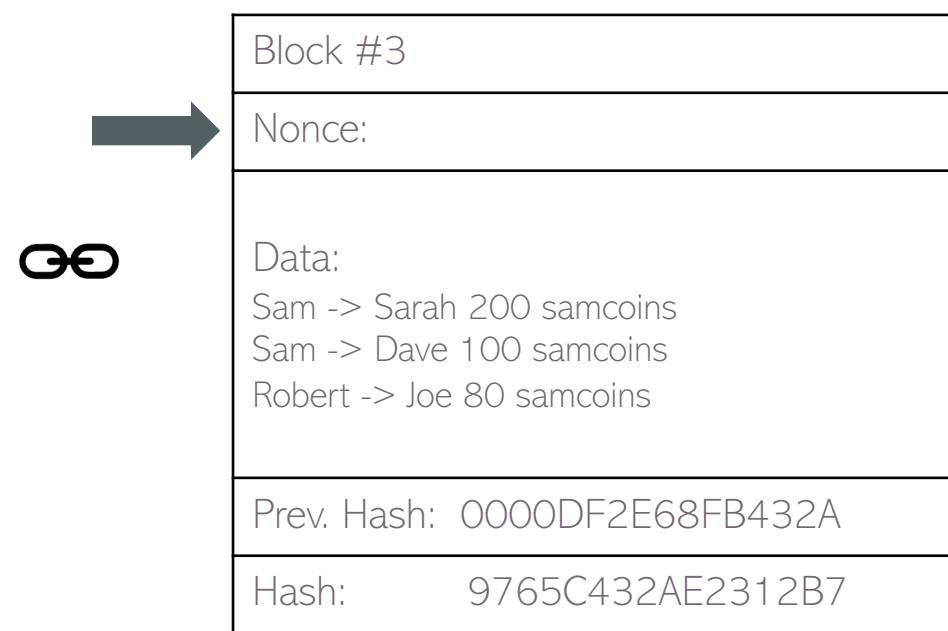
Sam -> Sarah 200 samcoins  
Sam -> Dave 100 samcoins  
Robert -> Joe 80 samcoins

Prev. Hash: 0000DF2E68FB432A

Hash: 9765C432AE2312B7

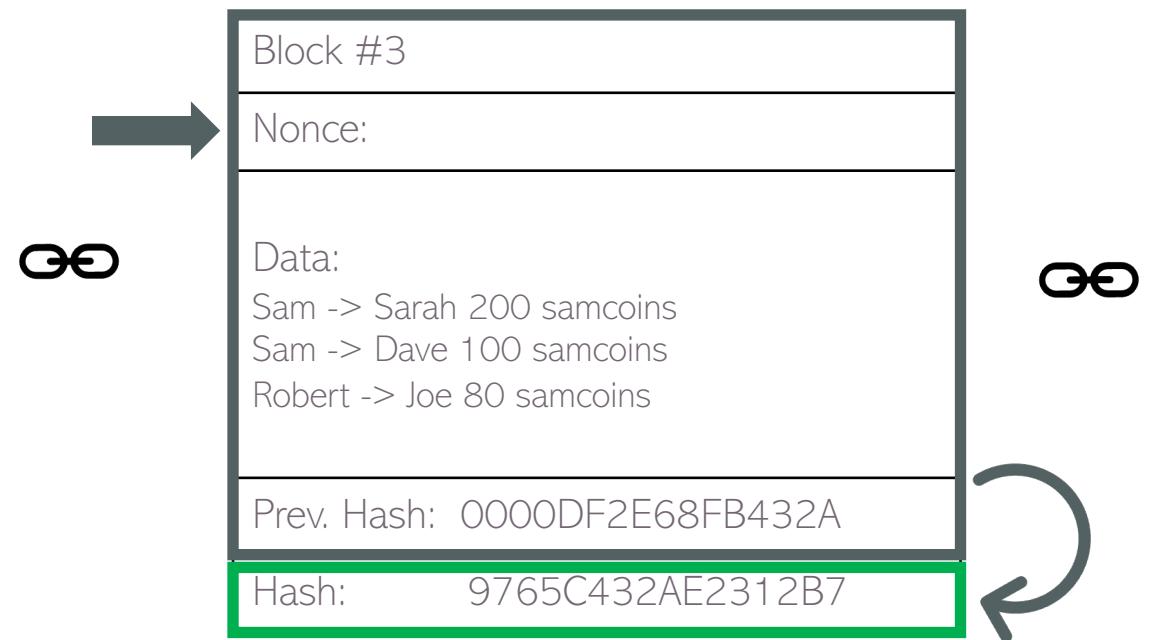


# Nonce



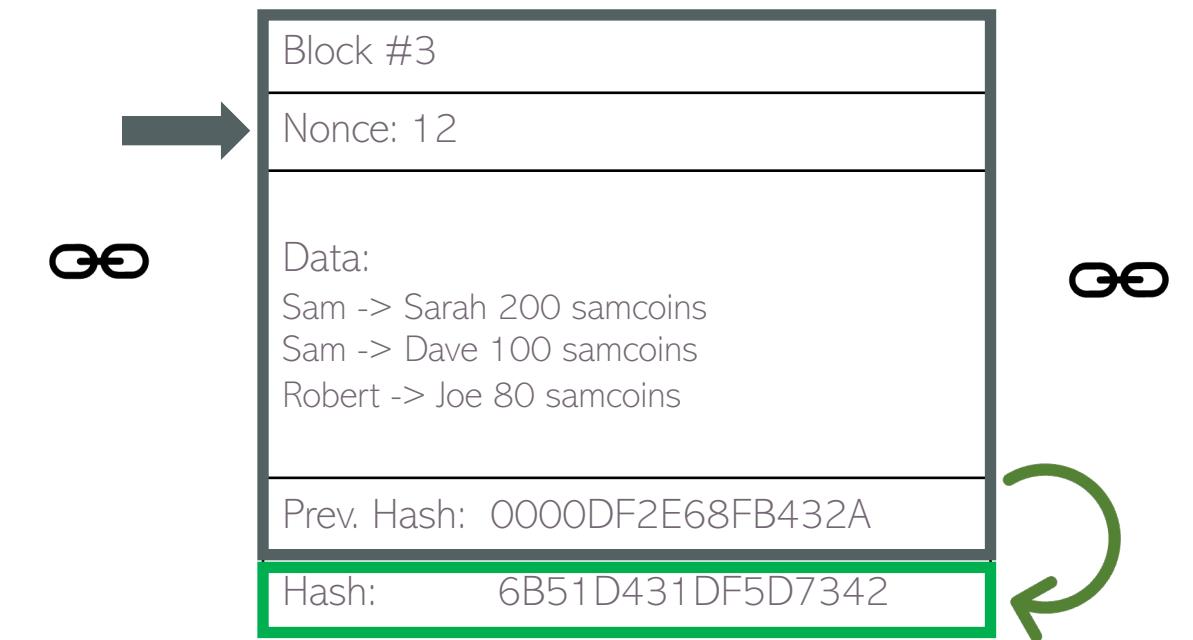
The nonce value helps miners to solve the puzzle.

# Nonce

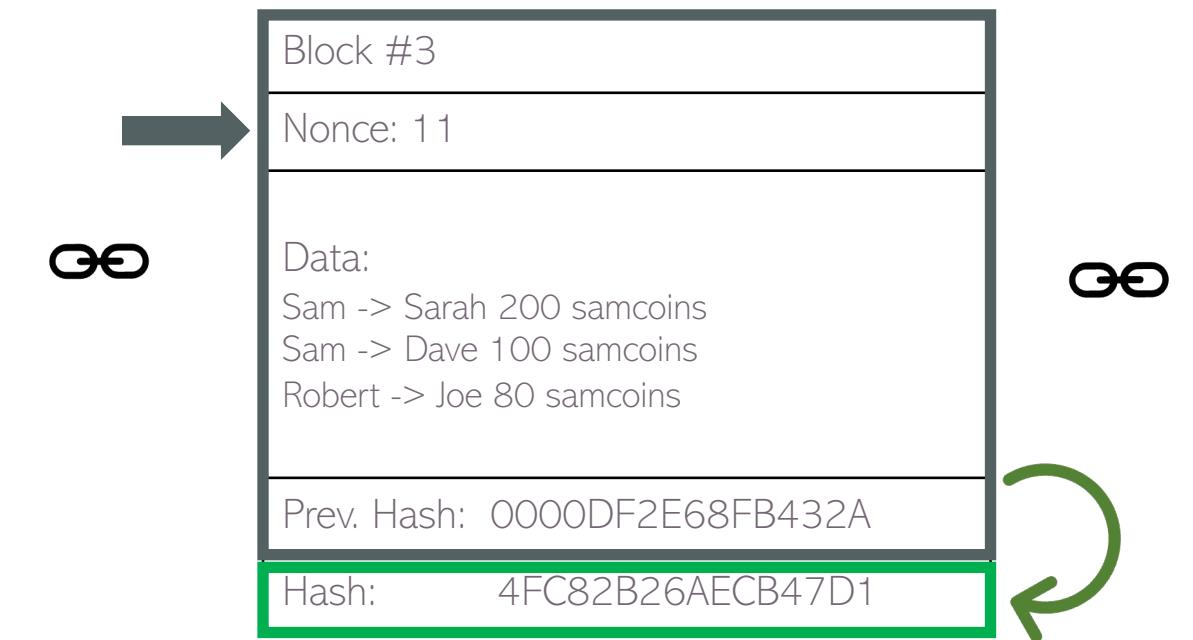


The nonce field gives miners extra control and flexibility to vary the hash of current block.

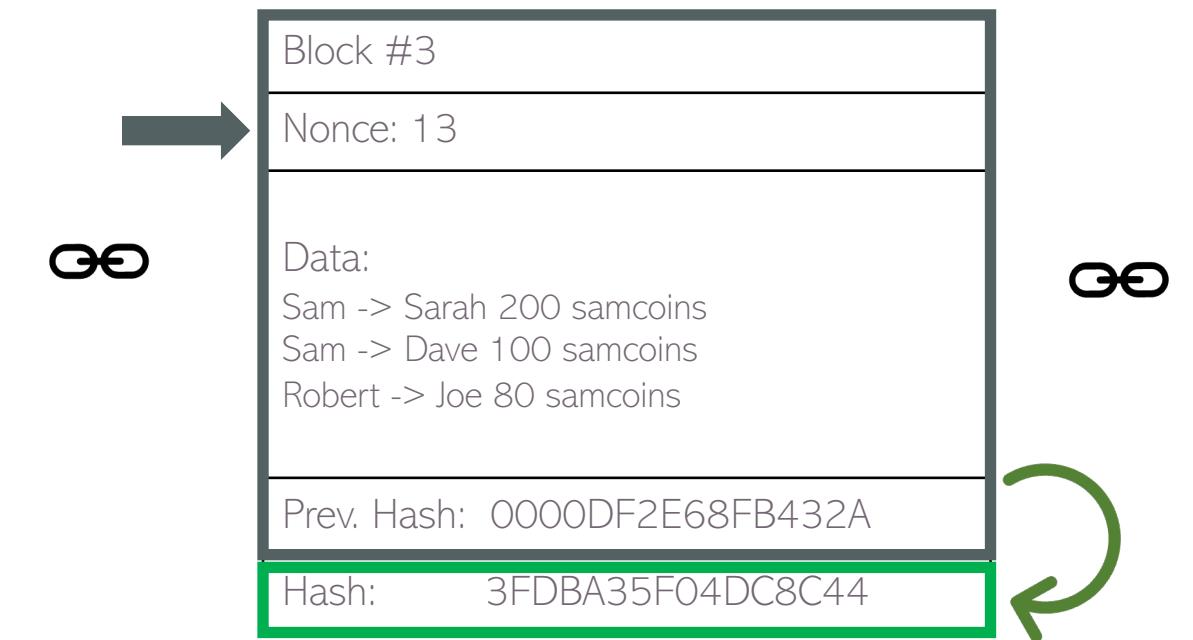
# Nonce



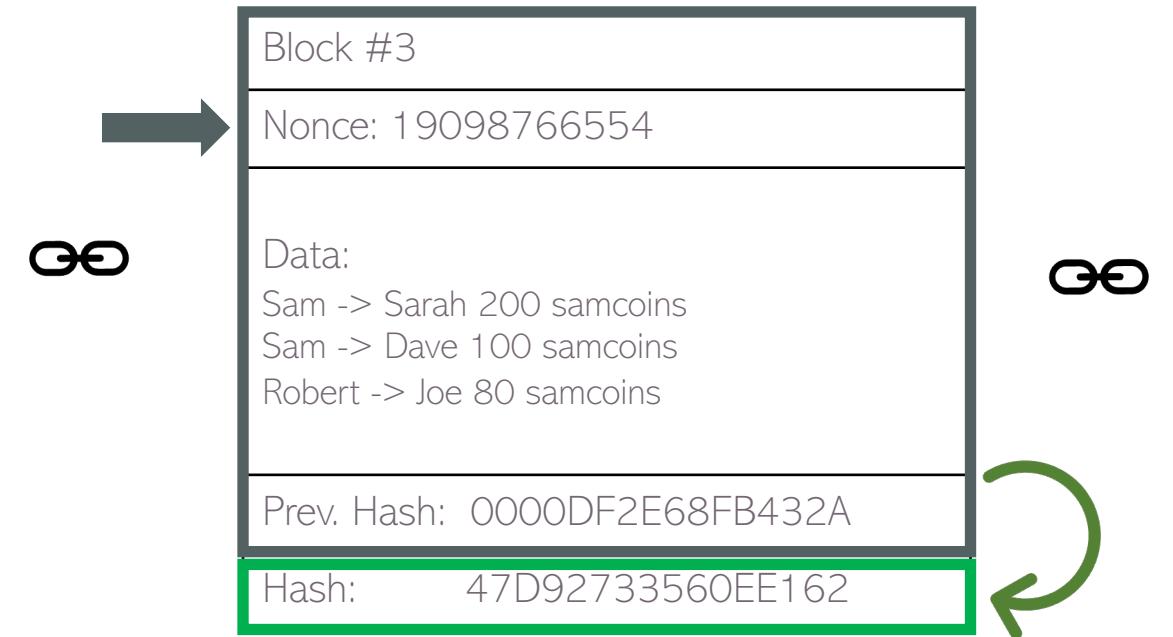
# Nonce



# Nonce



# Nonce



?

