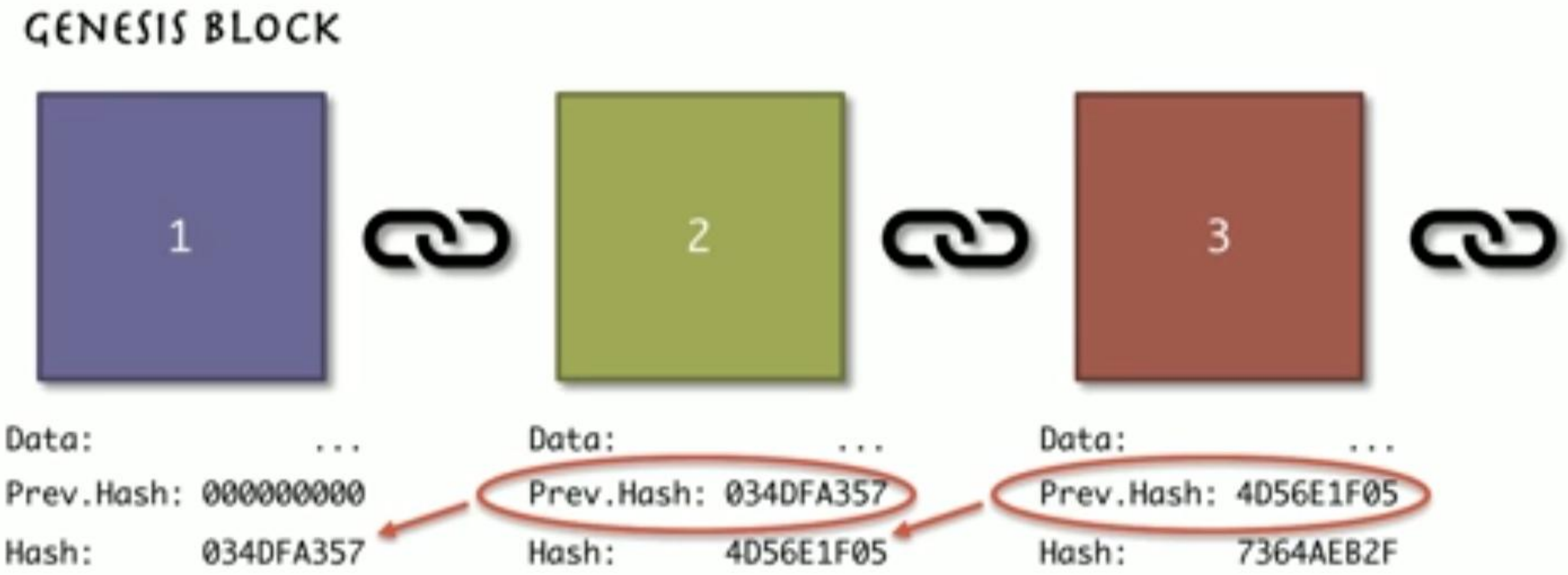
What we will learn in this section:

- What is a Blockchain?
- Understanding SHA256 Hash
- Immutable Ledger
- Distributed P2P Network
- How Mining Works (Part 1: The Nonce)
- How Mining Works (Part 2: The cryptographic puzzle)
- Byzantine Fault Tolerance
- Consensus Protocol (Part 1: Defense against attackers)
- Consensus Protocol (Part 2: Competing chains)
- Blockchain Demo

> A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography.
>
> – *Wikipedia*

