Blockchain and Cryptocurrency

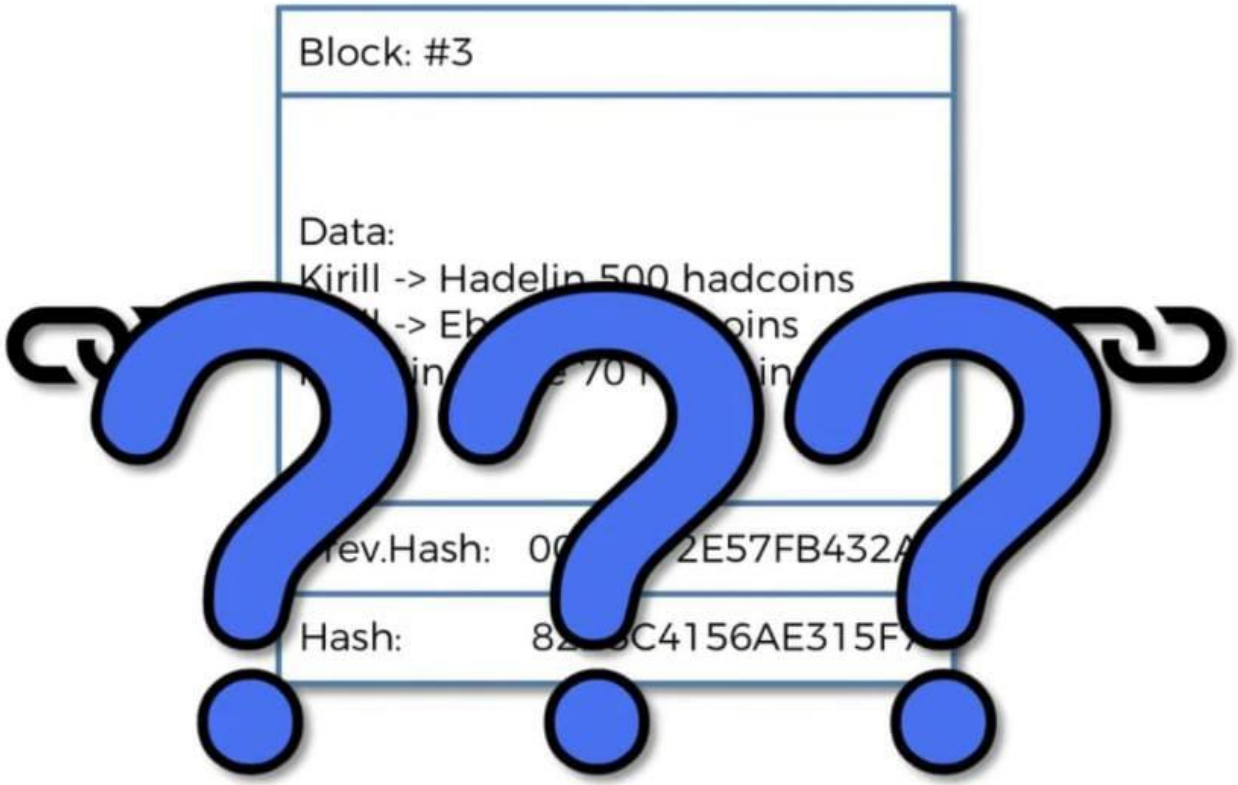
By: Syeda Tayyaba Bukhari

How mining works?
(The Nonce)

Information that a Block has:

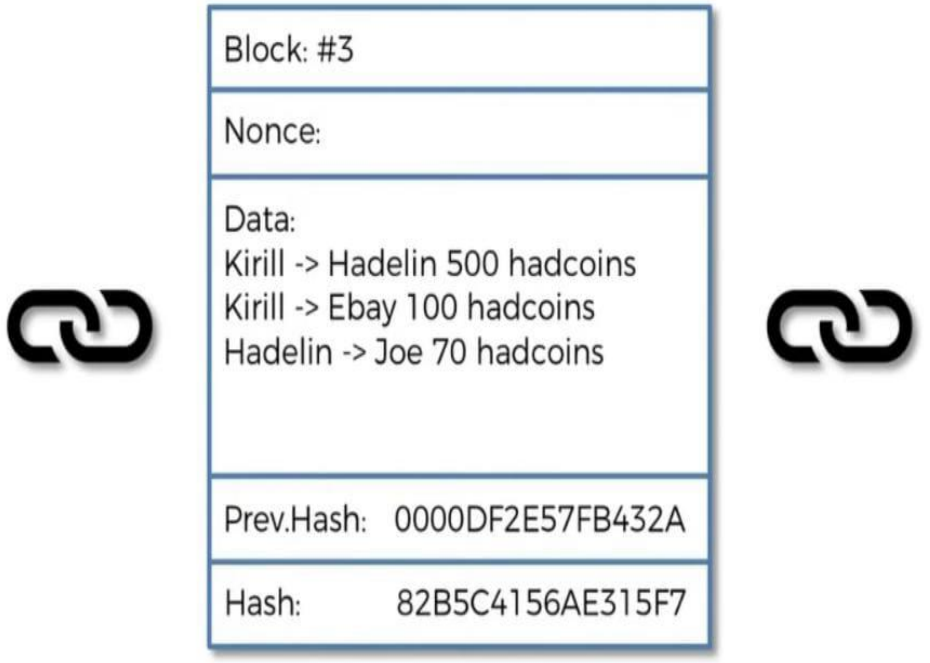
Computing Hash of a Block

If a generation of hash is this much simple, then for what the miners are in race ?



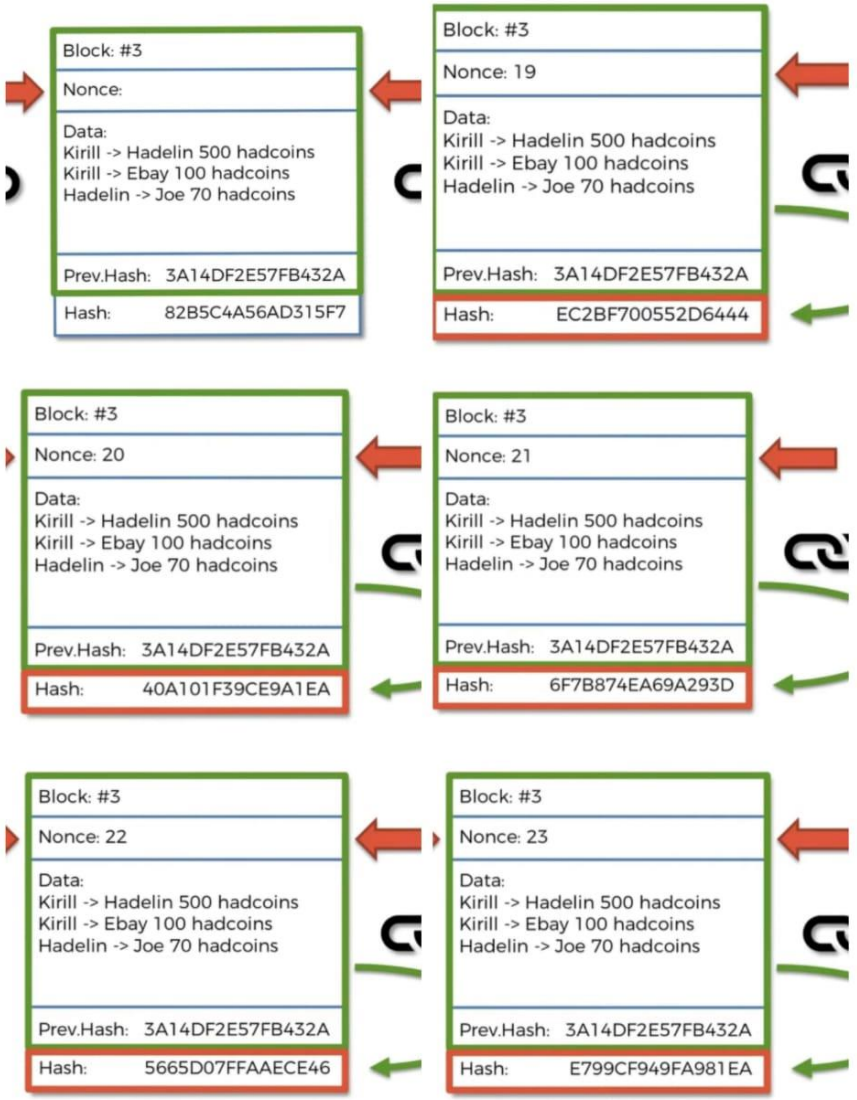
The Nonce

- Nonce: Number only used once
- Nonce is also included in computing the Hash along with Block Number, Data and Previous Hash
- The nonce keeps on changing which results in the changing of the Hash.