# How Mining Works

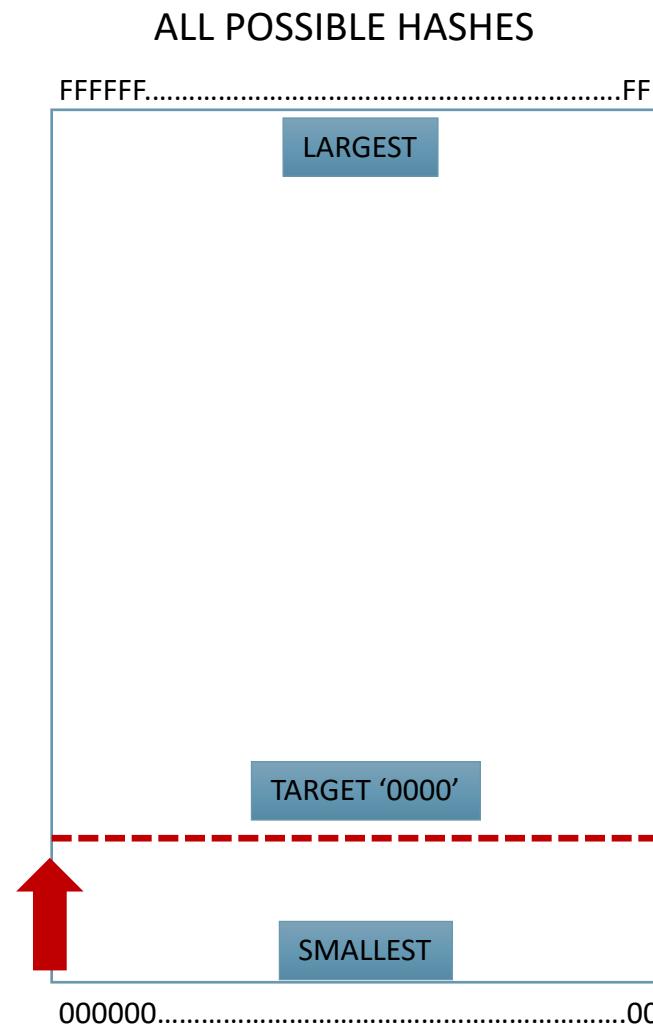
- A Hash is a Number.
- Hash of number 1:  
**Hexadecimal:**  
6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52  
ddb7875b4b
- Hash of “Hello World!”:  
**Hexadecimal:**  
7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd  
200126d9069

# How Mining Works

- A Hash is a Number.
- Hash of number 1:  
Hexadecimal:  
6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52  
ddb7875b4b
- Hash of “Hello World!”:  
Hexadecimal:  
7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd  
200126d9069

**TARGET** Hash leading zeros (e.g. ‘0000’)

A **target hash** is a number that a **hash of block** must be less than or equal to it to be added to the chain.



# How Mining Works

- A Hash is a Number.
- Hash of number 1:

Hexadecimal:

6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52  
ddb7875b4b

- Hash of “Hello World!”:

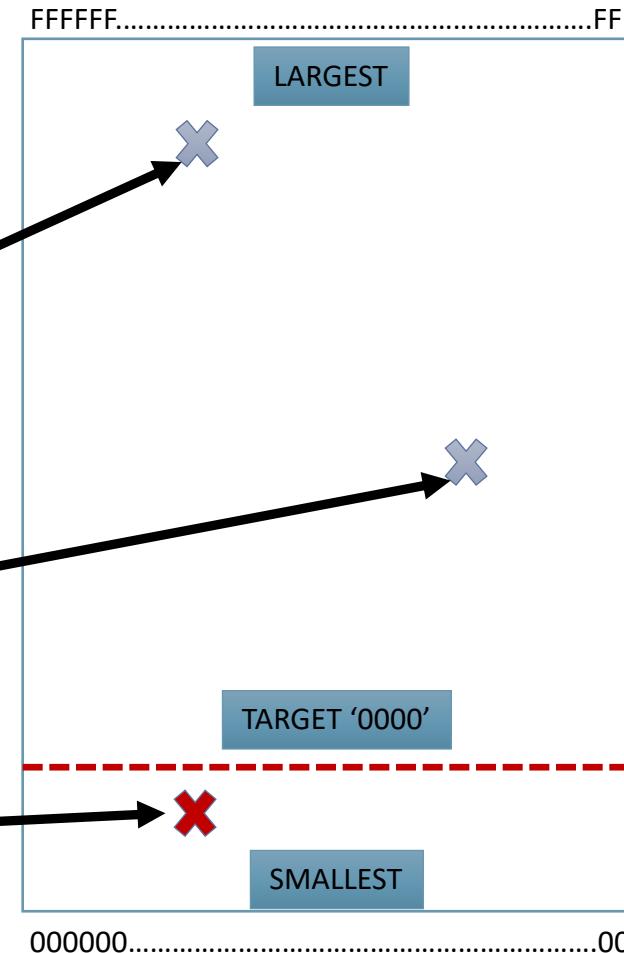
Hexadecimal:

7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284add  
200126d9069

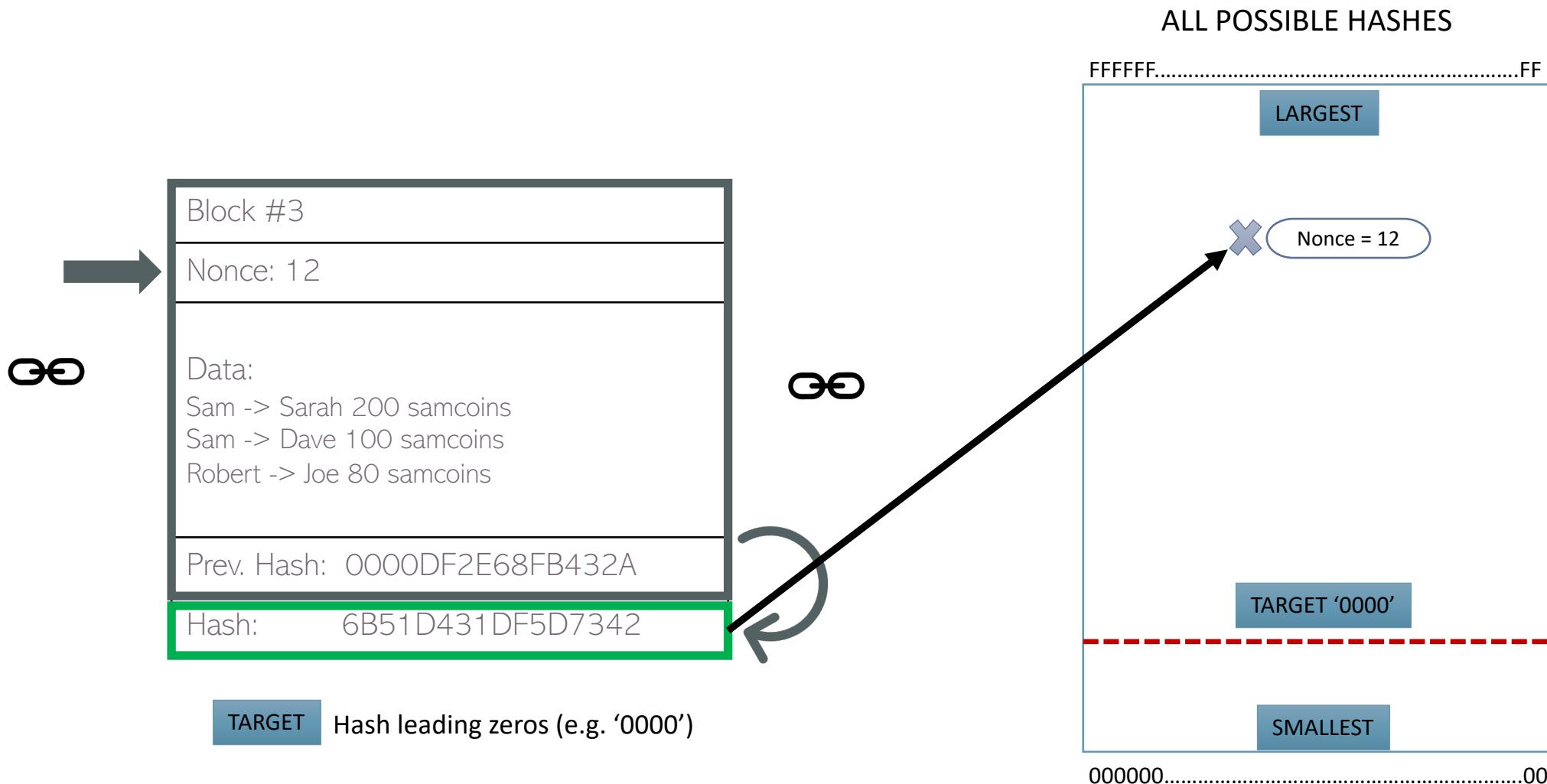
**TARGET** Hash leading zeros (e.g. ‘0000’)