1. Data: “Hello World!”
2. Prev.Hash: 034DFA357
3. Hash: 4D56E1F05

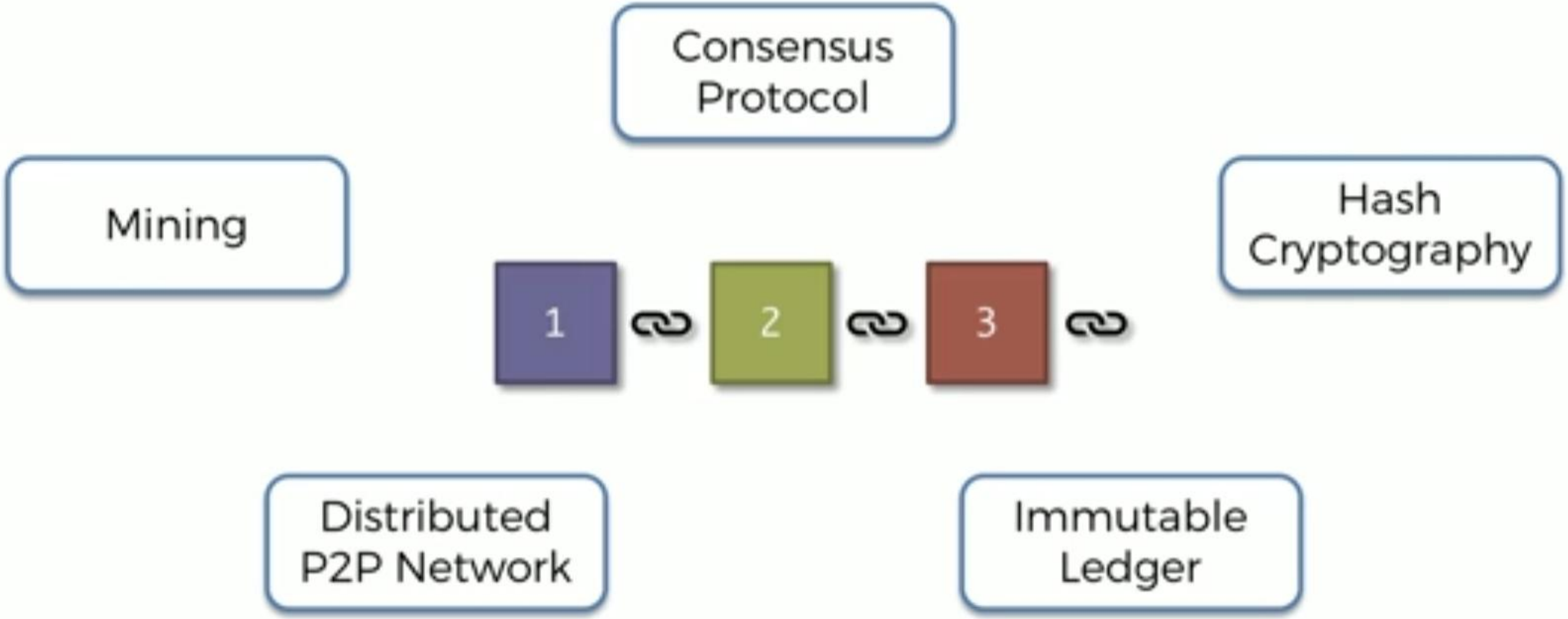


GENESIS BLOCK

Data: ...
Prev.Hash: 000000000
Hash: 034DFA357

Data: ...
Prev.Hash: 034DFA357
Hash: 4D56E1F05

Data: ...
Prev.Hash: 4D56E1F05
Hash: 7364AEB2F



Consensus Protocol

Mining

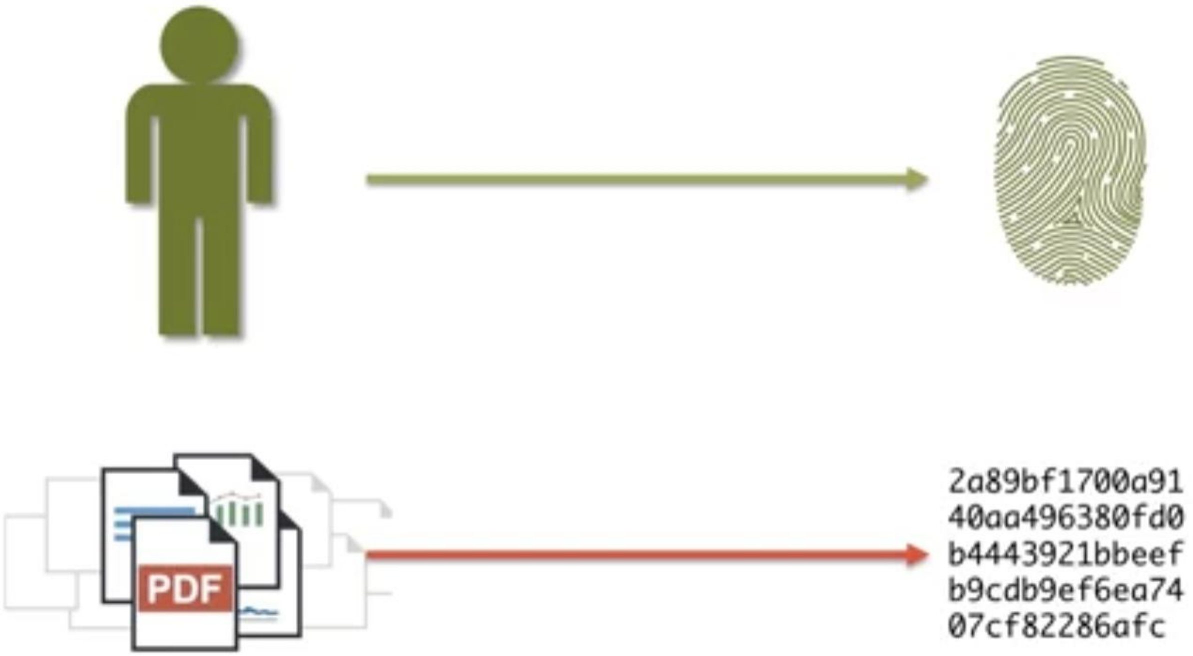
Hash Cryptography

Distributed P2P Network

Immutable Ledger

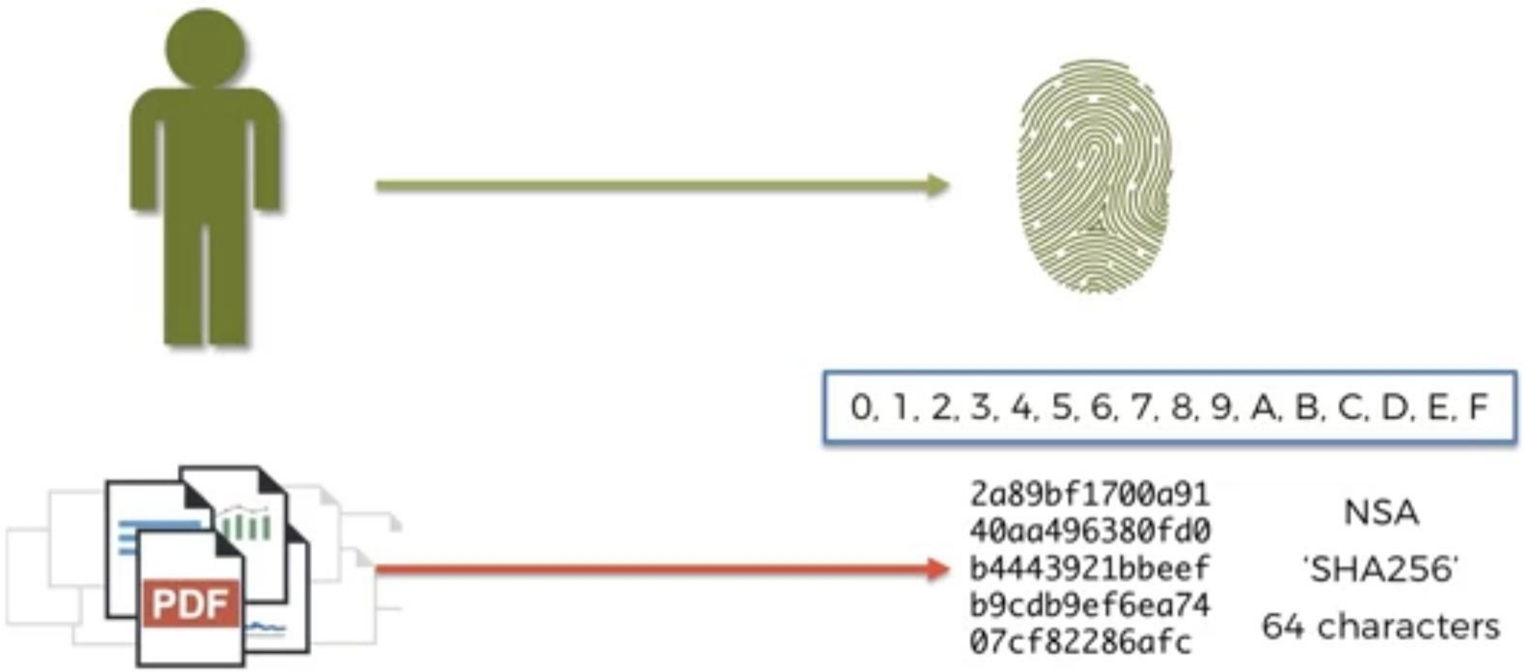
Understanding SHA256 Hash

Understanding SHA256 Hash



```
2a89bf1700a91
40aa496380fd0
b4443921bbeef
b9cdb9ef6ea74
07cf82286afc
```

Understanding SHA256 Hash



0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

```
2a89bf1700a91
40aa496380fd0
b4443921bbeef
b9cdb9ef6ea74
07cf82286afc
```

NSA

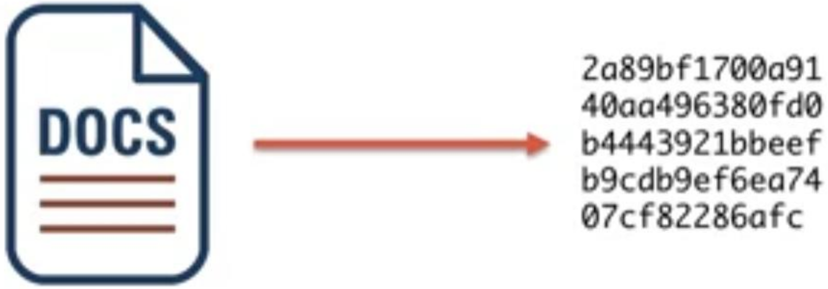
‘SHA256’

64 characters

Understanding SHA256 Hash

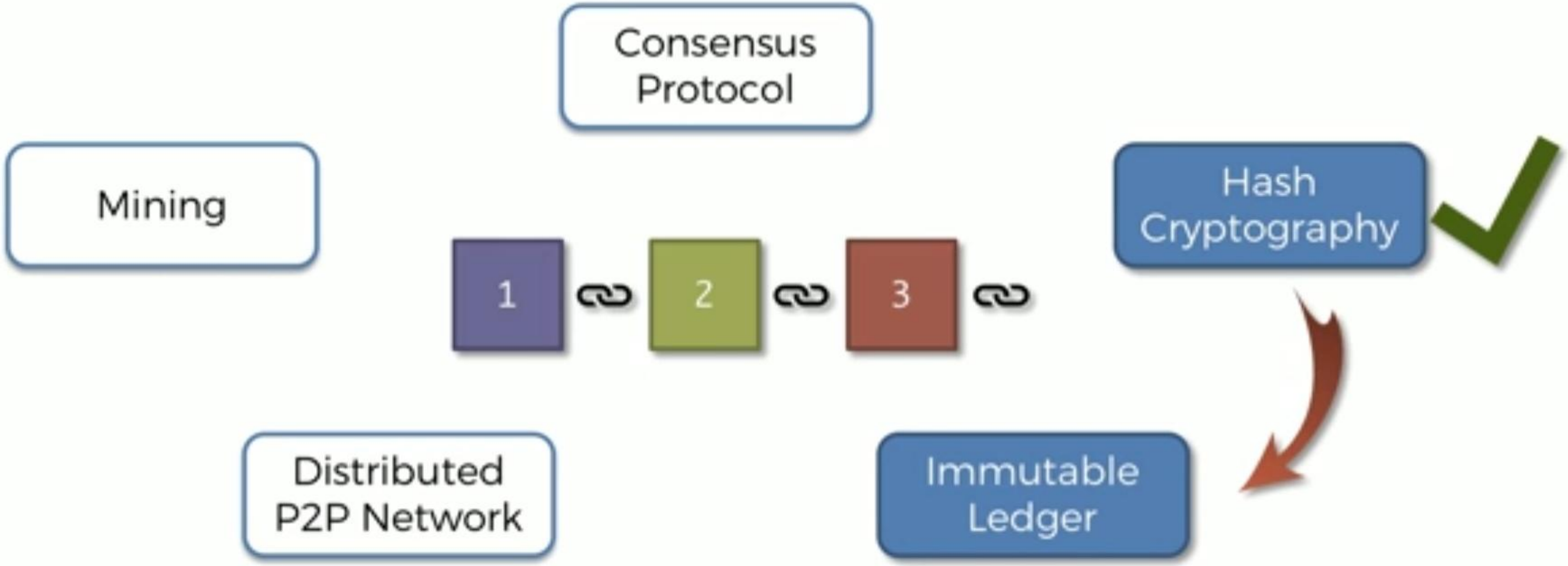
The 5 requirements for Hash algorithms:

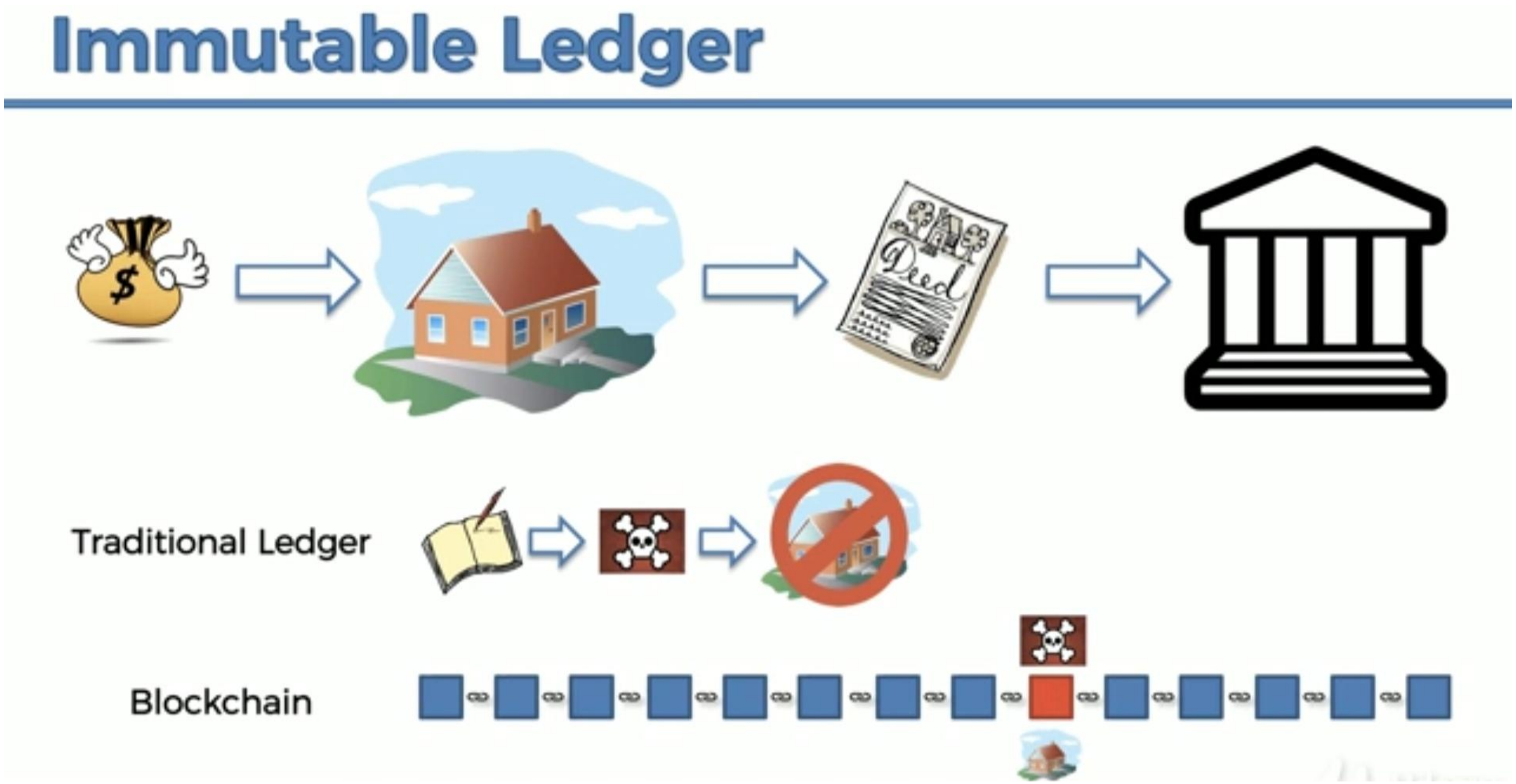
1. One-Way
2. Deterministic
3. Fast Computation
4. The Avalanche Effect
5. Must withstand collisions



```
2a89bf1700a91
40aa496380fd0
b4443921bbeef
b9cdb9ef6ea74
07cf82286afc
```