000000000000000000000000c18148a1d65dfc2d4b1fa3d67  
7284add200126d9069

ALL POSSIBLE HASHES

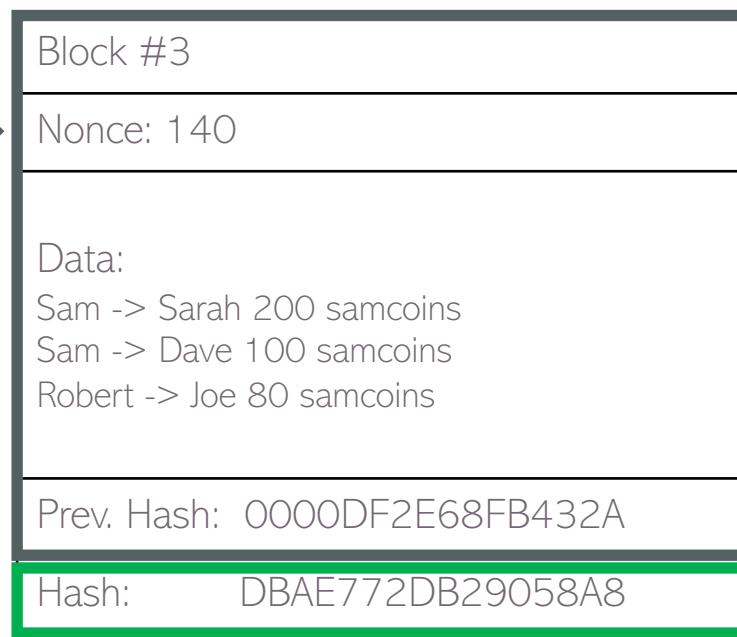


# How Mining Works

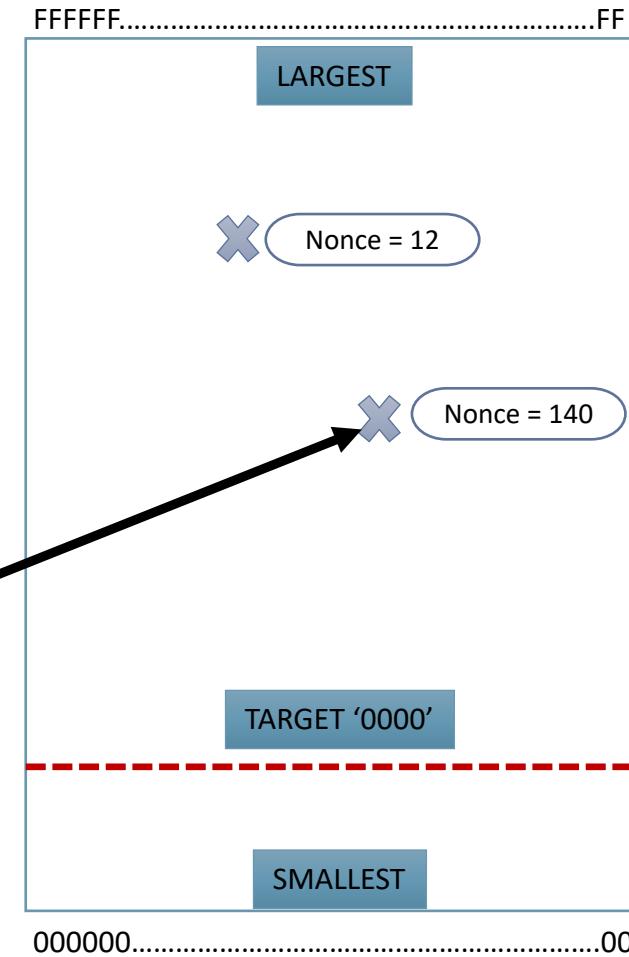


# How Mining Works

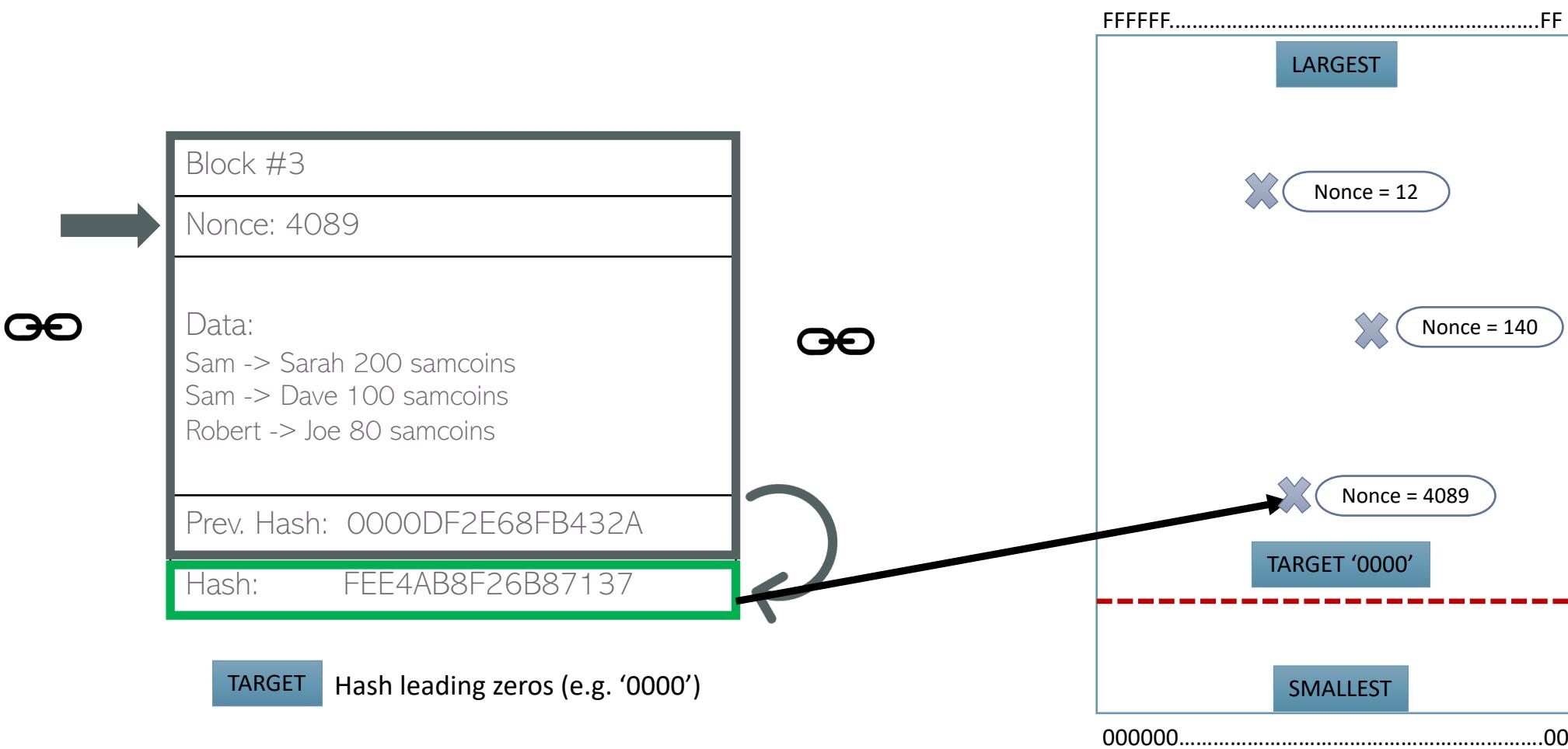
∞ ∞



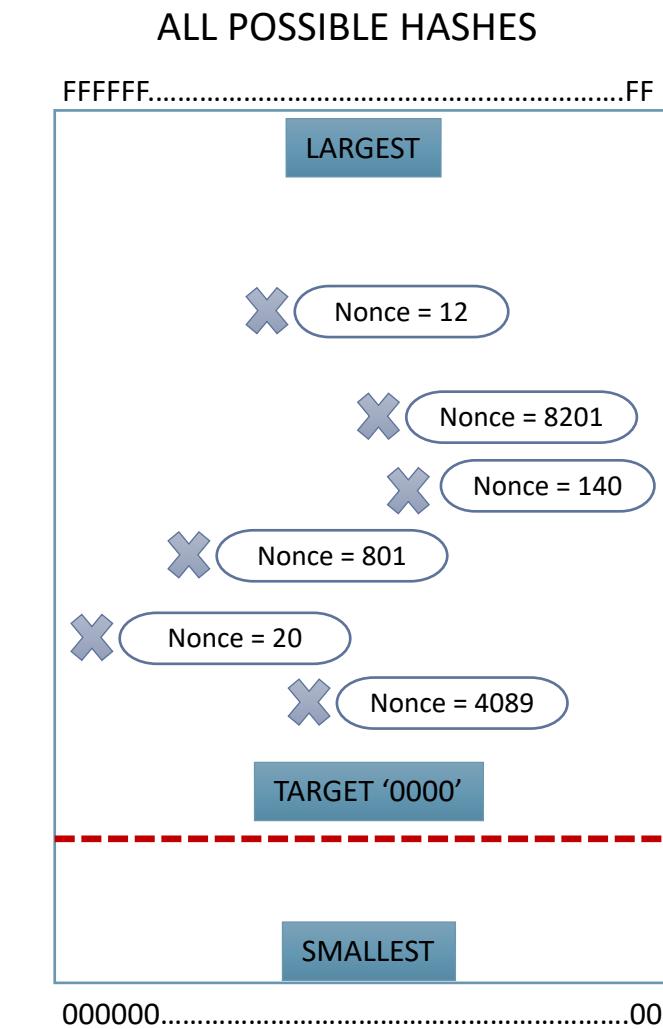
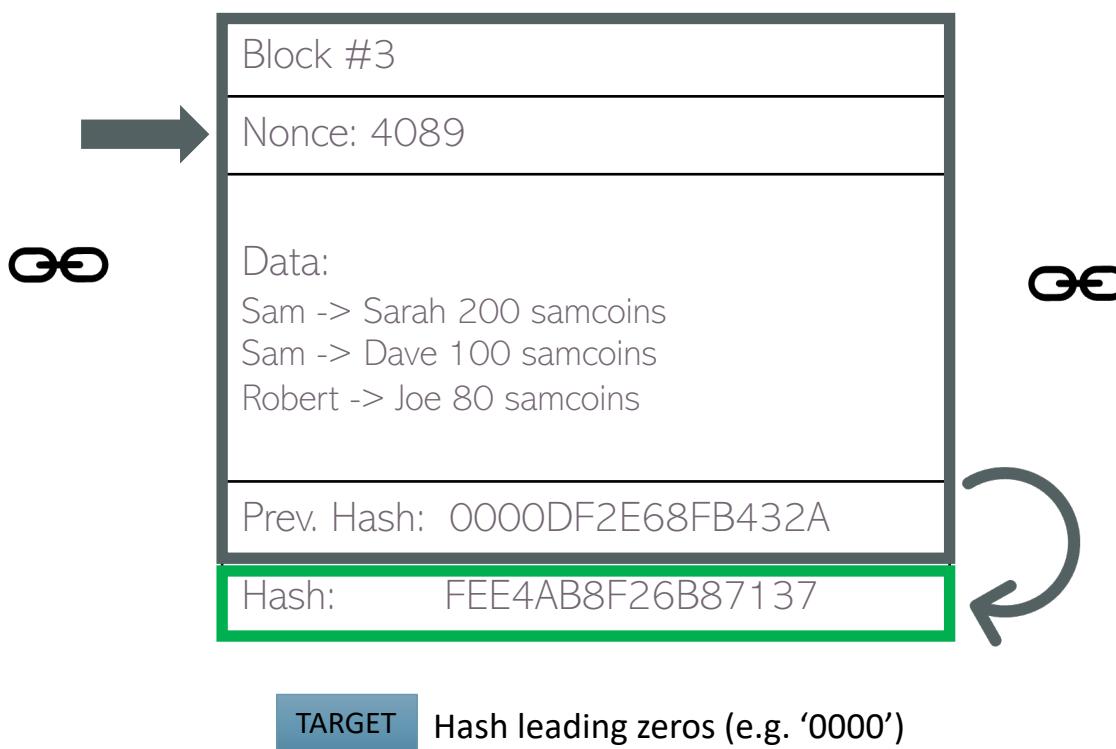
ALL POSSIBLE HASHES



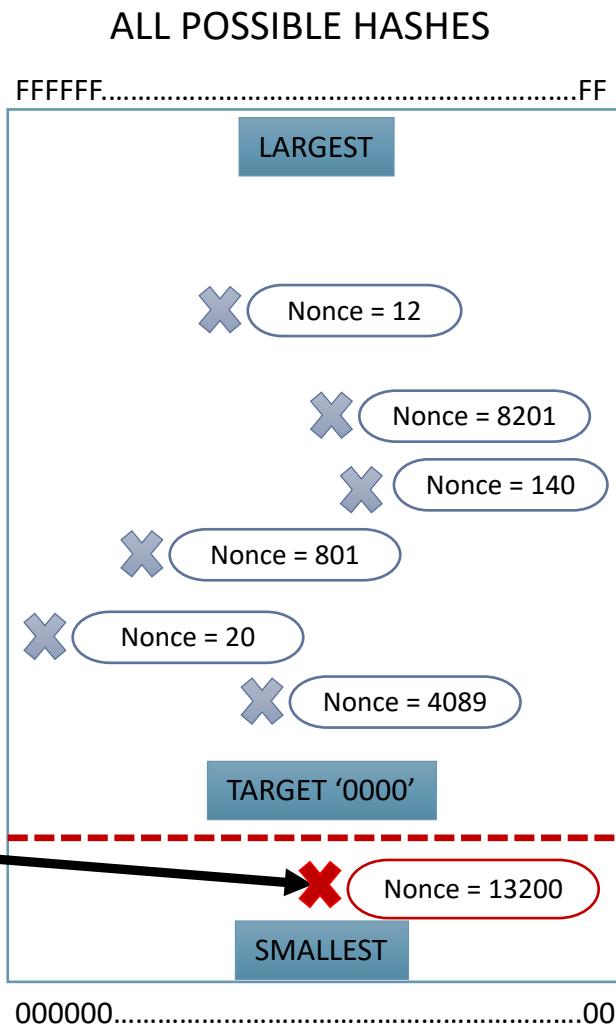
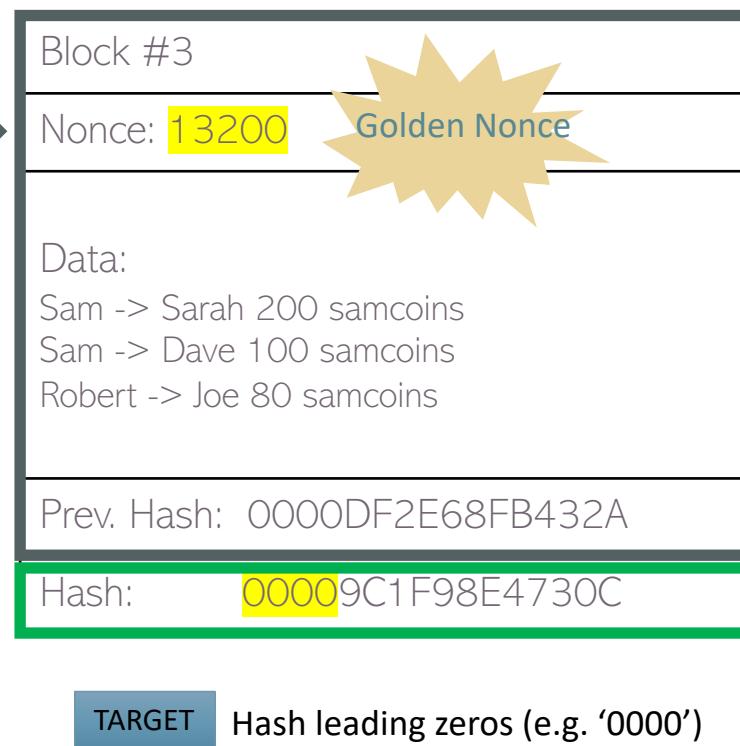
# How Mining Works



# How Mining Works



# How Mining Works



# Blockchain Components

Hash Cryptography

Immutable Ledger

Distributed P2P Network

Mining

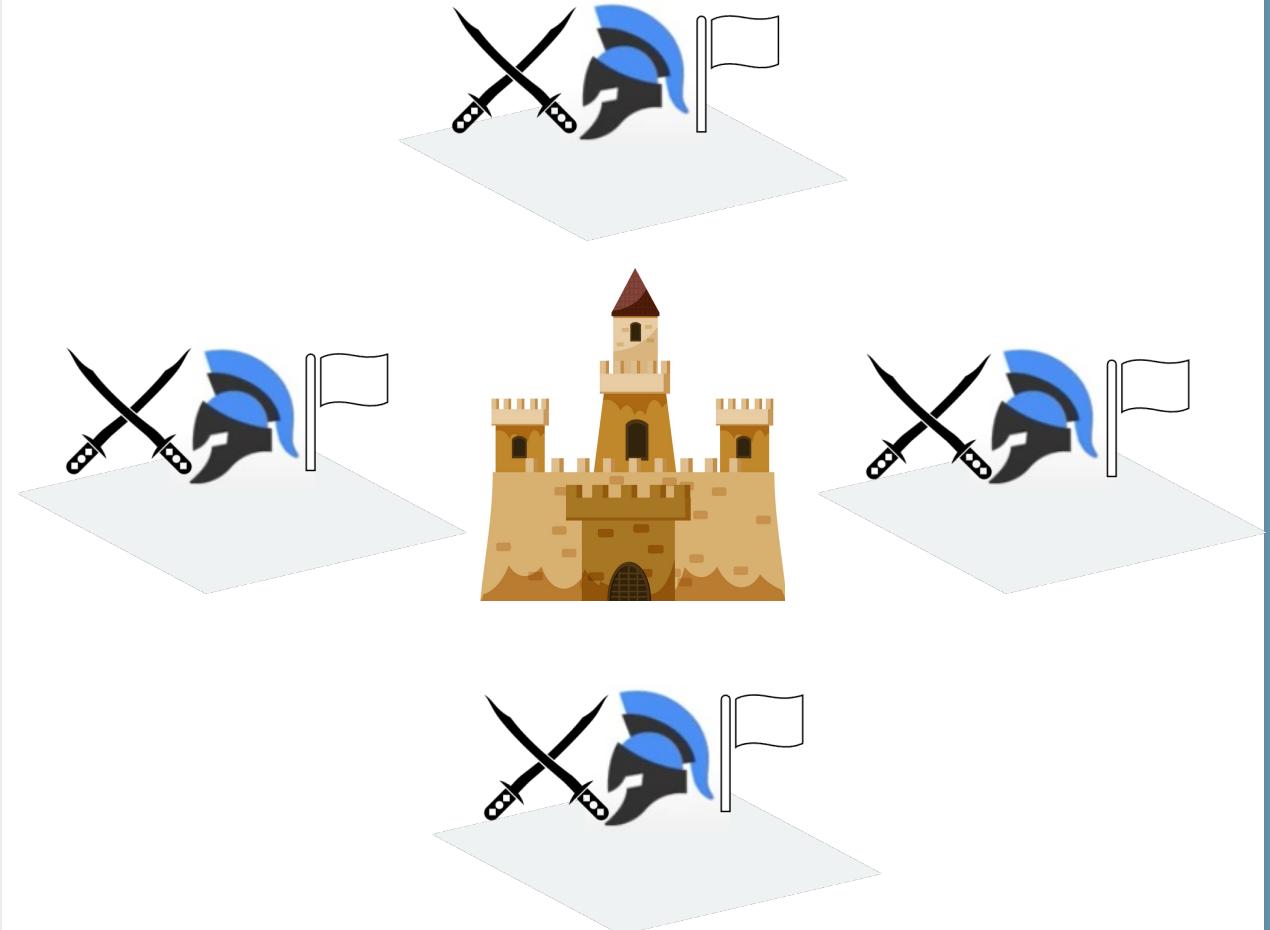
Consensus Protocol

# Byzantine Fault Tolerance

# Byzantine Fault Tolerance

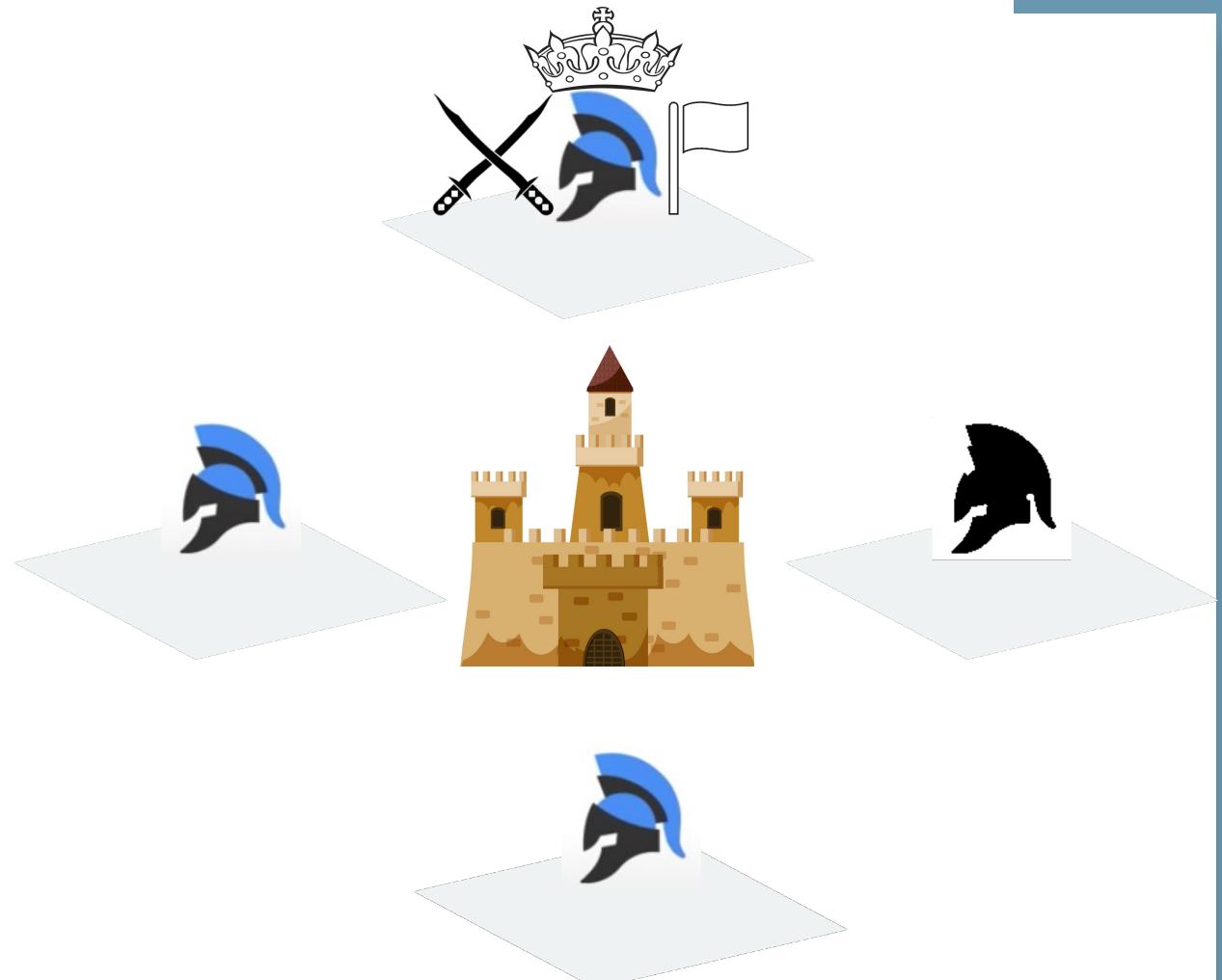


# Byzantine Fault Tolerance



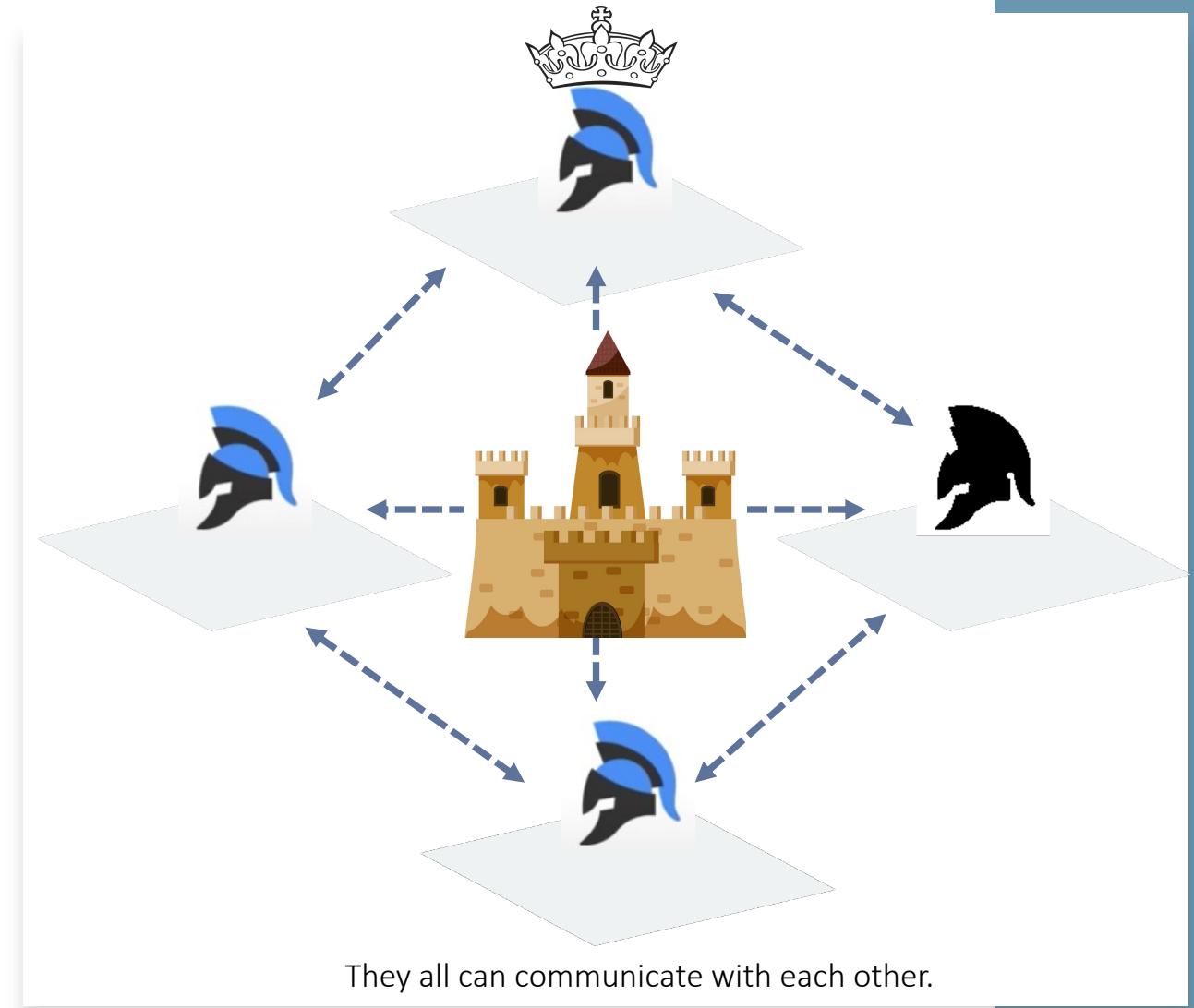
Generals must agree are they attacking or retreating.

# Byzantine Fault Tolerance

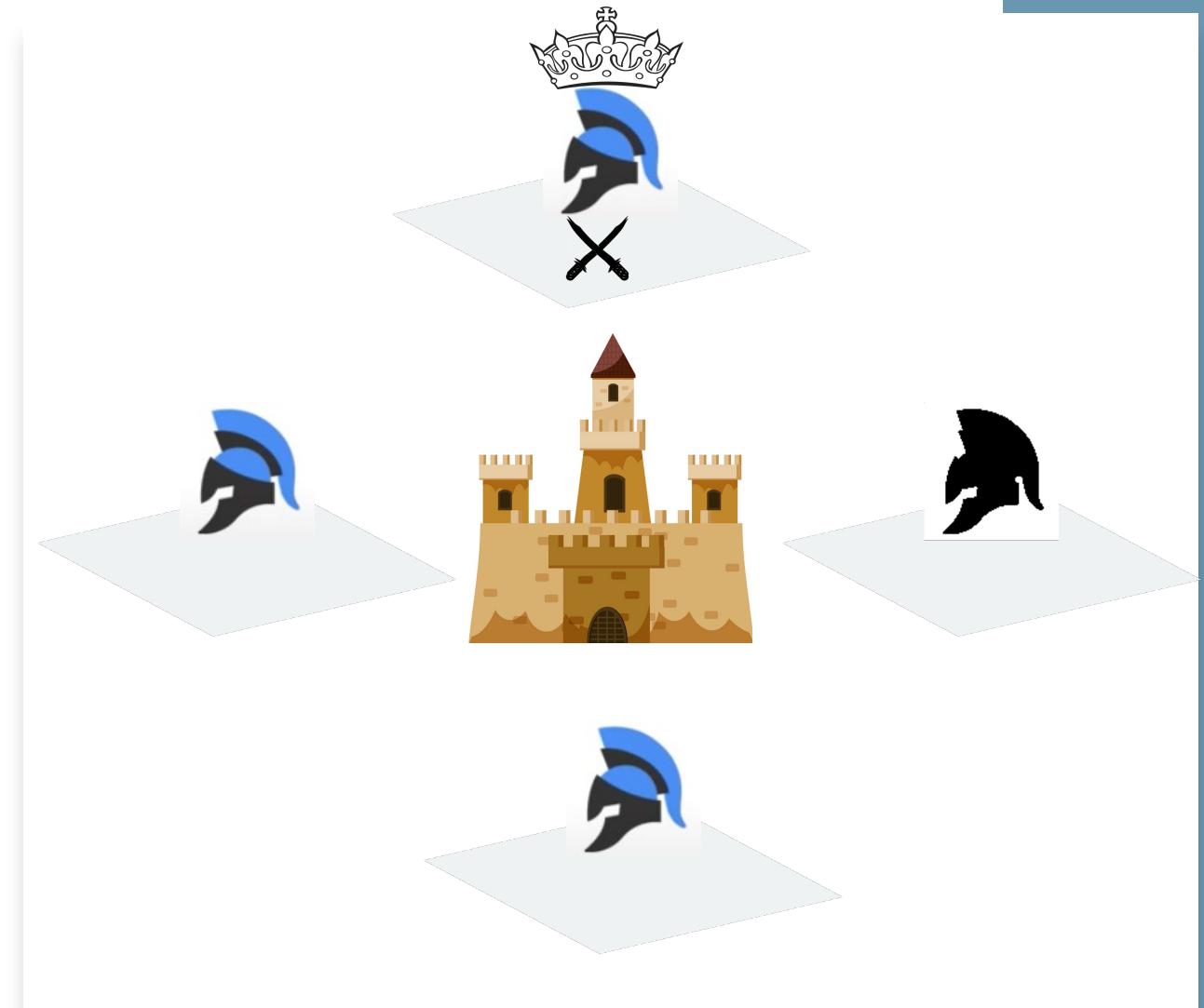


There is a main Commander and a traitor who is not known to others.