Immutable Ledger



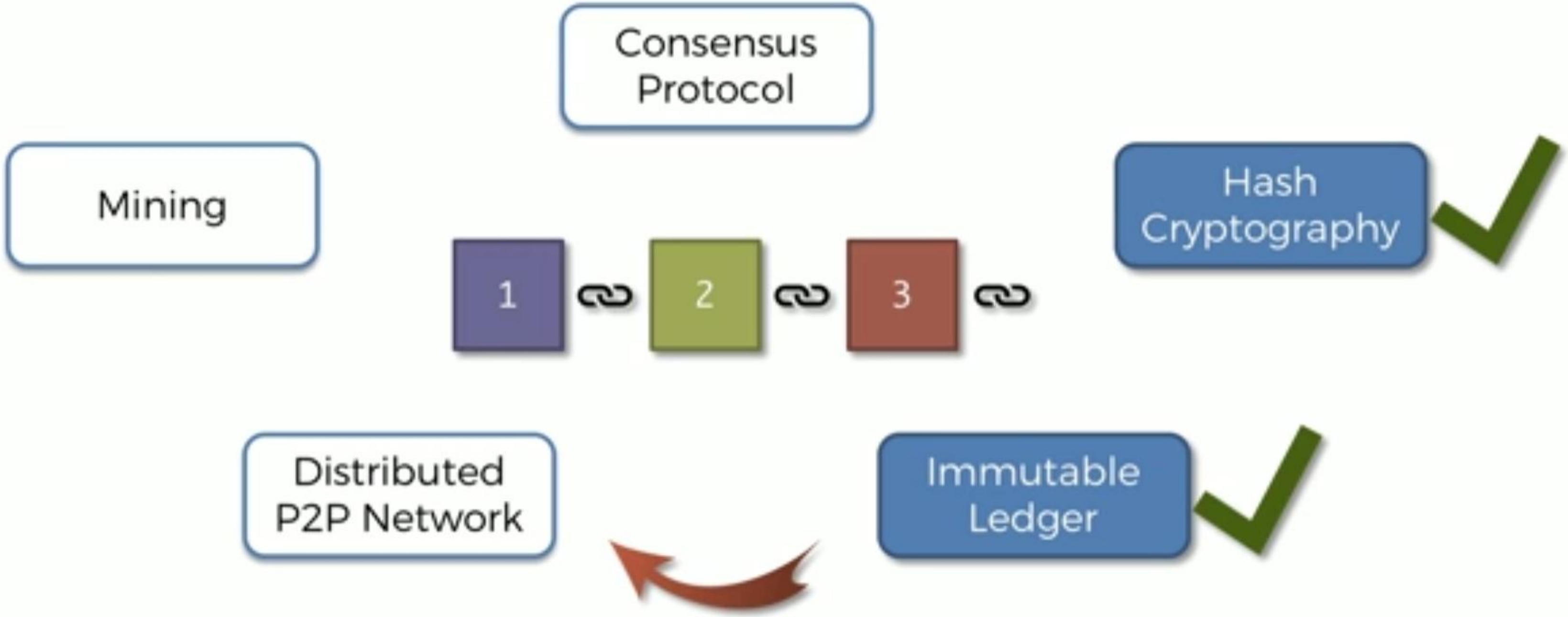


Immutable Ledger

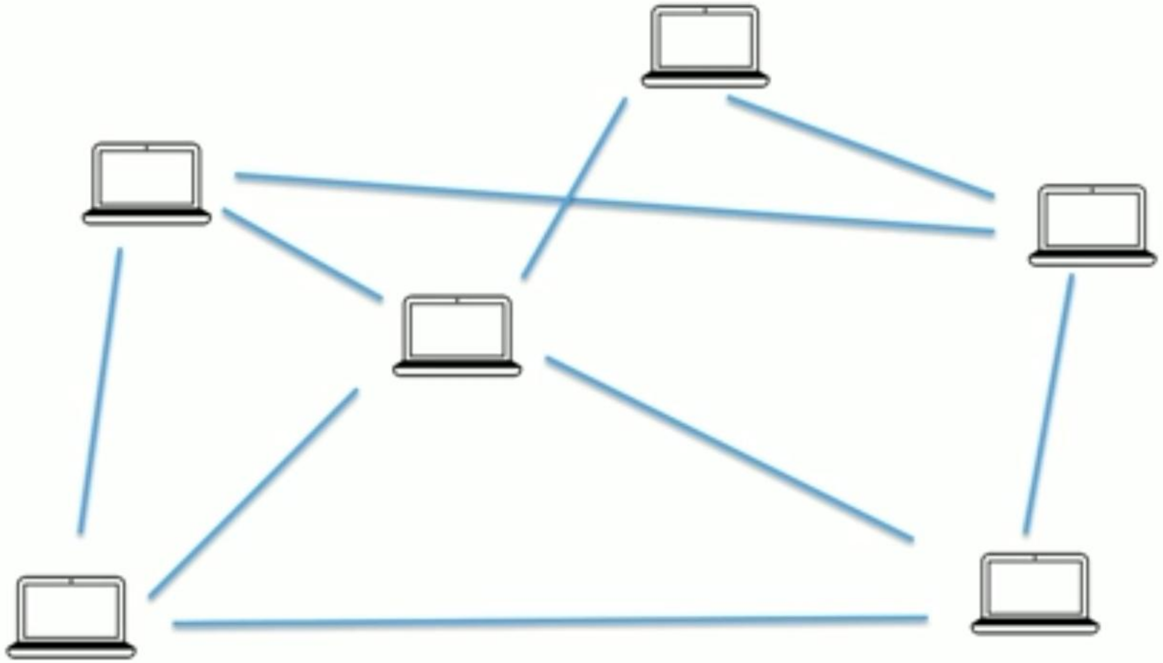
Traditional Ledger

Blockchain

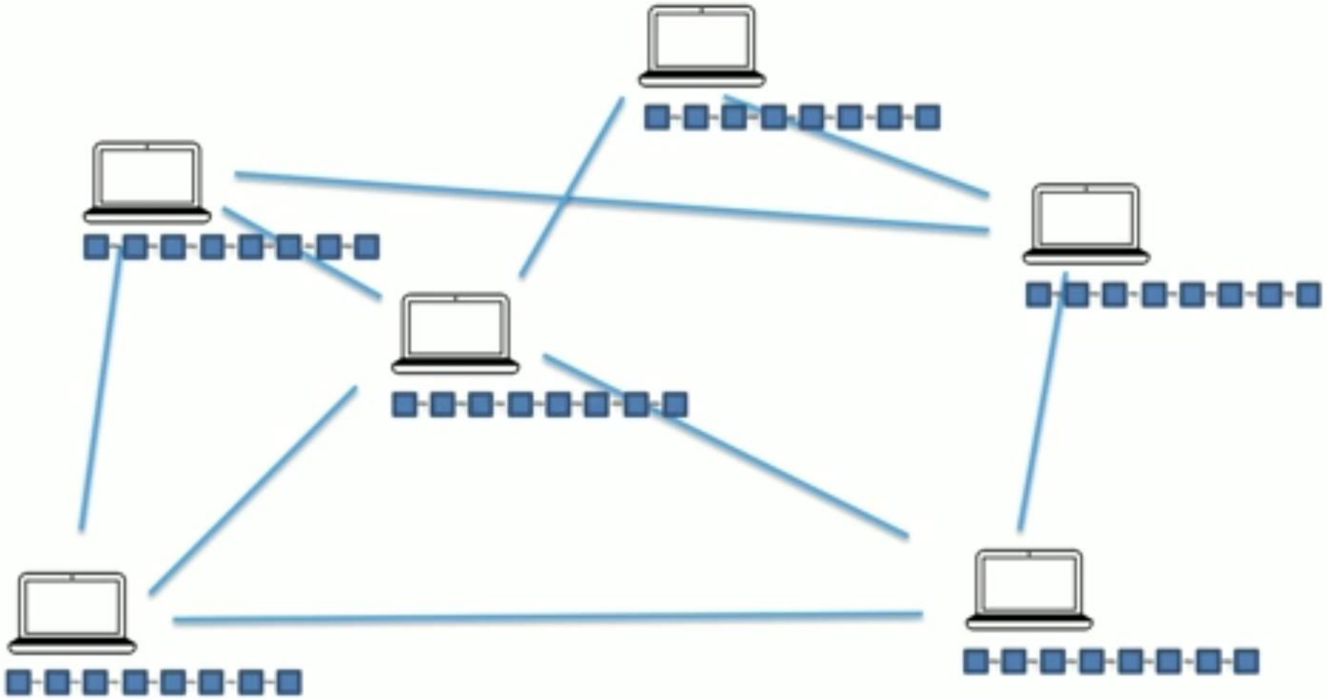
Distributed P2P Network



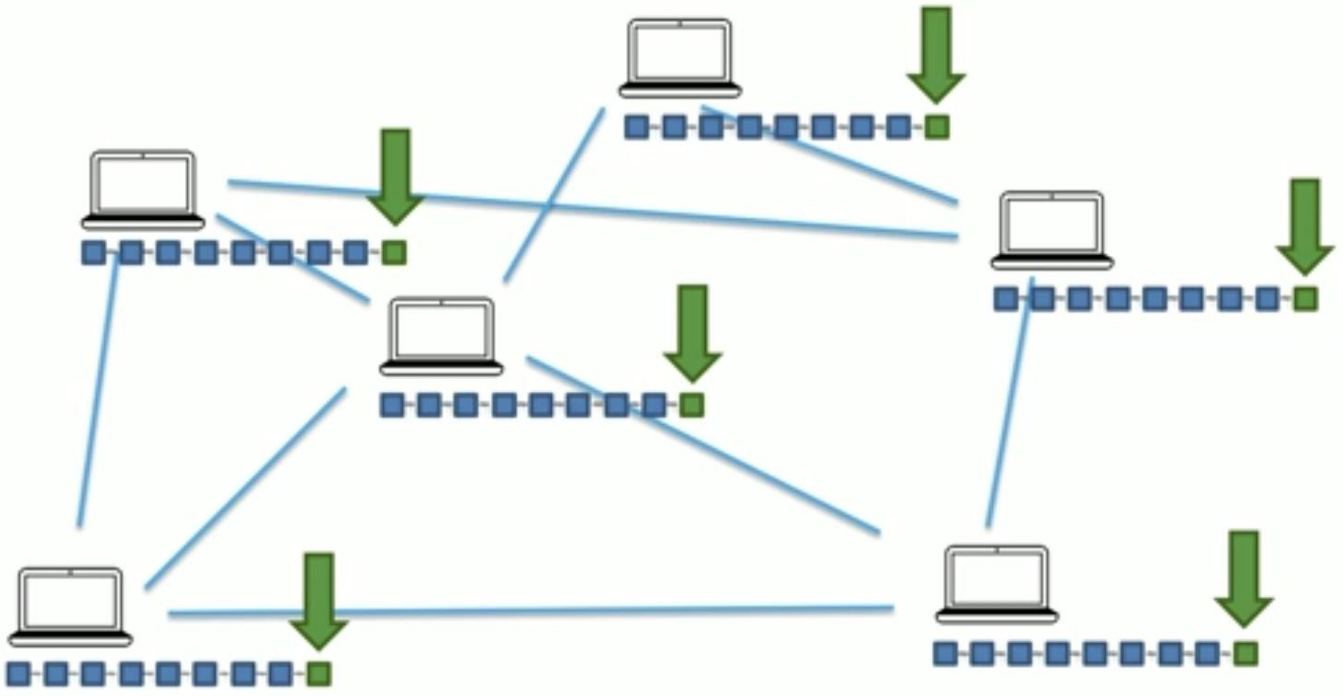
Distributed P2P Network



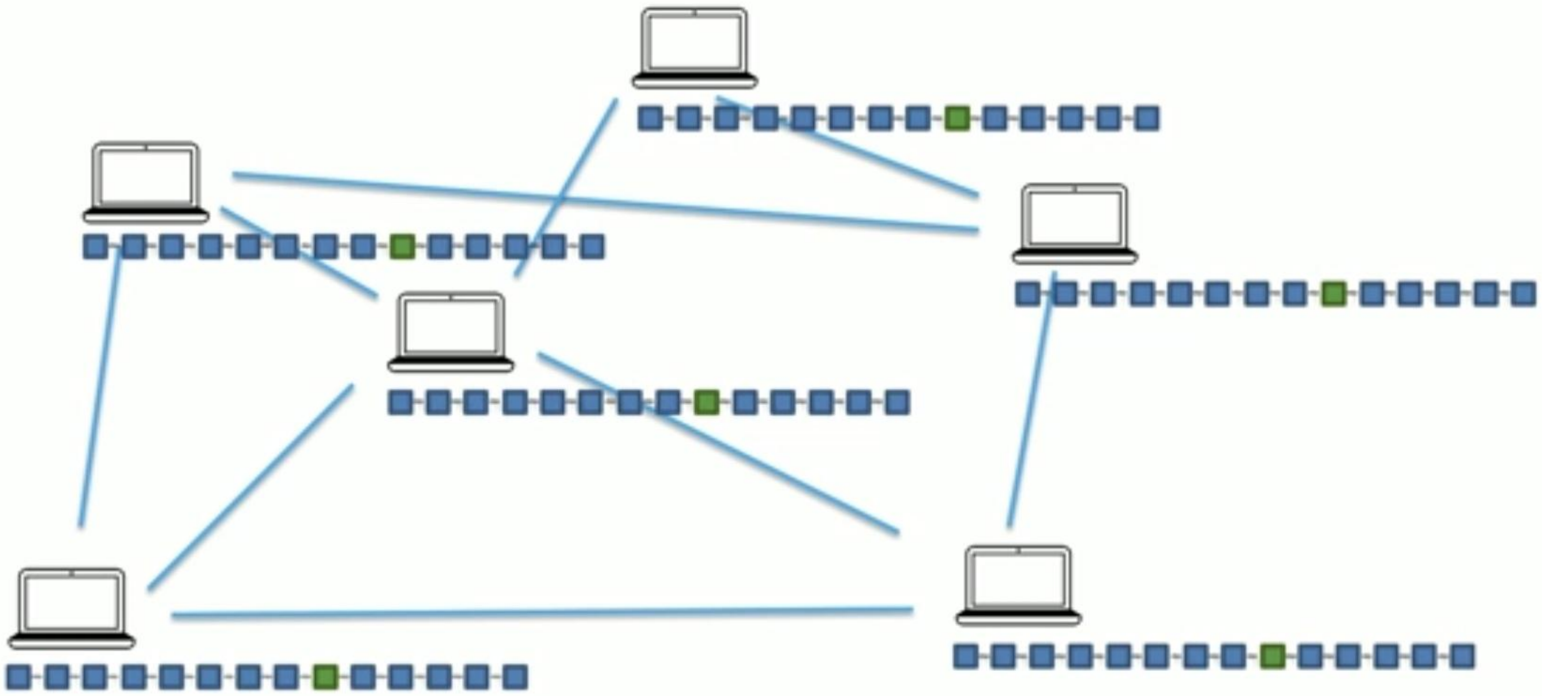
Distributed P2P Network



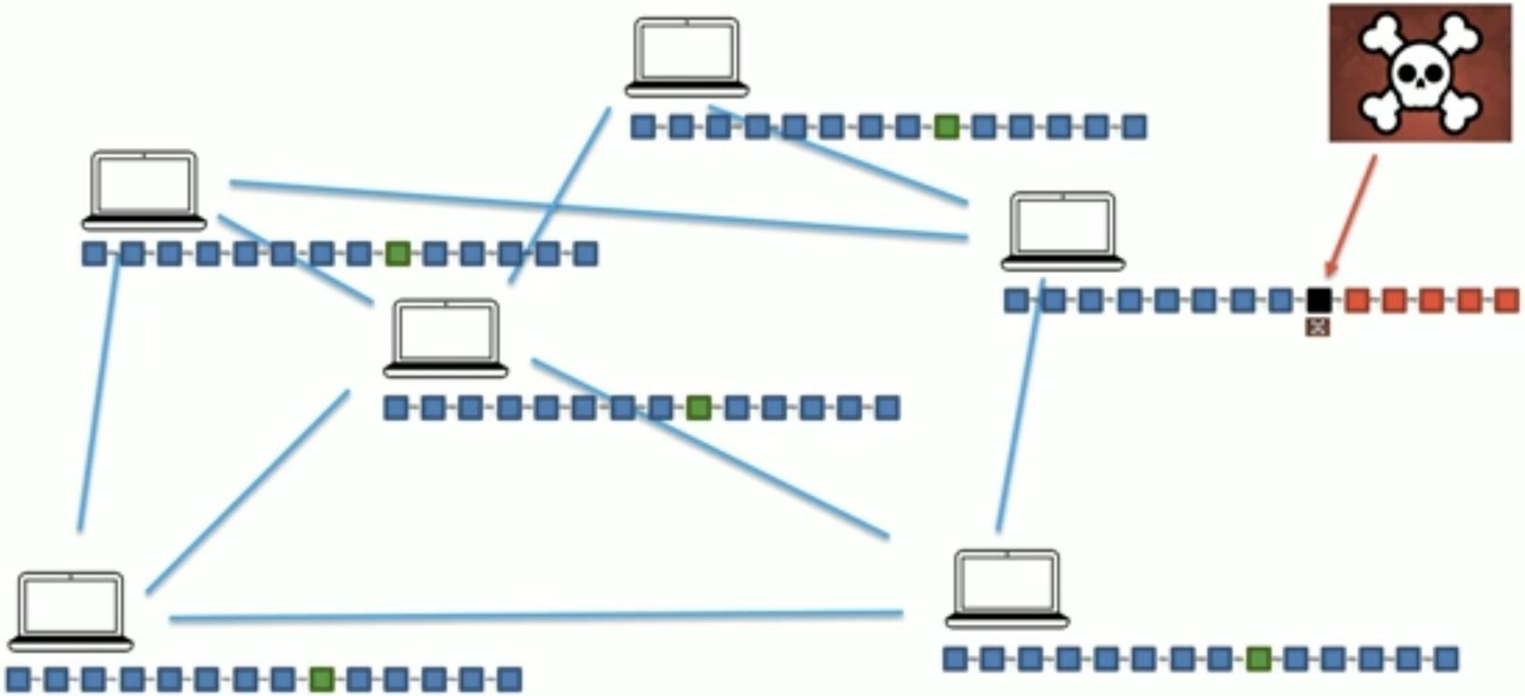
Distributed P2P Network