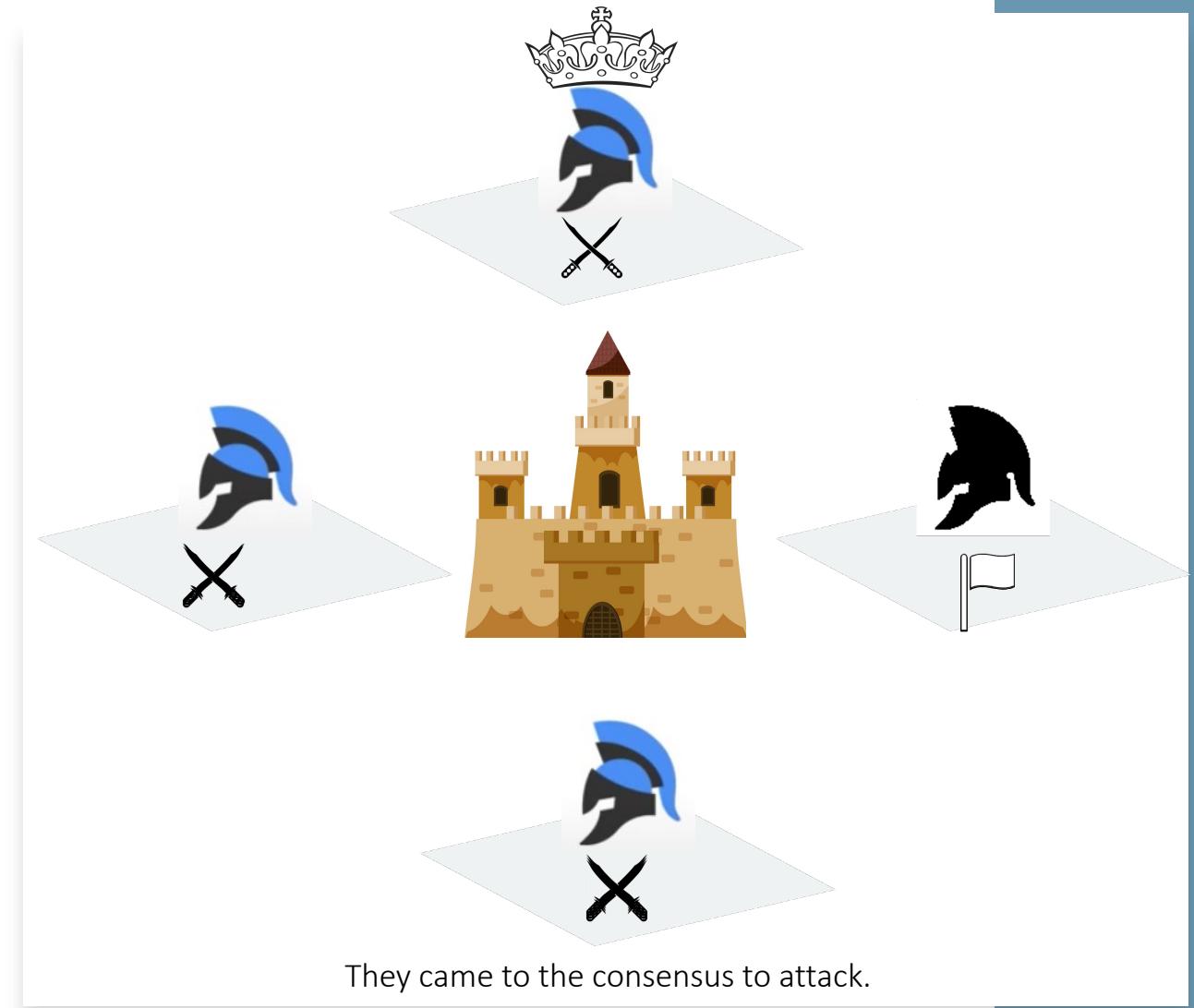
# Byzantine Fault Tolerance



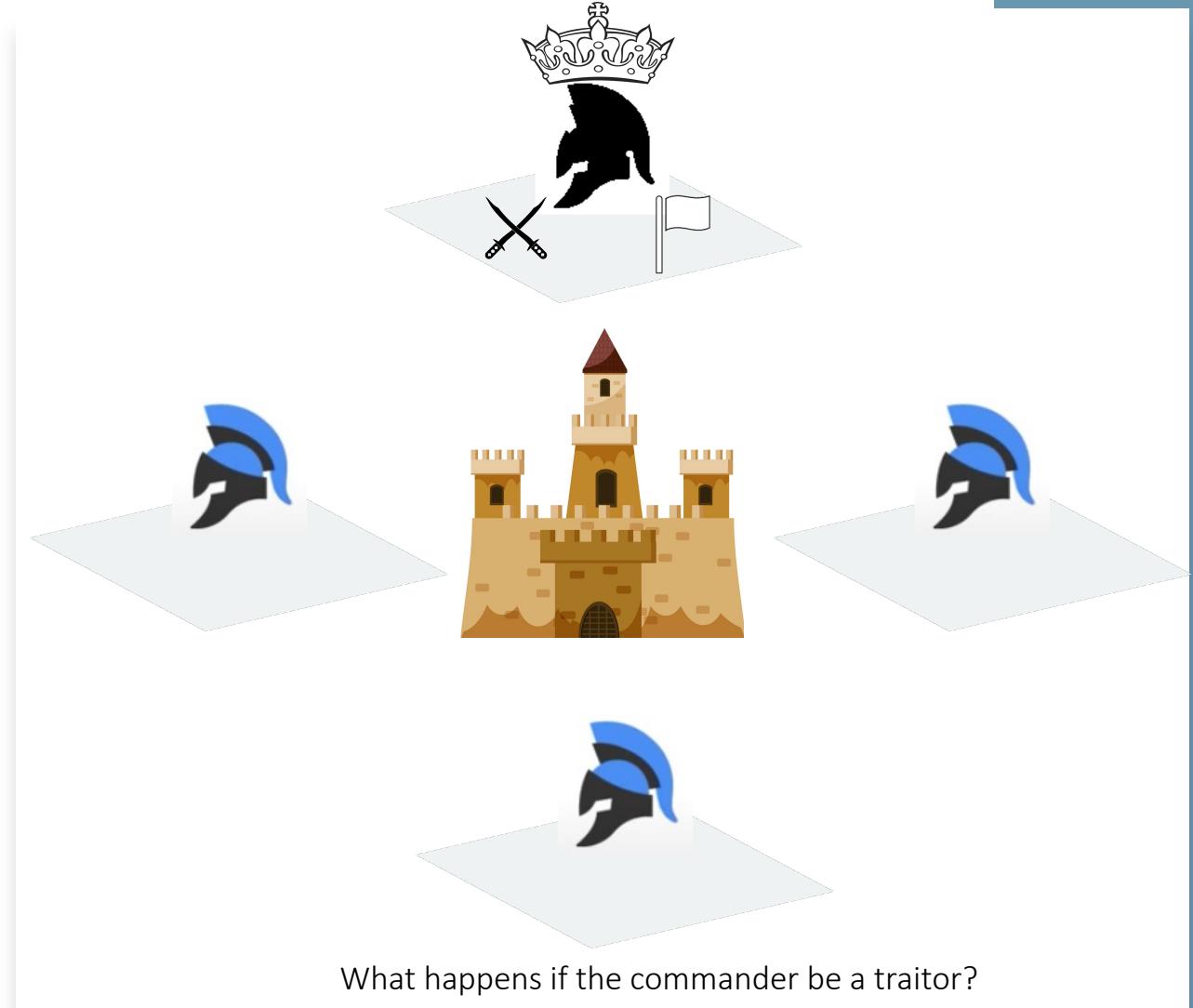
# Byzantine Fault Tolerance



# Byzantine Fault Tolerance



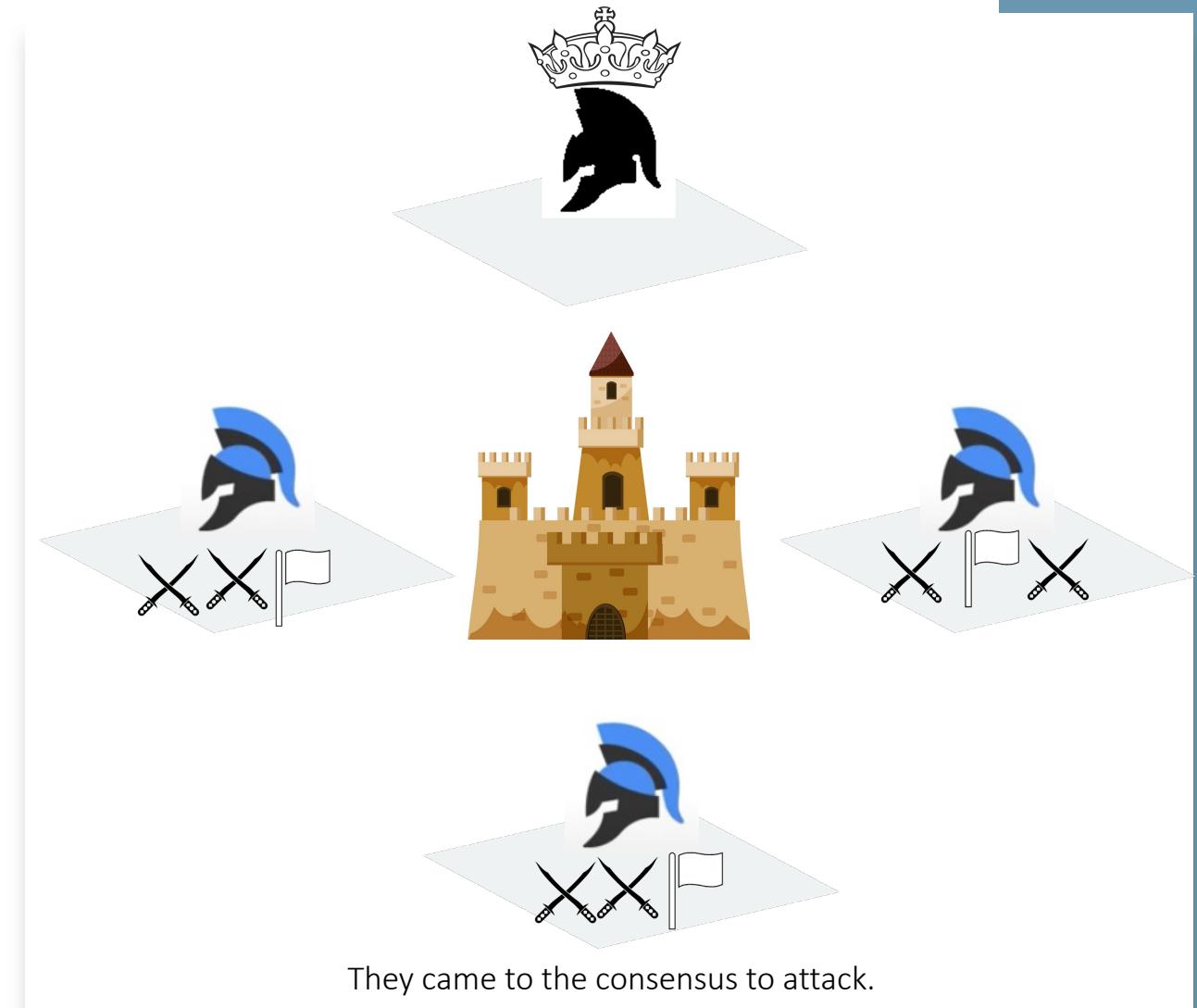
# Byzantine Fault Tolerance



# Byzantine Fault Tolerance

Question:  
To what level the  
algorithm can tolerate?

The number of traitors should  
not exceed 33% of the total.

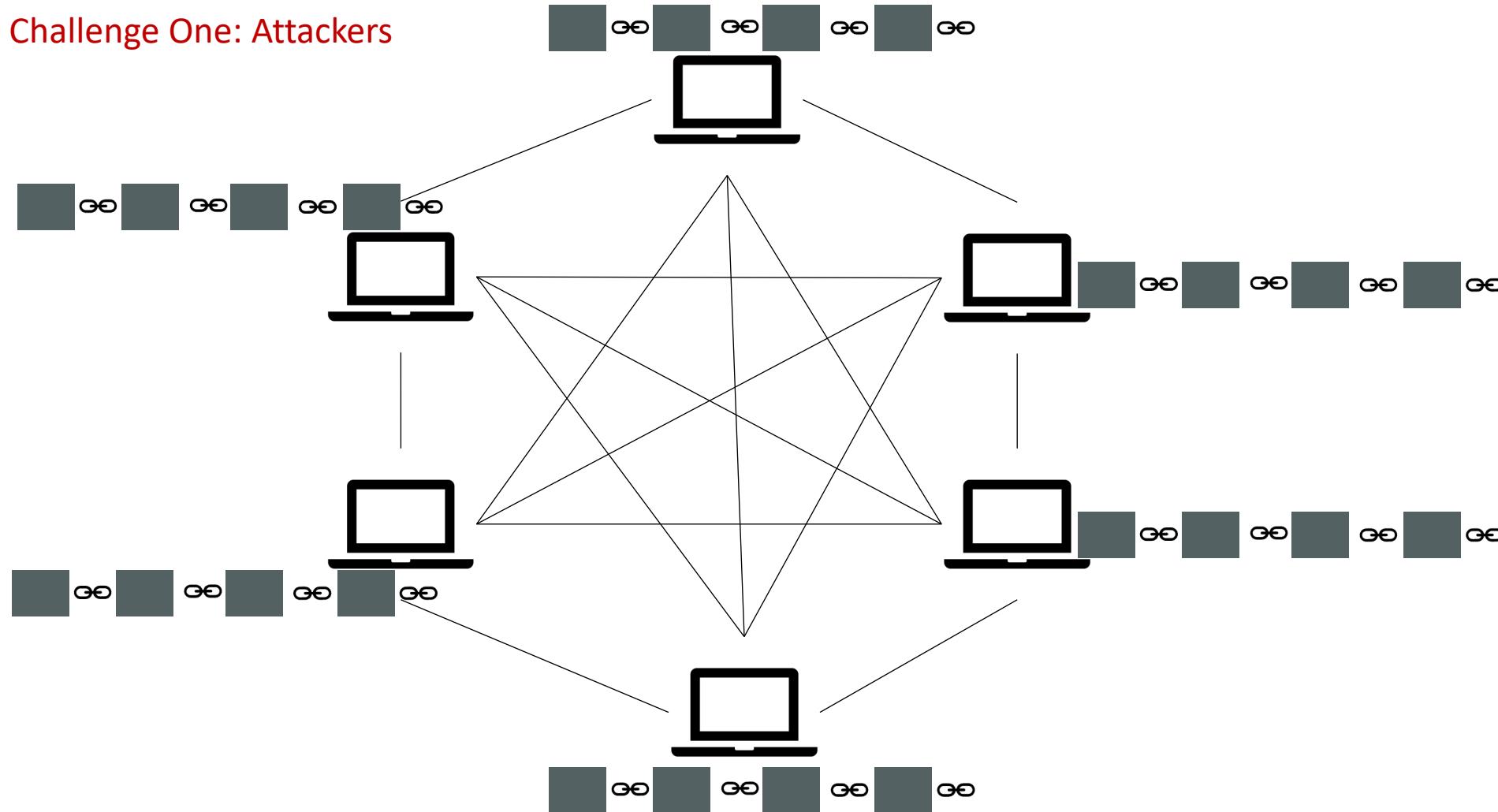


# Consensus Protocol

A consensus protocol is a process through which all the peers of a Blockchain network reach a common agreement about the present state of the distributed ledger.