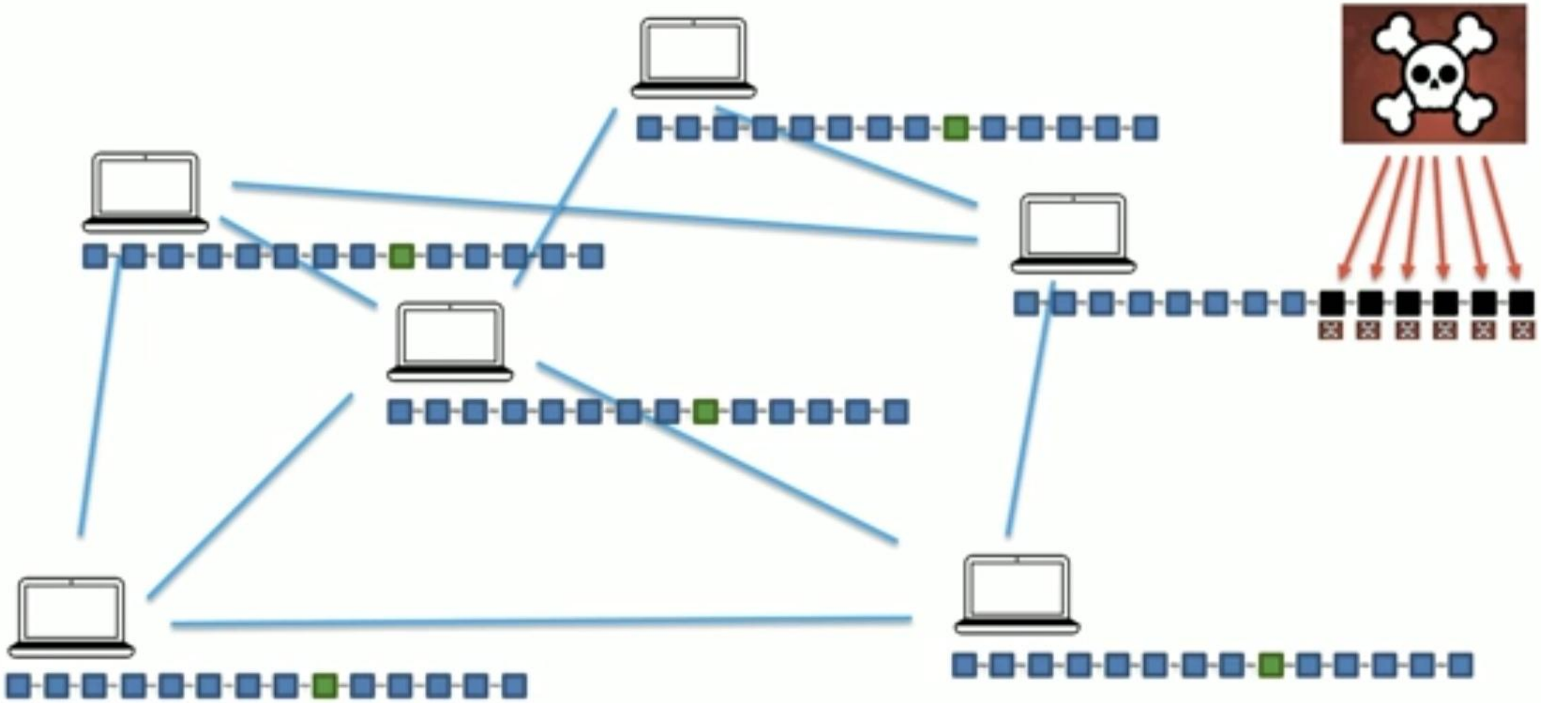
Distributed P2P Network



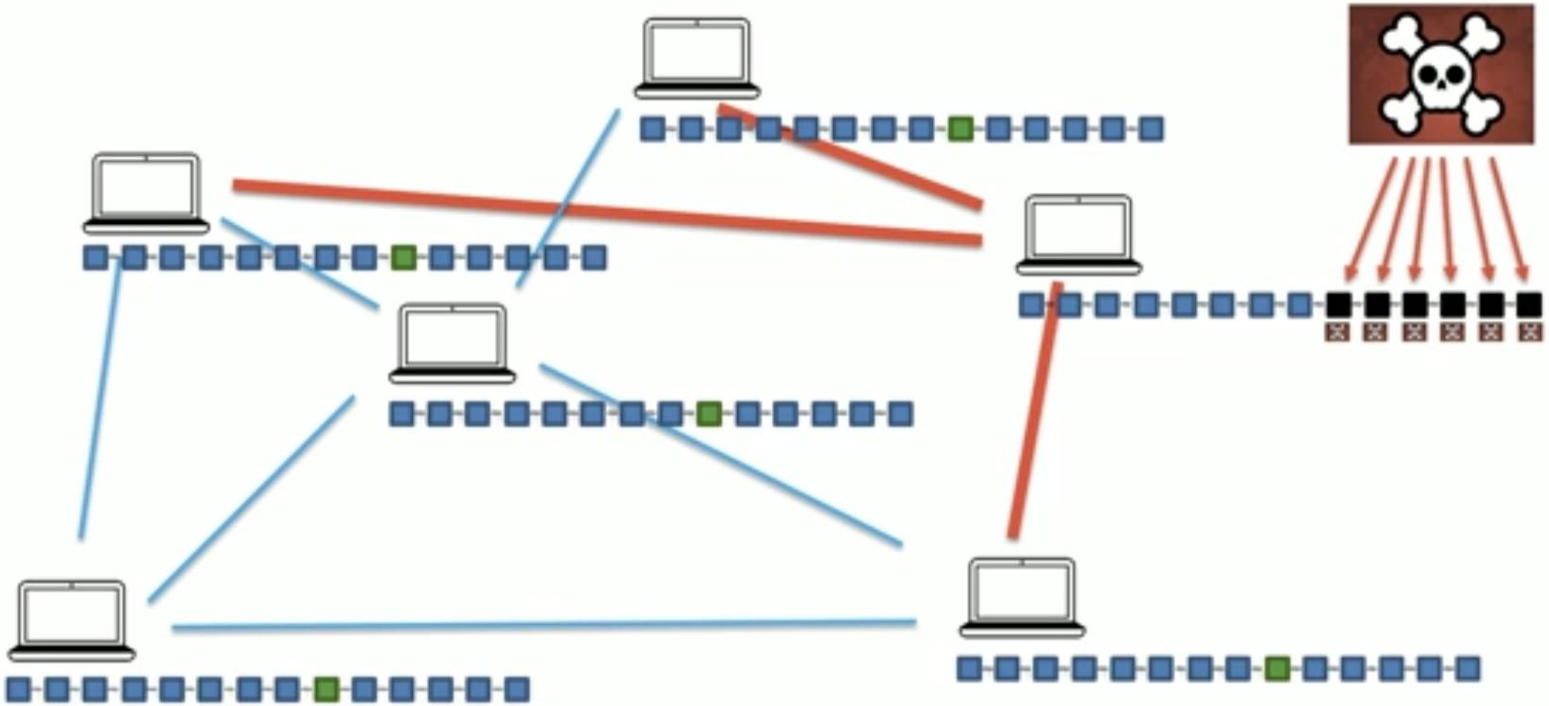
Distributed P2P Network



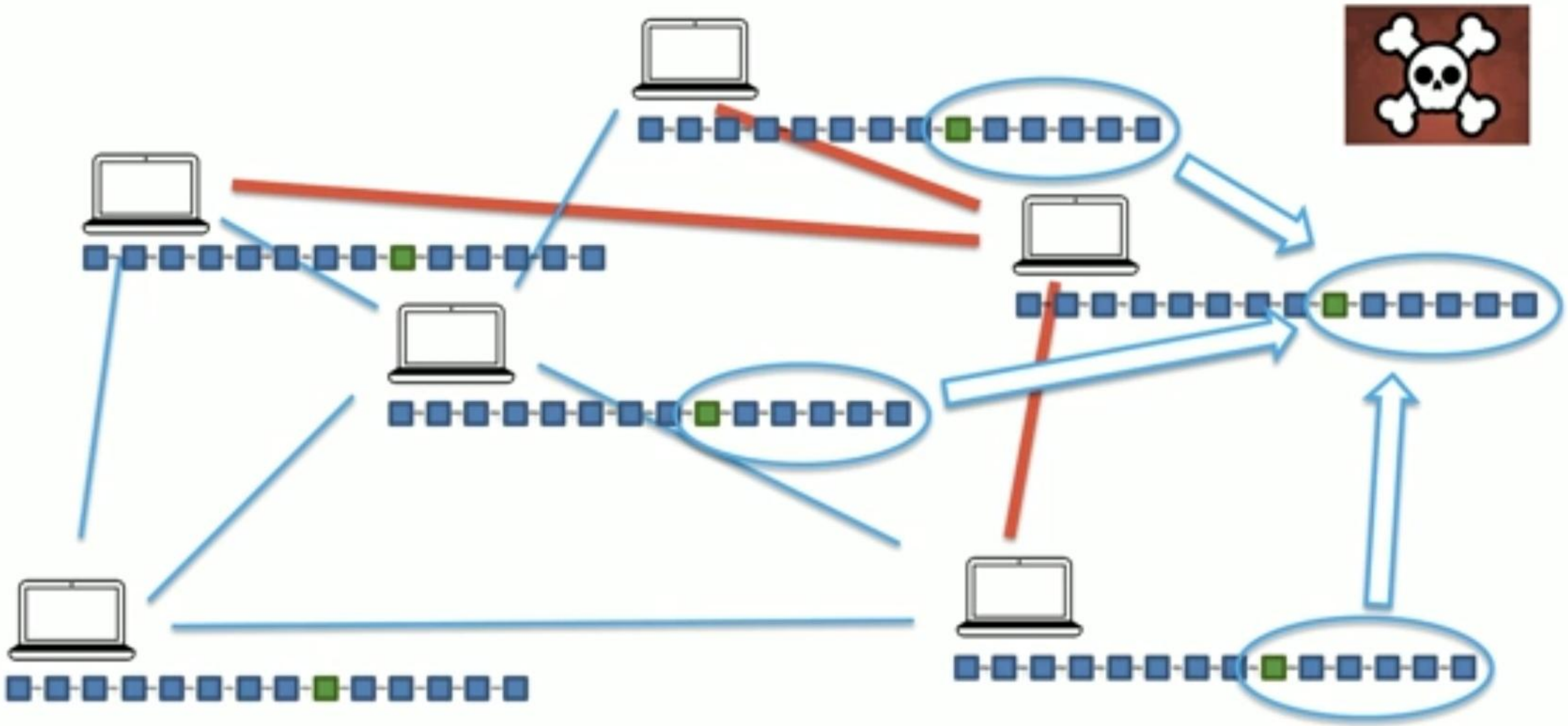
Distributed P2P Network



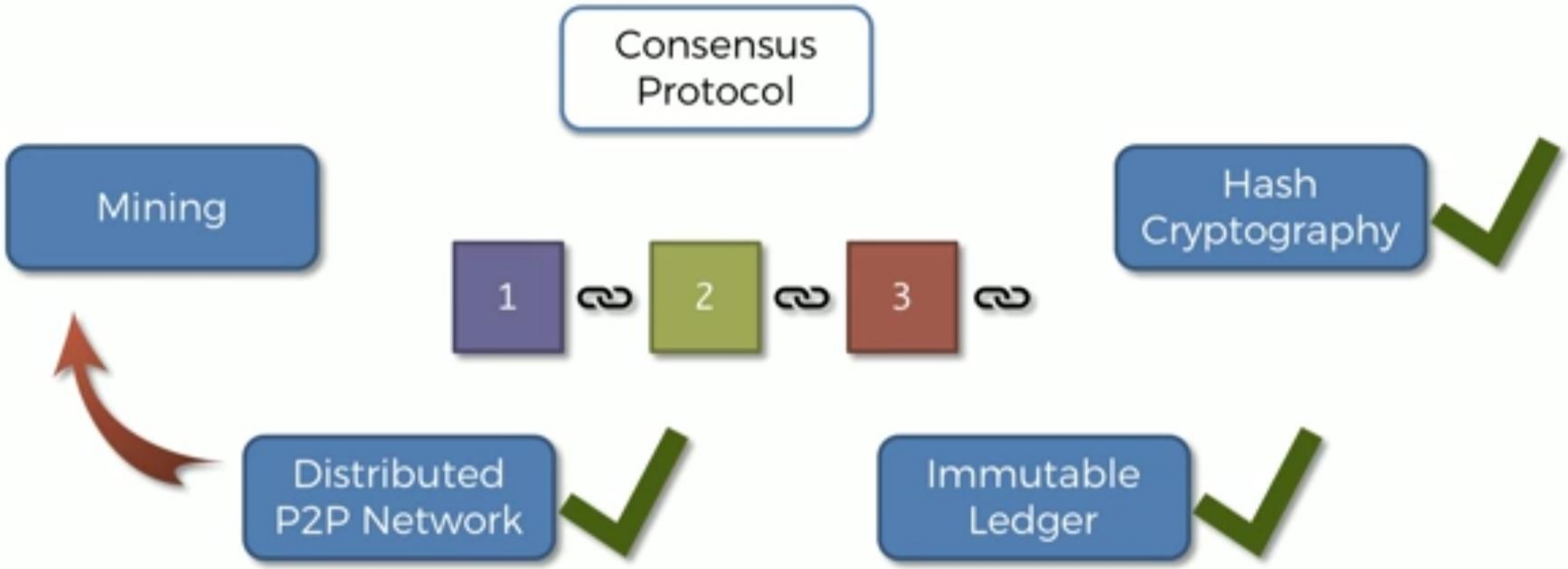
Distributed P2P Network



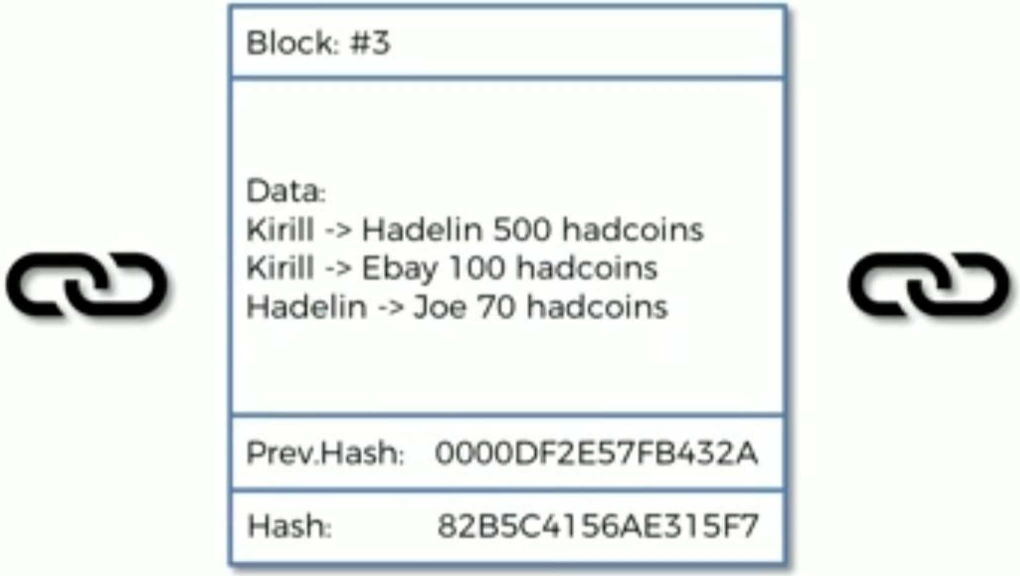
Distributed P2P Network



How Mining Works



How Mining Works



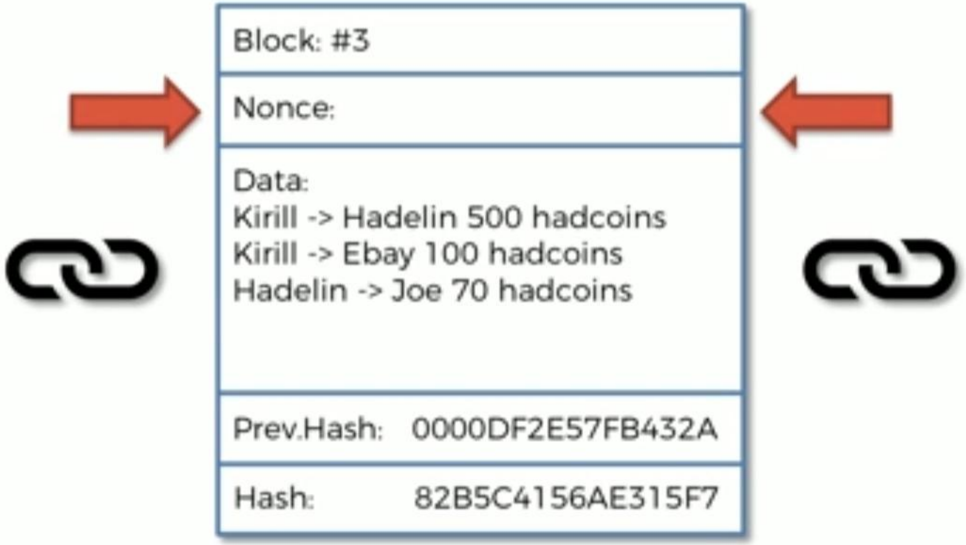
Block: #3

Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins

Prev.Hash: 0000DF2E57FB432A

Hash: 82B5C4156AE315F7

How Mining Works



Block: #3

Nonce:

Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins

Prev.Hash: 0000DF2E57FB432A

Hash: 82B5C4156AE315F7

How Mining Works

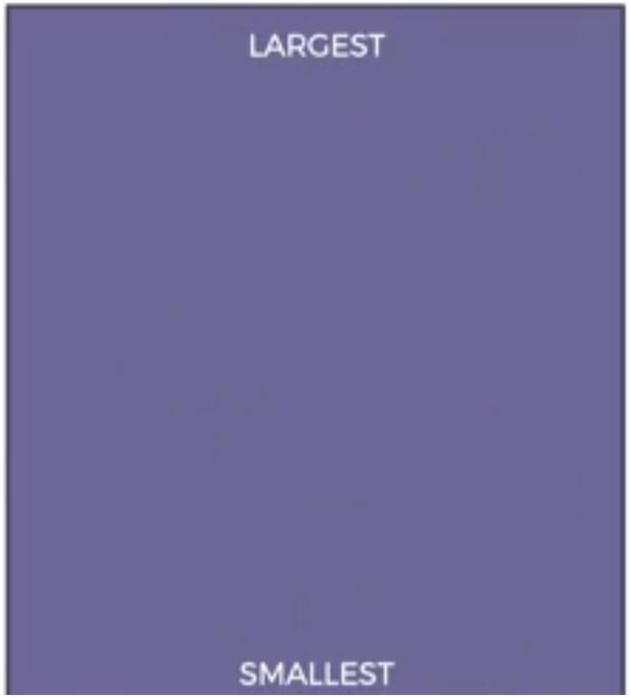
A Hash is a Number

```
18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68
          =11232962686236154915841062771303455665105266333
                            445130312258268457057784990824

000000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923
          =00000000000000218420711603109937116824492054445
                            852323869008912526075378993443

0000000000000000000000000000000000000159CAA4B1EDA0FED66CB5E915C8F
          =00000000000000000000000000000000000000000000438
                            342898295709947707018187988111
```

- ALL POSSIBLE HASHES -



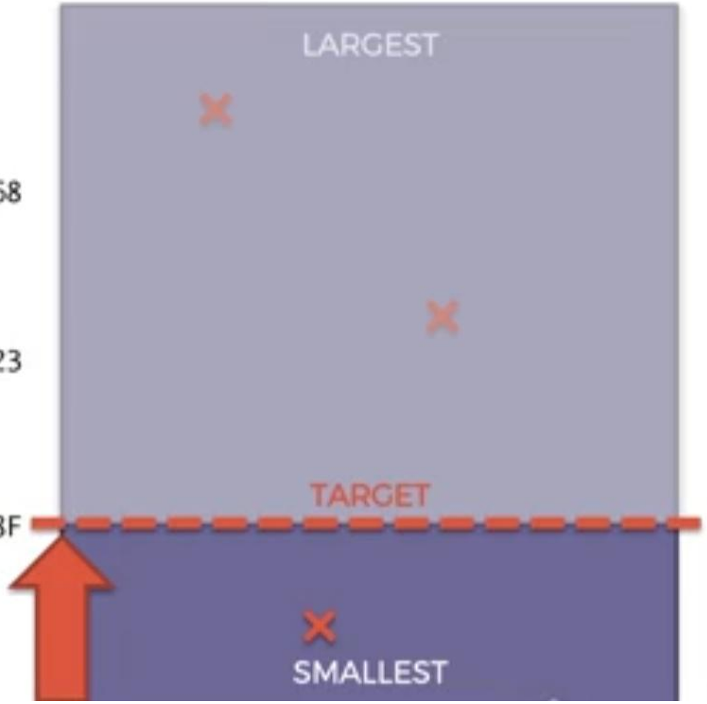
How Mining Works

18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

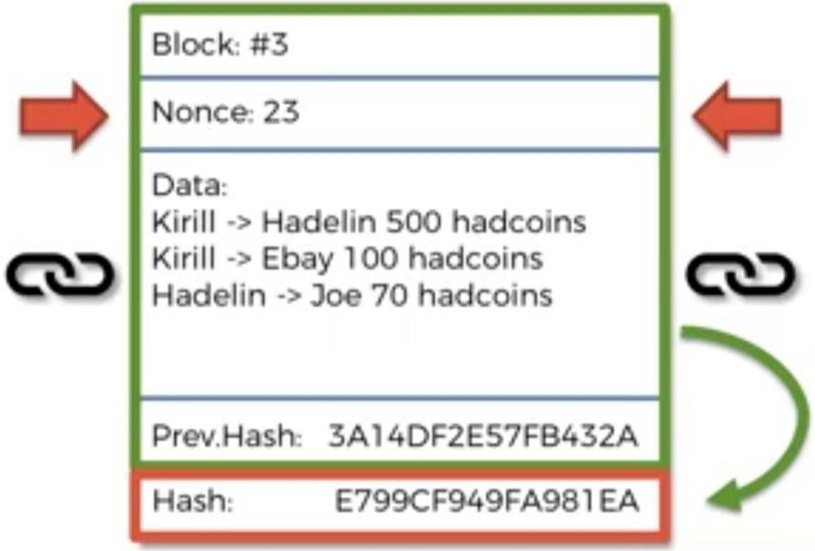
000000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

0000000000000000000000000000000000159CAA4B1EDA0FED66CB5E915C8F

- ALL POSSIBLE HASHES -



How Mining Works



Block: #3

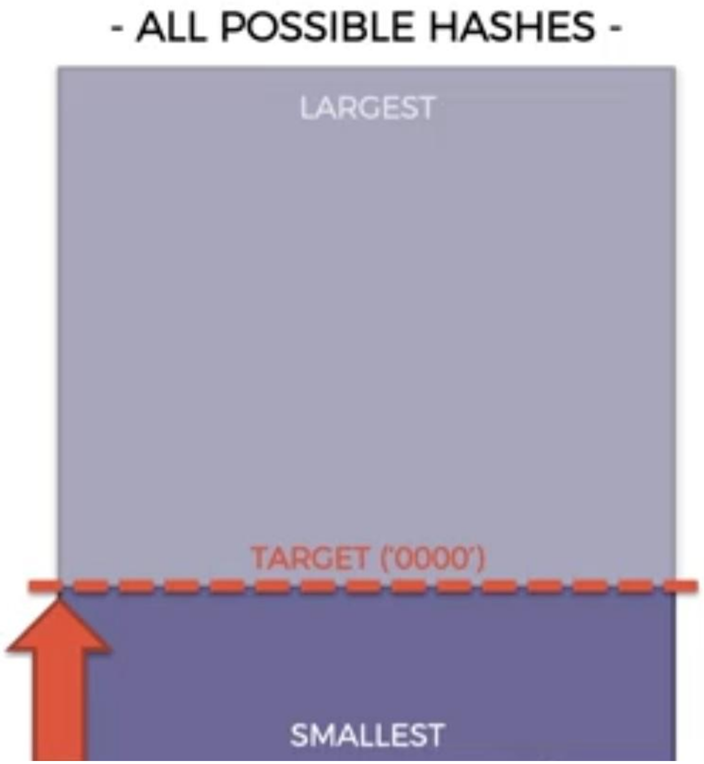
Nonce: 23

Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins

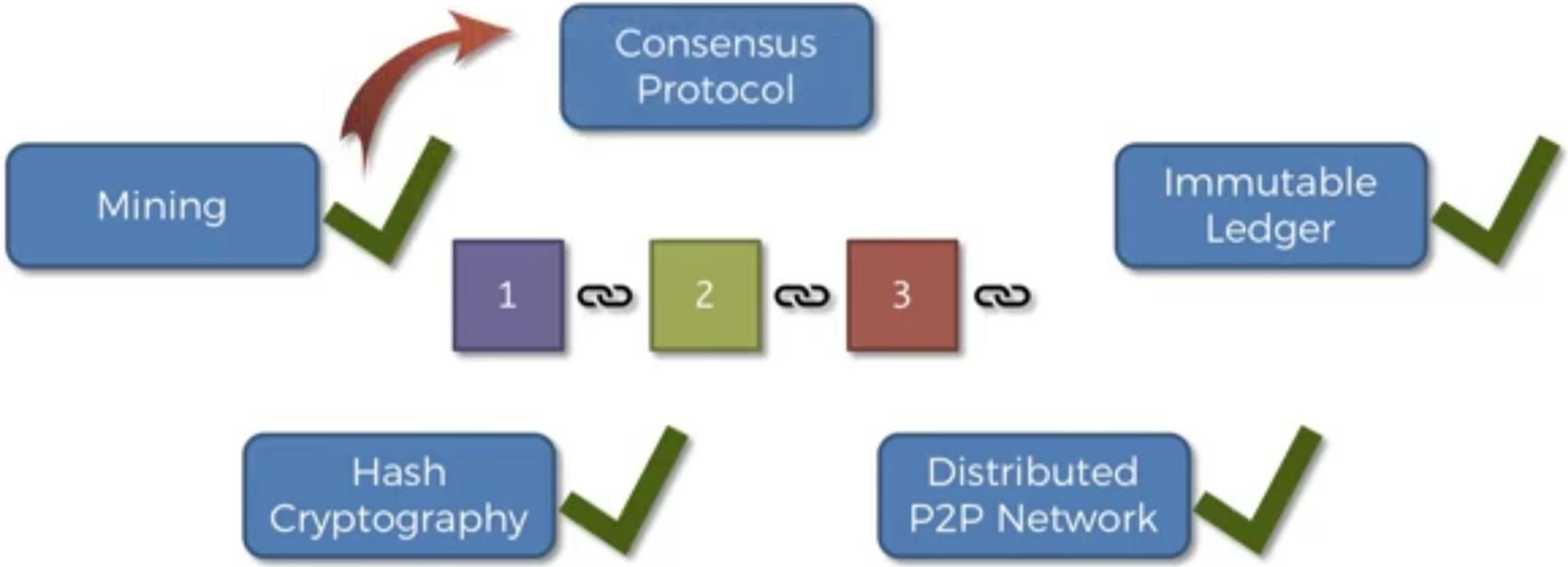
Prev.Hash: 3A14DF2E57FB432A

Hash: E799CF949FA981EA

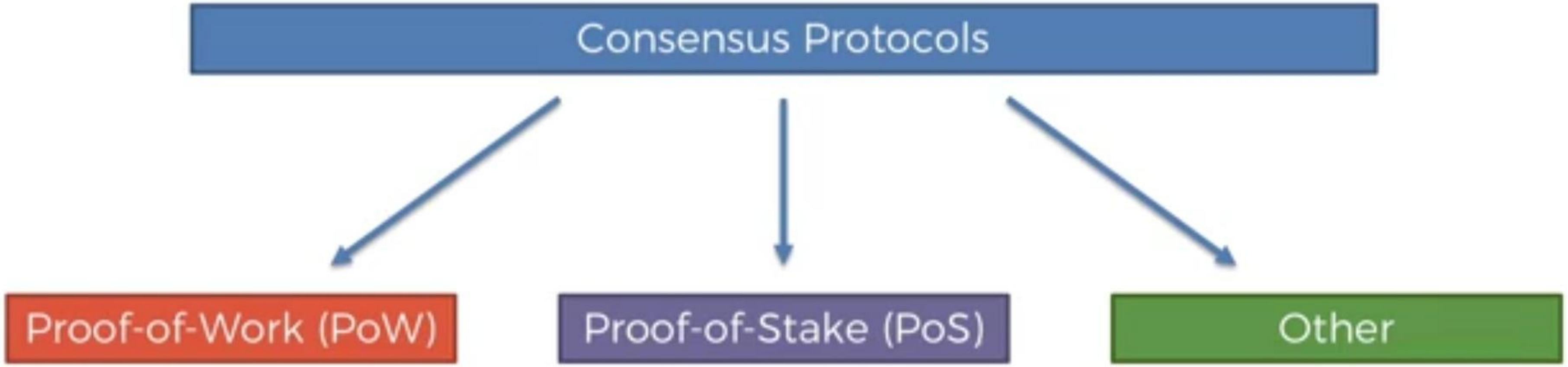
TIP: Express Target with leading Zeroes
E.g. '0000'