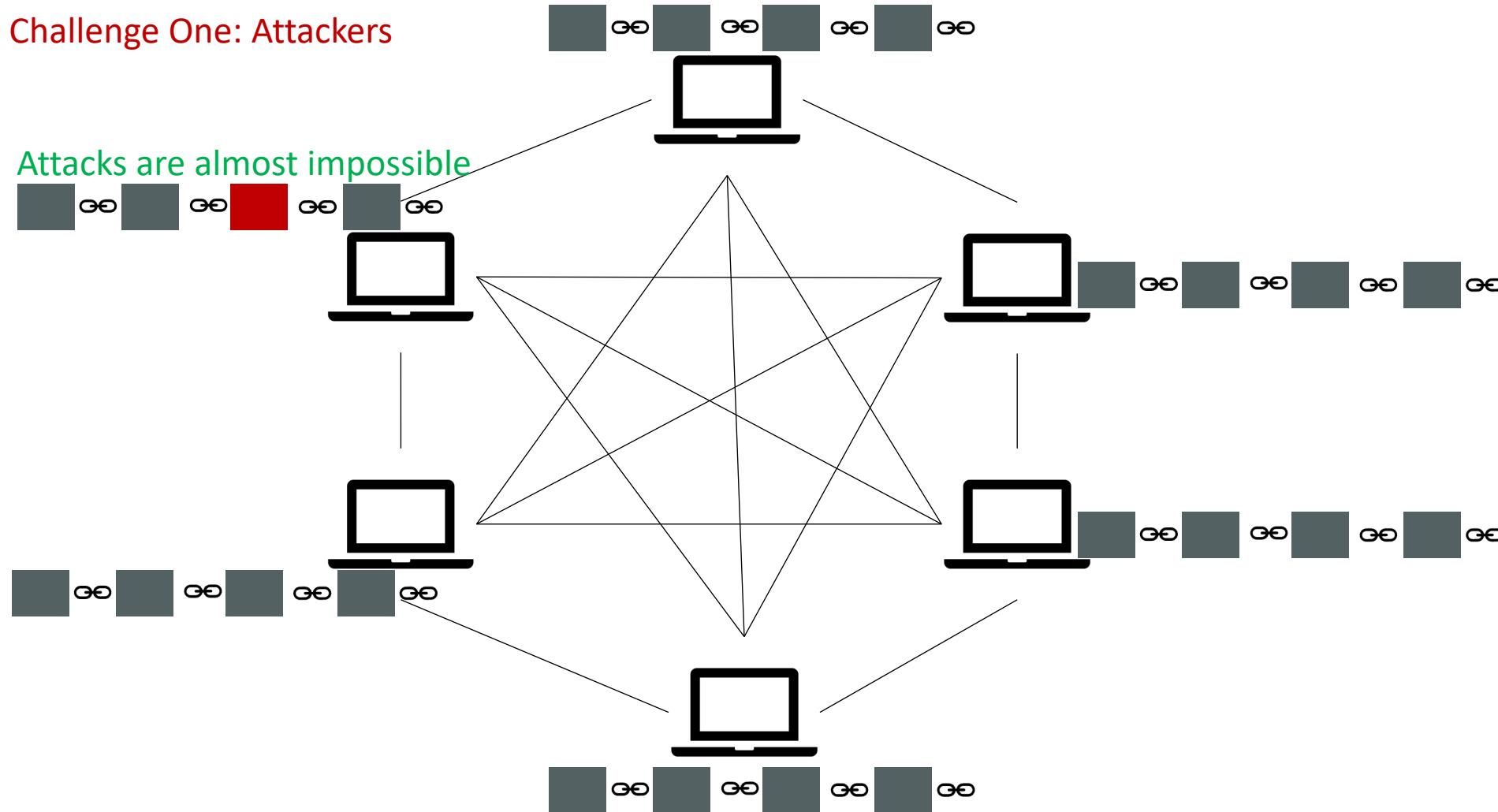
# Consensus Protocol

Challenge One: Attackers



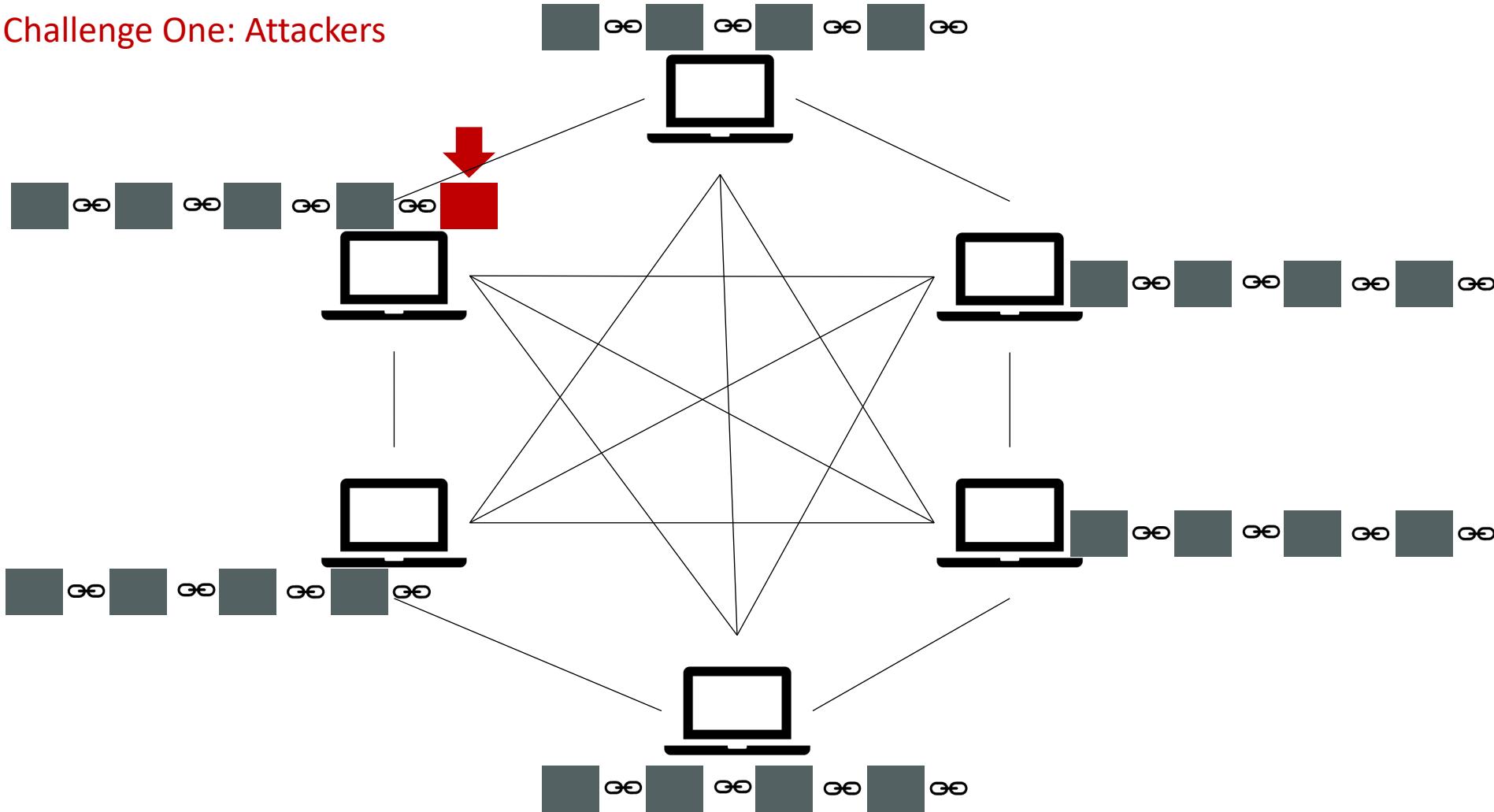
# Consensus Protocol

Challenge One: Attackers



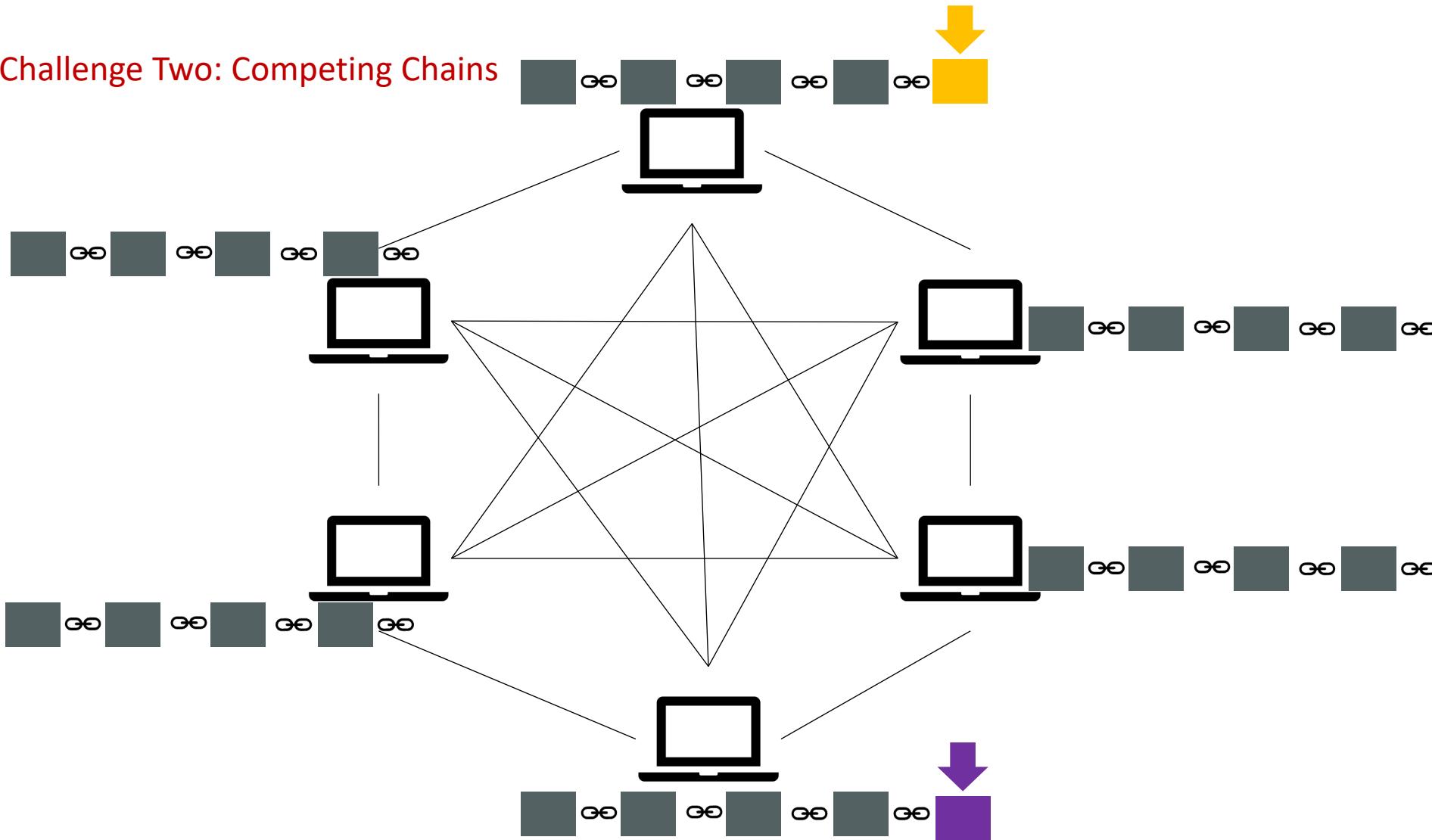
# Consensus Protocol

Challenge One: Attackers



# Consensus Protocol

Challenge Two: Competing Chains



# Consensus Protocol

- A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a **common agreement** about the **present state of the distributed ledger**.

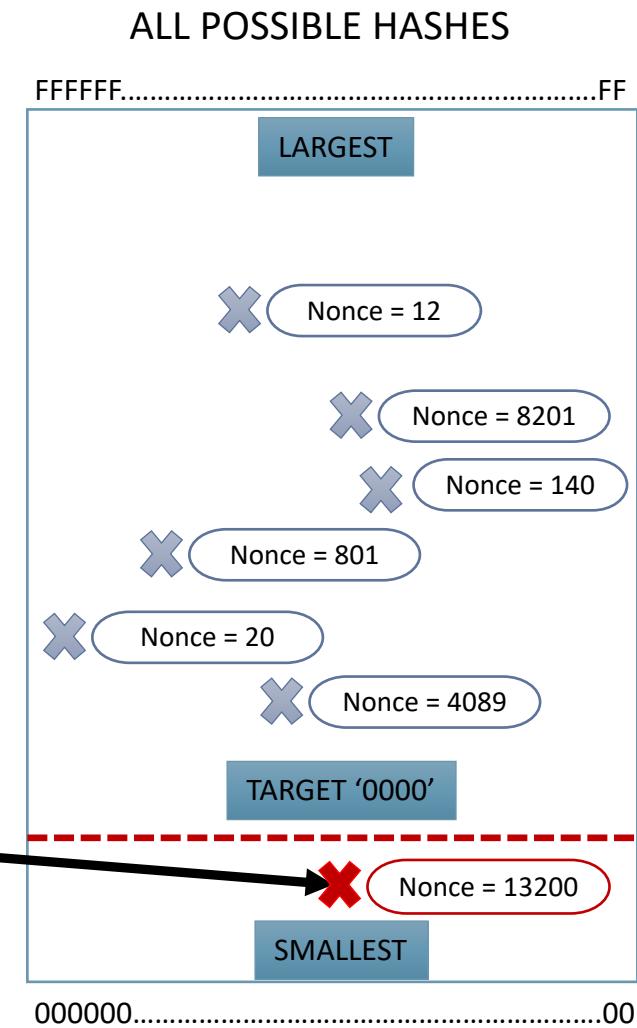
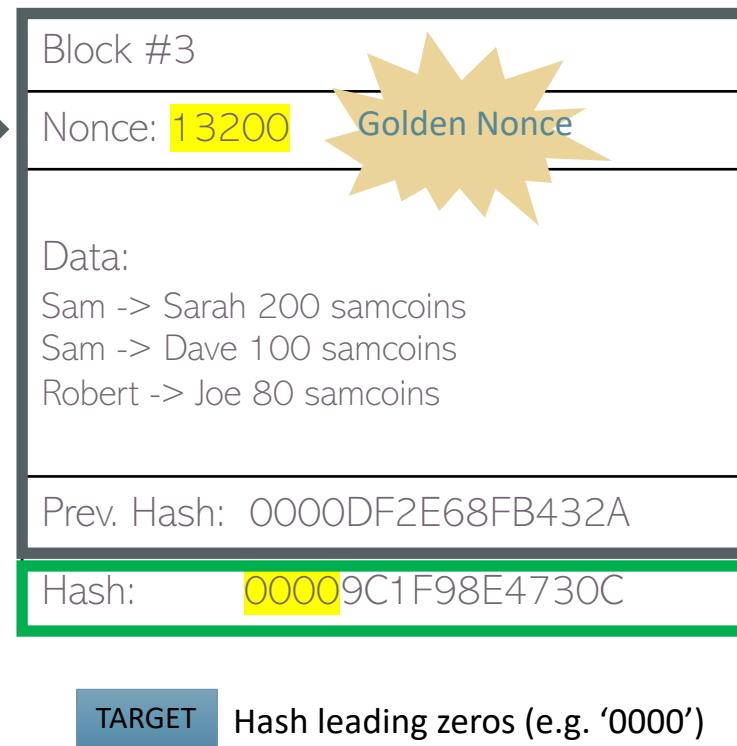
## Main Consensus Protocols

Proof-of-Work (PoW)

Proof-of-Stack (PoS)

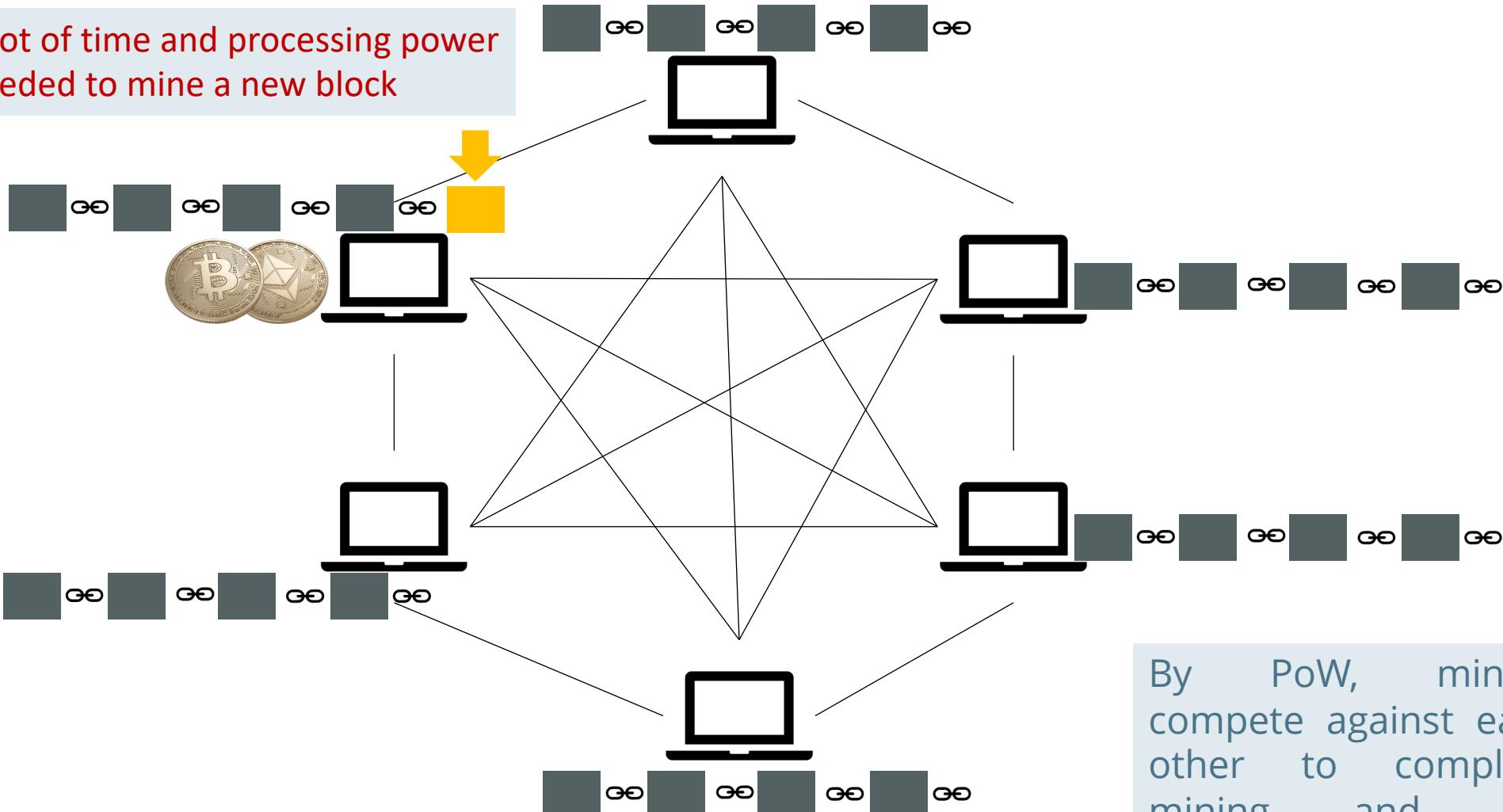
Others(E.g. DPoS, PBFT, Ripple)