Consensus Protocol



Consensus Protocol



Consensus Protocols

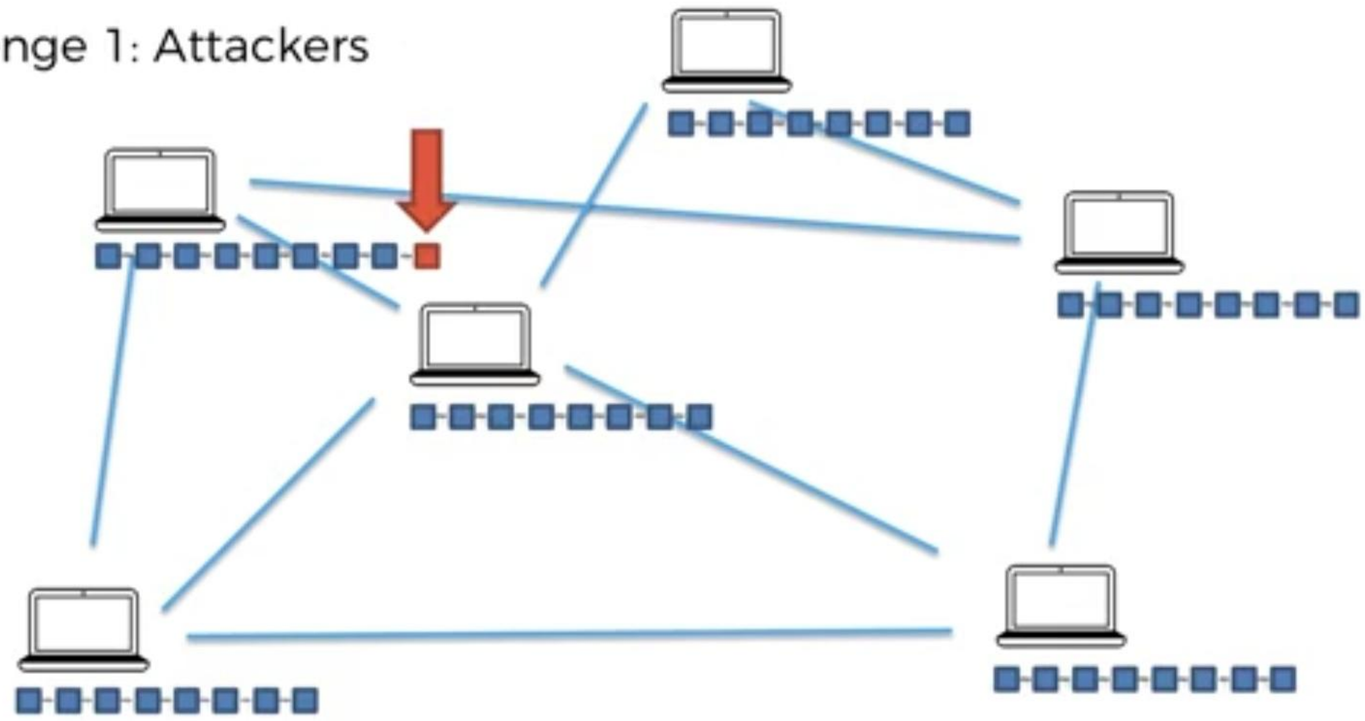
Proof-of-Work (PoW)

Proof-of-Stake (PoS)

Other

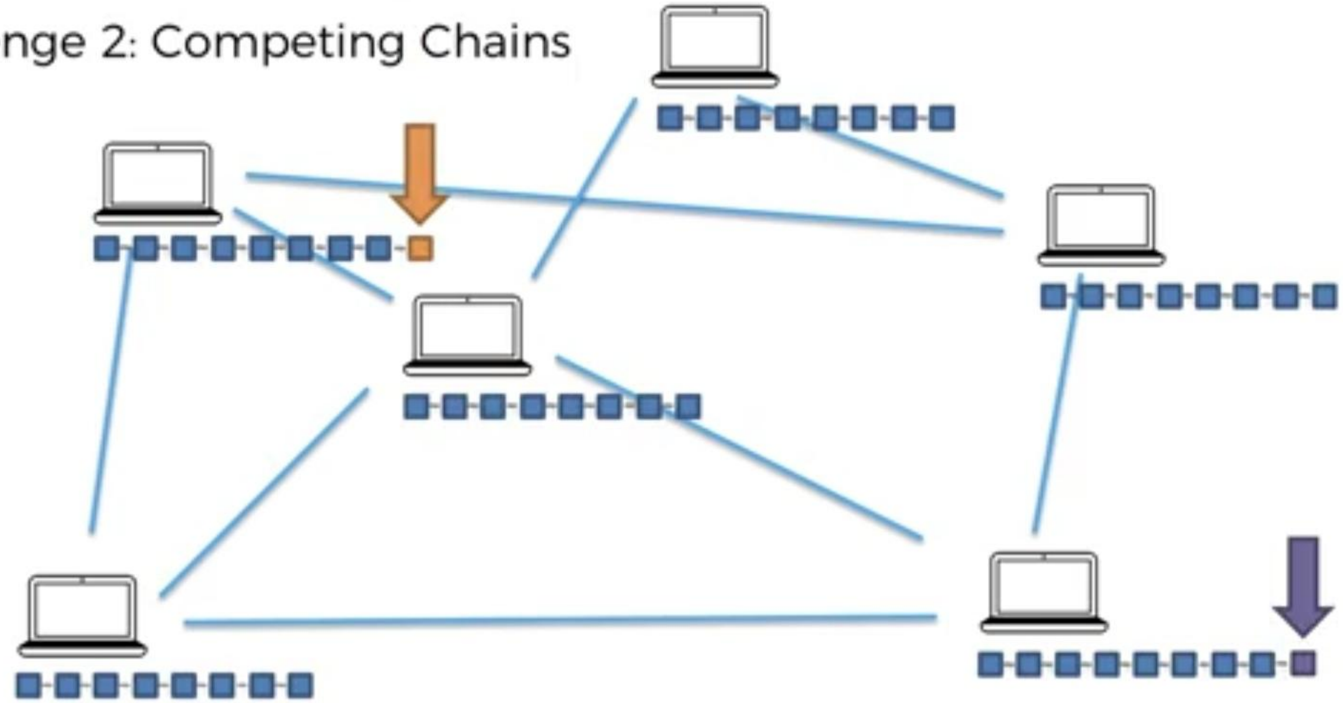
Consensus Protocol

Challenge 1: Attackers

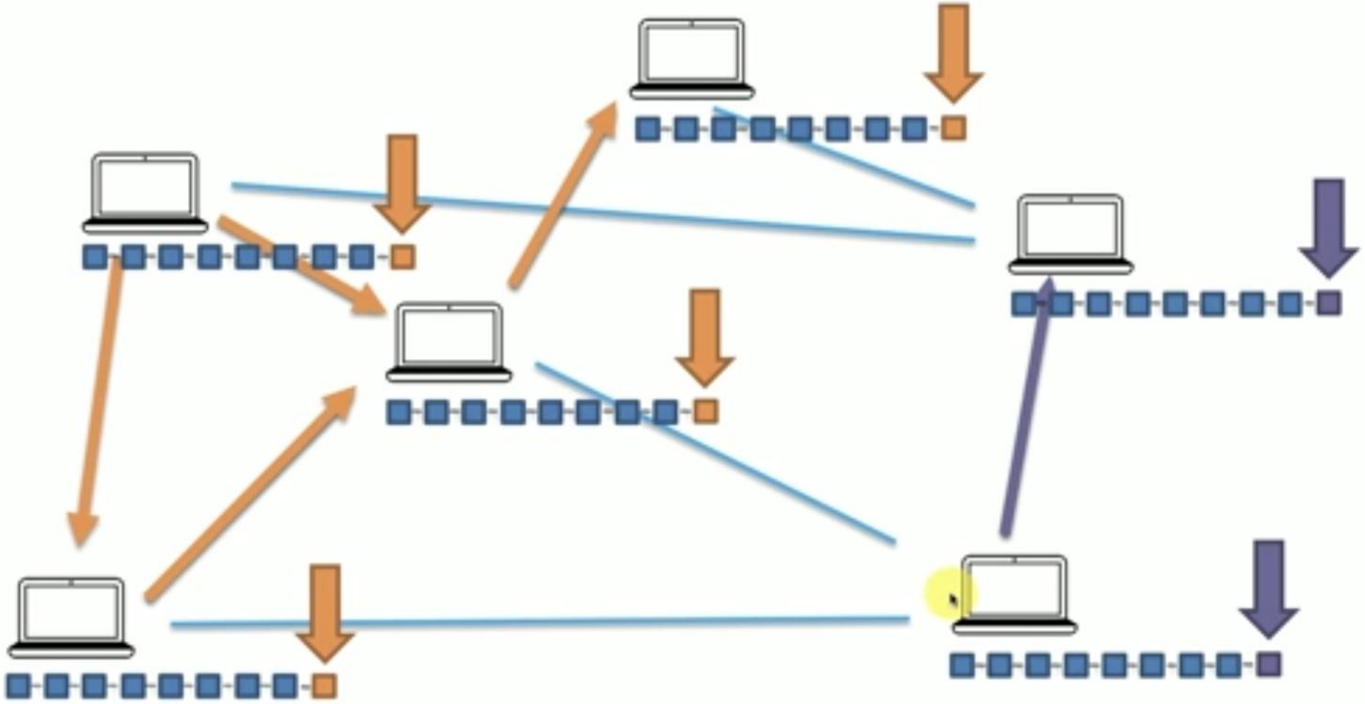


Consensus Protocol

Challenge 2: Competing Chains



Consensus Protocol



Consensus Protocol