# Consensus Protocol



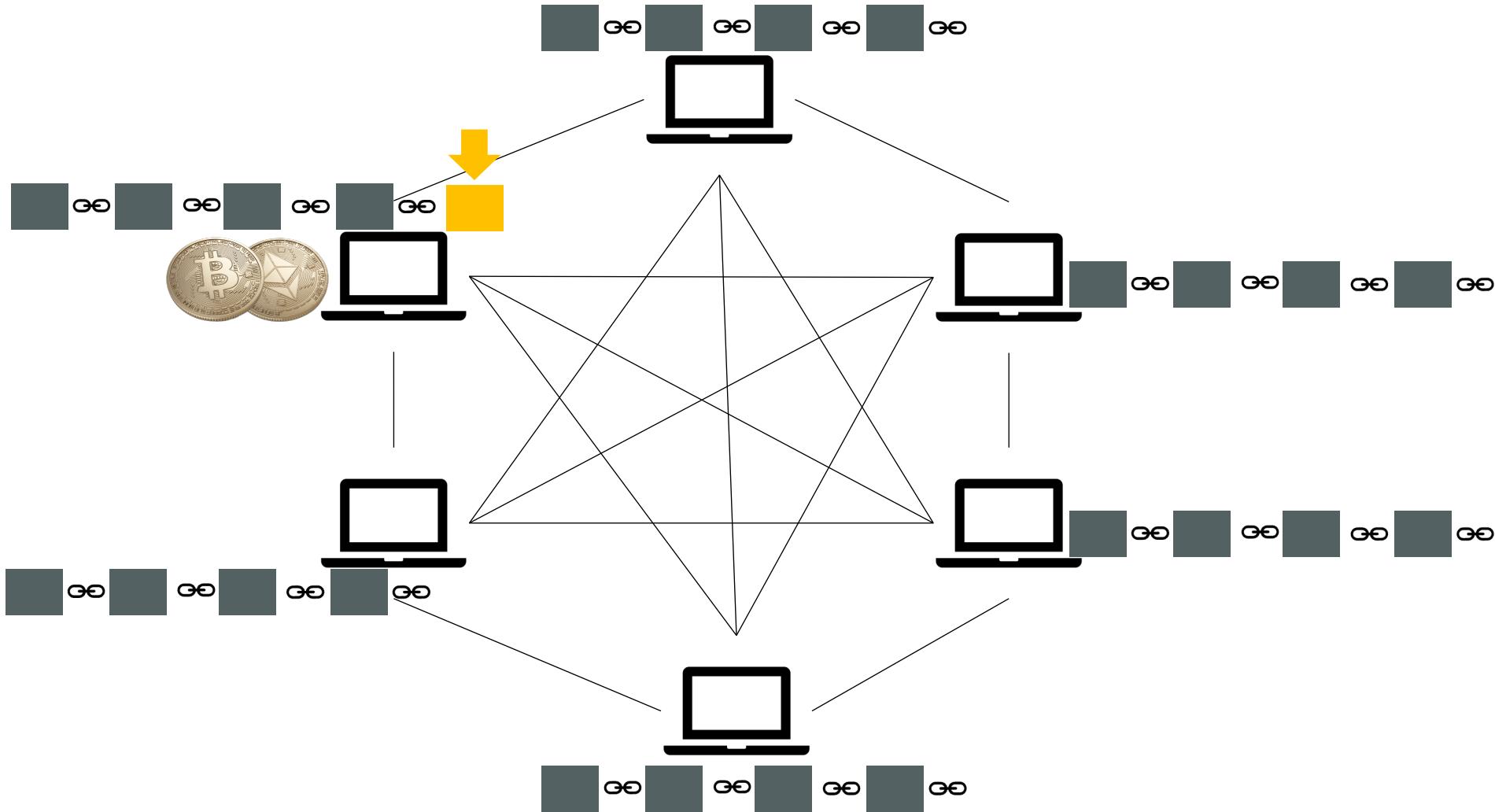
# Consensus Protocol

A lot of time and processing power  
needed to mine a new block

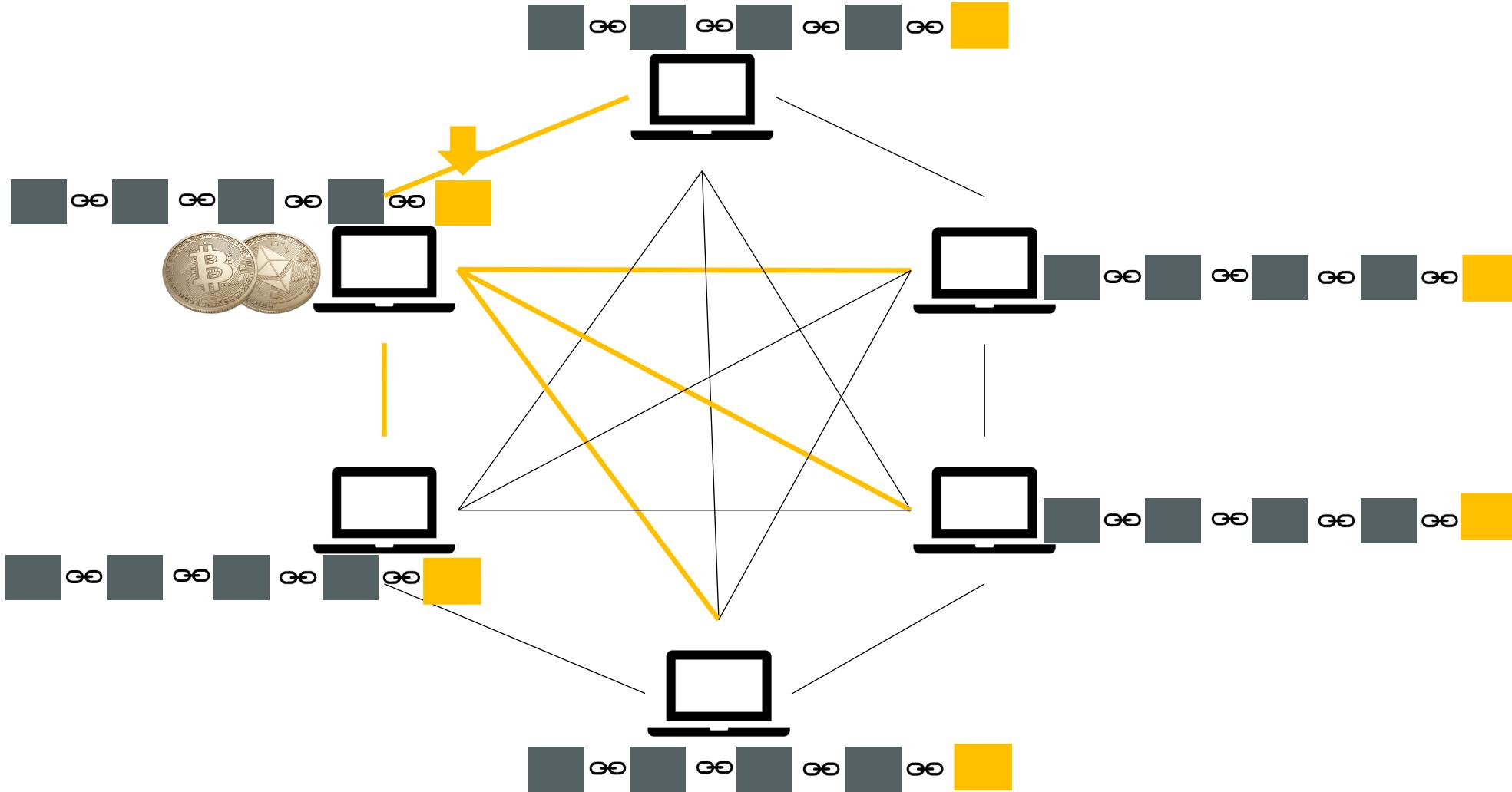


Challenge 1  
Attackers

# Consensus Protocol



# Consensus Protocol



Challenge 1  
Attackers

# Consensus Protocol

1. Check syntactic correctness
2. Reject if duplicate of block we have in any of the three categories
3. Transaction list must be non-empty
4. Block hash must satisfy claimed  $n\text{Bits}$  proof of work
5. Block timestamp must not be more than two hours in the future
6. First transaction must be coinbase (i.e. only 1 input, with hash=0, n=-1), the rest must not be
7. For each transaction, apply "tx" checks 2-4
8. For the coinbase (first) transaction, scriptSig length must be 2-100
9. Reject if sum of transaction sig opcounts > MAX\_BLOCK\_SIGOPS
10. Verify Merkle hash
11. Check if prev block (matching *prev* hash) is in main branch or side branches. If not, add this to orphans done with block
12. Check that  $n\text{Bits}$  value matches the difficulty rules
13. Reject if timestamp is the median time of the last 11 blocks or before
14. For certain old blocks (i.e. on initial block download) check that hash matches known values
15. Add block into the tree. There are three cases: 1. block further extends the main branch; 2. block extends a side branch; 3. block extends a side branch and makes it the new main branch.
16. For case 1, adding to main branch:
  1. For all but the coinbase transaction, apply the following:

[https://en.bitcoin.it/wiki/Protocol\\_rules](https://en.bitcoin.it/wiki/Protocol_rules)

Challenge 1  
Attackers

# Consensus Protocol

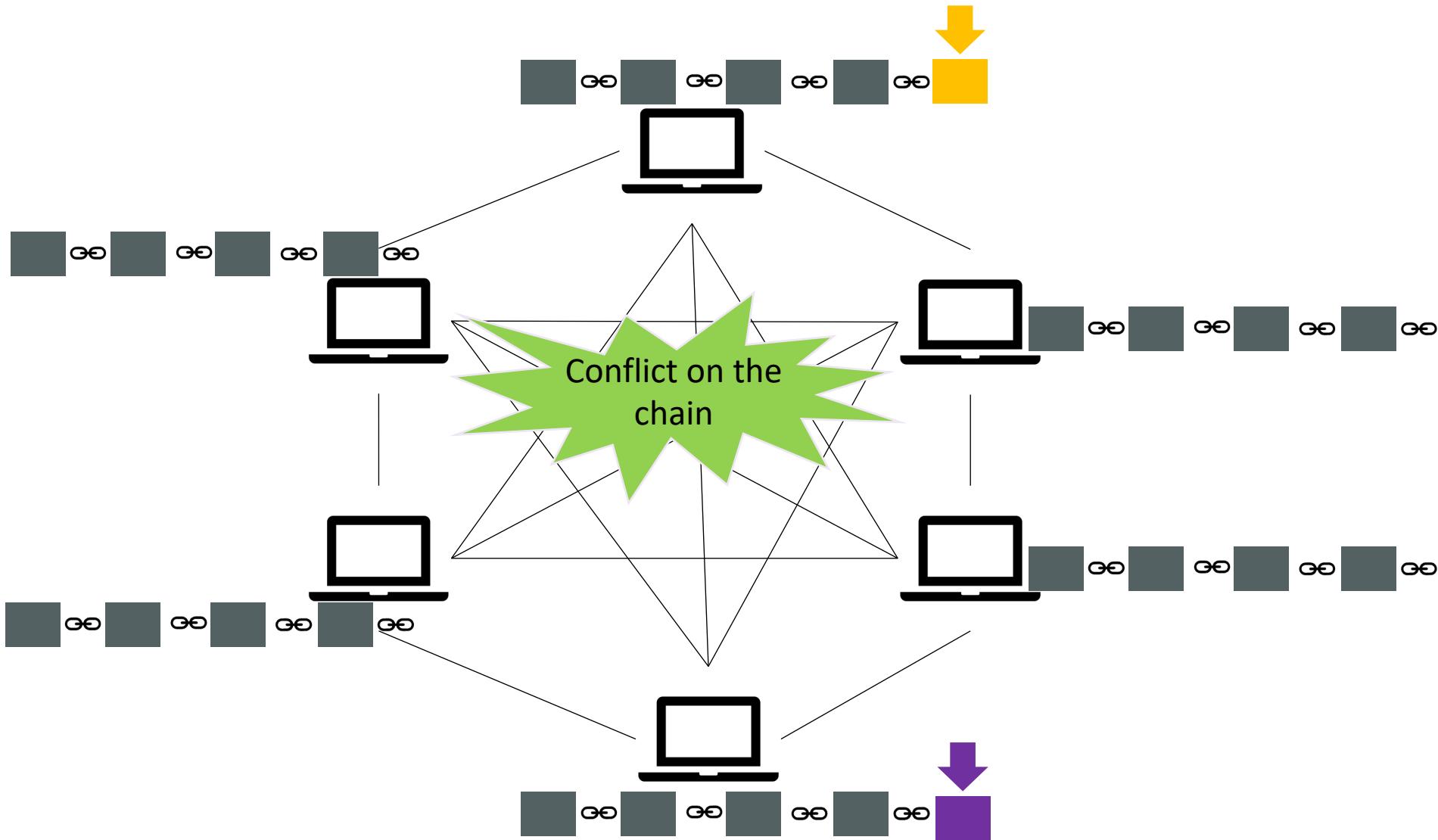
1. Check syntactic correctness
2. Reject if duplicate of block we have in any of the three categories
3. Transaction list must be non-empty
4. Block hash must satisfy claimed  $n\text{Bits}$  proof of work
5. Block timestamp must not be more than two hours in the future
6. First transaction must be coinbase (i.e. only 1 input, with hash=0, n=-1), the rest must not be
7. For each transaction, apply "tx" checks 2-4
8. For the coinbase (first) transaction, scriptSig length must be 2-100
9. Reject if sum of transaction sig opcounts > MAX\_BLOCK\_SIGOPS
10. Verify Merkle hash
11. Check if prev block (matching *prev* hash) is in main branch or side branch done with block
12. Check that  $n\text{Bits}$  value matches the difficulty rules
13. Reject if timestamp is the median time of the last 11 blocks or before
14. For certain old blocks (i.e. on initial block download) check that hash matches known values
15. Add block into the tree. There are three cases: 1. block further extends the main branch; 2. block extends a side branch; 3. block extends a side branch and makes it the new main branch.
16. For case 1, adding to main branch:
  1. For all but the coinbase transaction, apply the following:

[https://en.bitcoin.it/wiki/Protocol\\_rules](https://en.bitcoin.it/wiki/Protocol_rules)

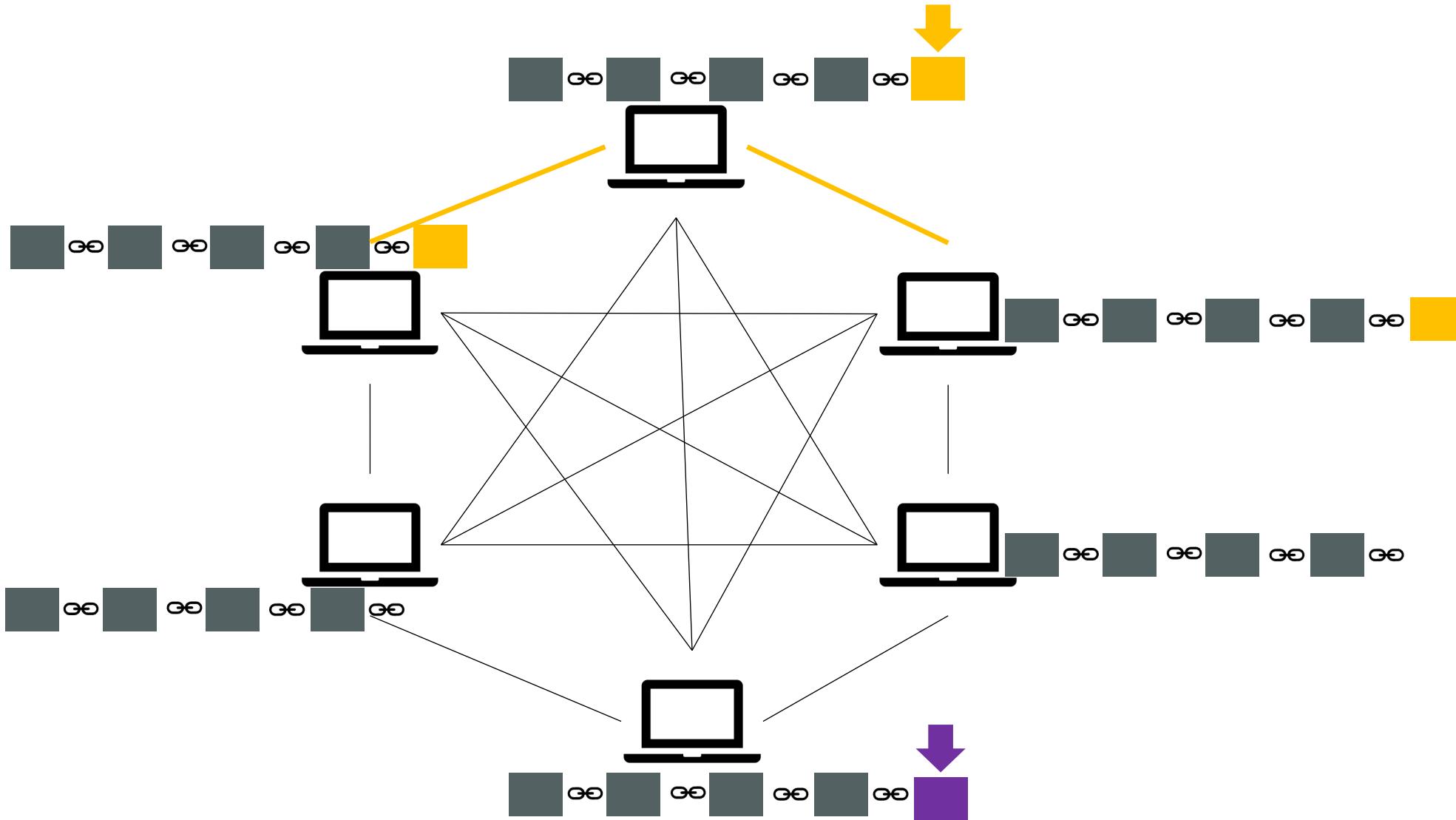
Challenge 1  
Attackers

Cryptographic Puzzles:  
Hard to Solve – Easy to Verify

# Consensus Protocol

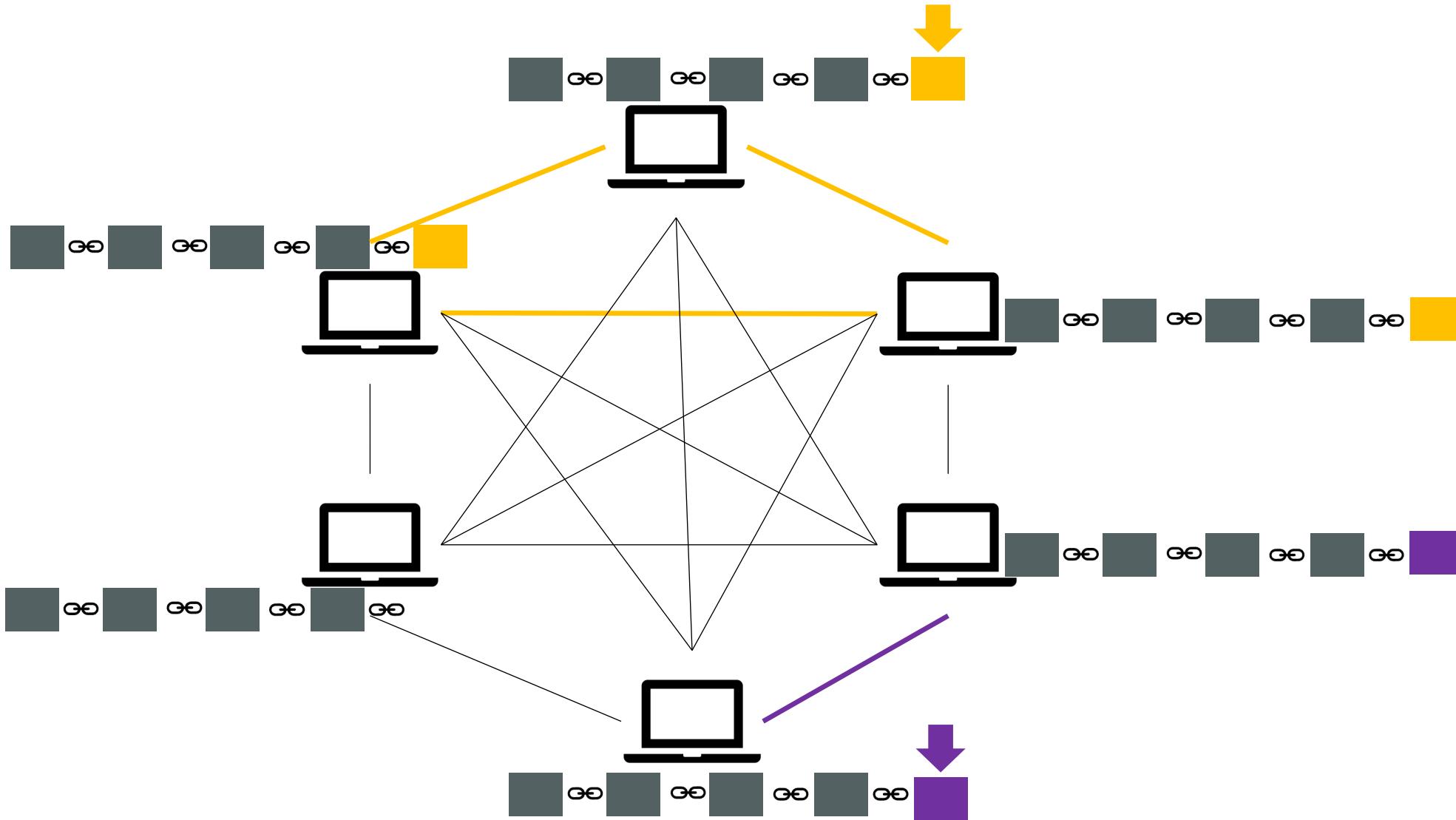


# Consensus Protocol



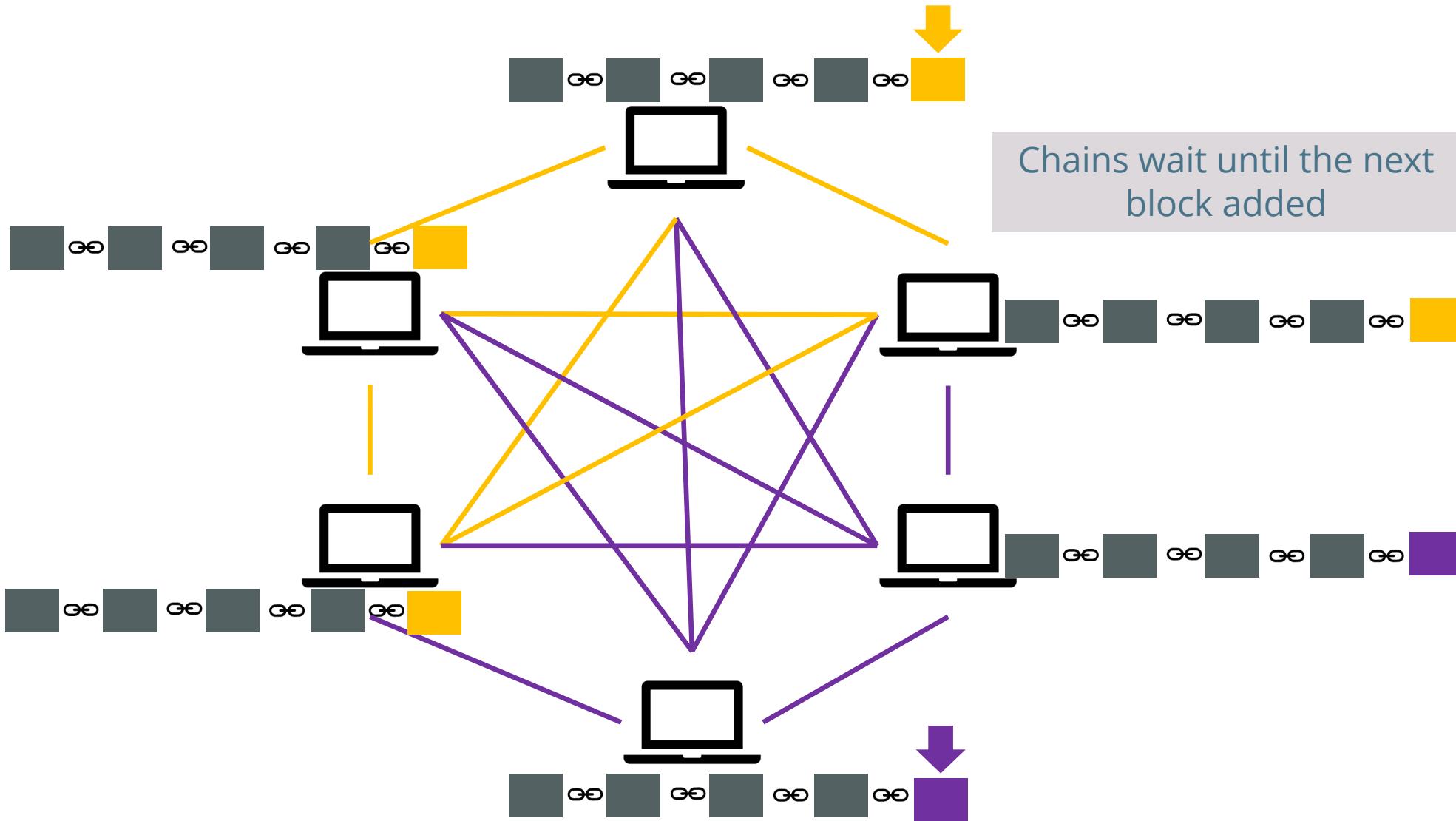
Challenge 2  
Competing  
Chains

# Consensus Protocol

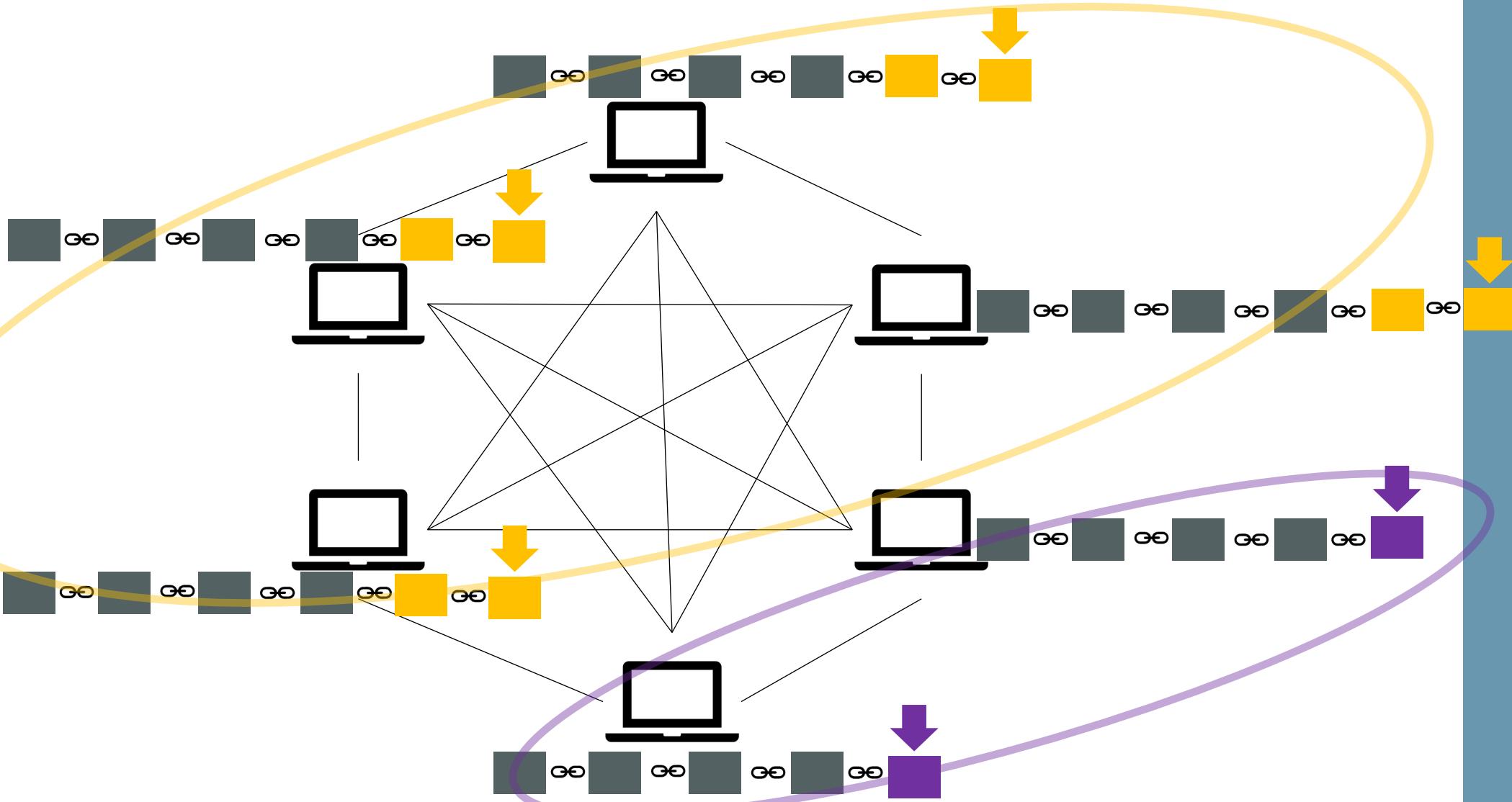


Challenge 2  
Competing  
Chains

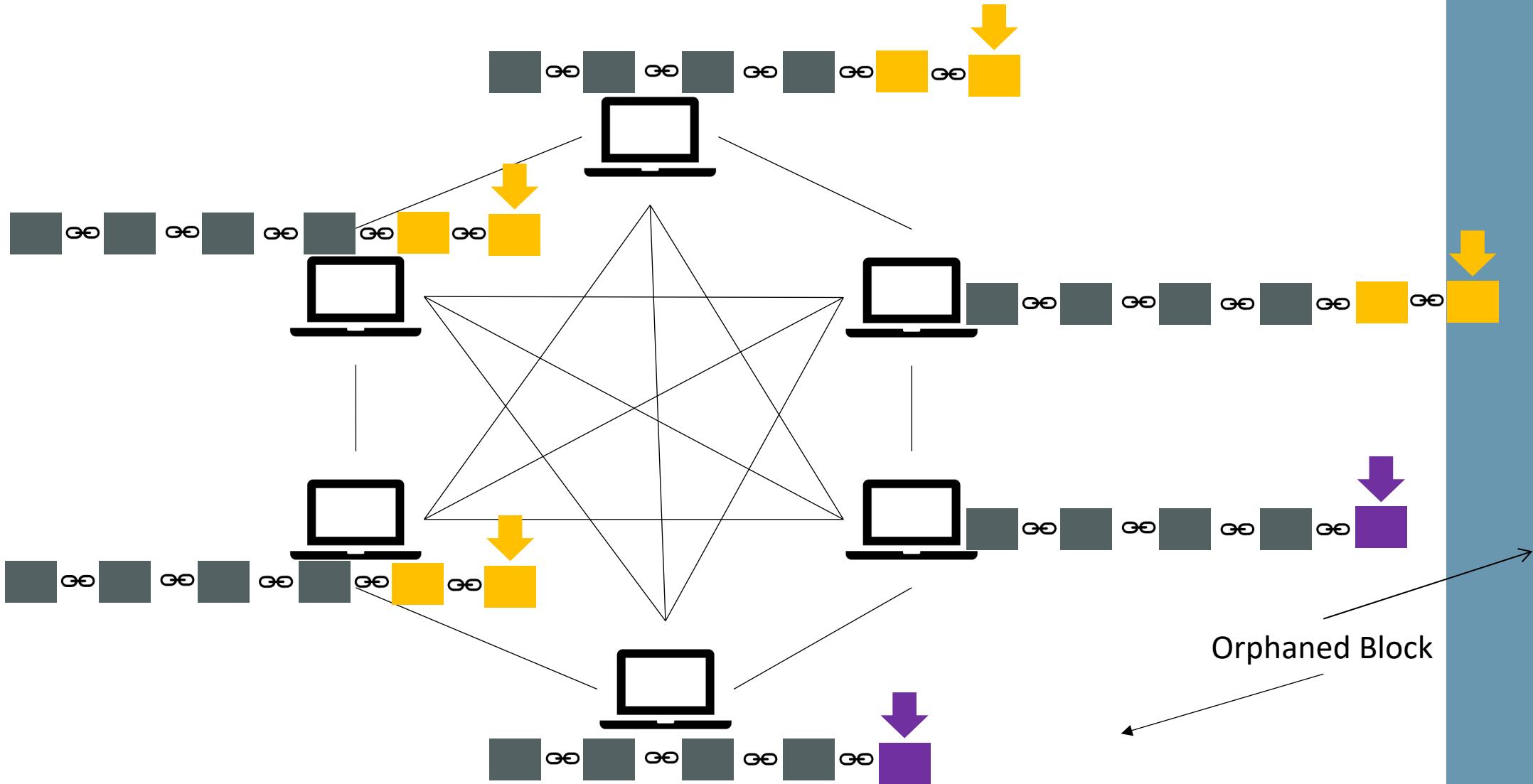
# Consensus Protocol



# Consensus Protocol



# Consensus Protocol



# Blockchain Components

Hash Cryptography

Immutable Ledger

Distributed P2P Network

Mining

Consensus Protocol

# References

- [1] Haber, Stuart, and W. Scott Stornetta. "How to time-stamp a digital document." Conference on the Theory and Application of Cryptography. Springer, Berlin, Heidelberg, 1990. [https://www.anf.es/pdf/Haber\\_Stornetta.pdf](https://www.anf.es/pdf/Haber_Stornetta.pdf)
- [2] Nakamoto, S. "Bitcoin: A P2P Electronic Cash System." (2009). <https://bitcoin.org/bitcoin.pdf>
- [3] Wouter, Penard, and Tim V. Werkhoven. "On the Secure Hash Algorithm family" Chapter one of Cryptography in Context, 2008. <https://webspace.science.uu.nl/~tel00101/liter/Books/CrypCont.pdf>