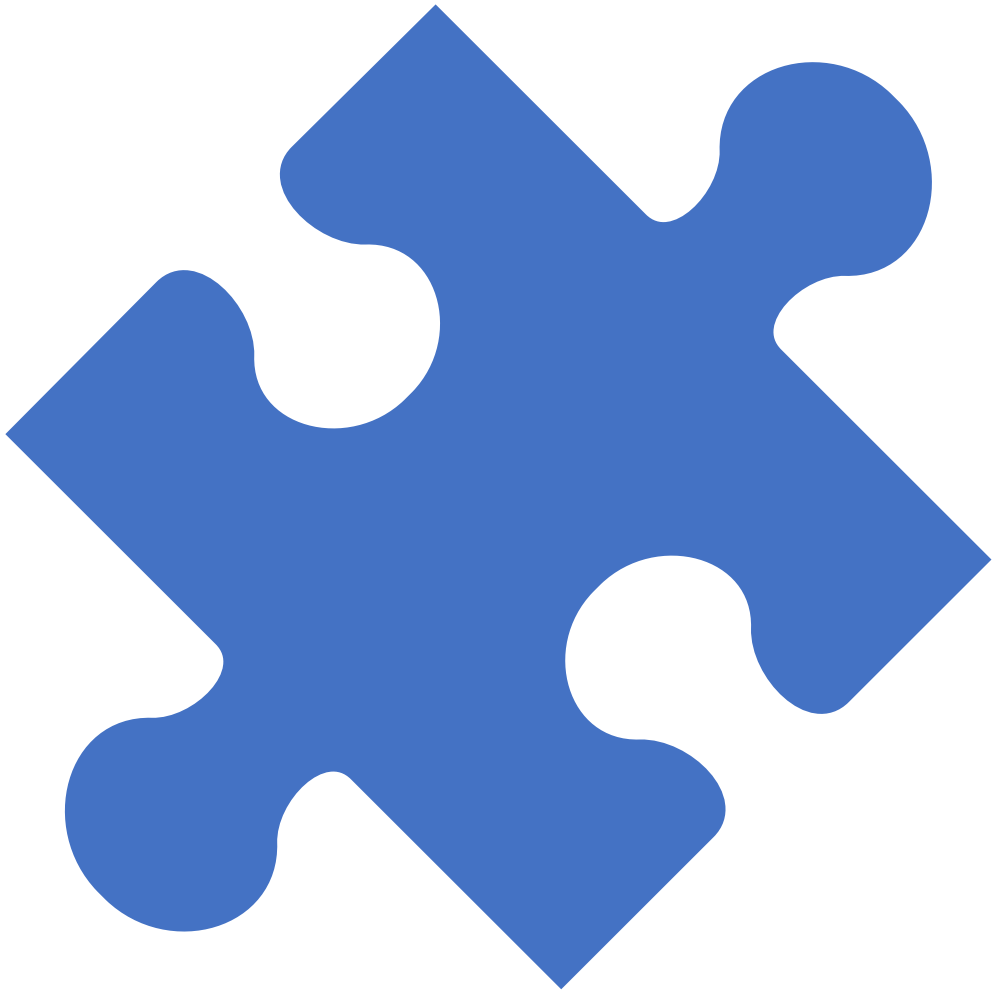


Nonce added extra power and flexibity to the security of the network


Block: #3
Nonce:
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 3A14DF2E57FB432A
Hash: 82B5C4A56AD315F7


Block: #3
Nonce:
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 3A14DF2E57FB432A
Hash: 82B5C4A56AD315F7
Block: #3
Nonce: 19
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 3A14DF2E57FB432A
Hash: EC2BF700552D6444
Block: #3
Nonce: 20
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 3A14DF2E57FB432A
Hash: 40A101F39CE9A1EA
Block: #3
Nonce: 21
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 3A14DF2E57FB432A
Hash: 6F7B874EA69A293D
Block: #3
Nonce: 22
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 3A14DF2E57FB432A
Hash: 5665D07FFAAECE46
Block: #3
Nonce: 23
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 3A14DF2E57FB432A
Hash: E799CF949FA981EA

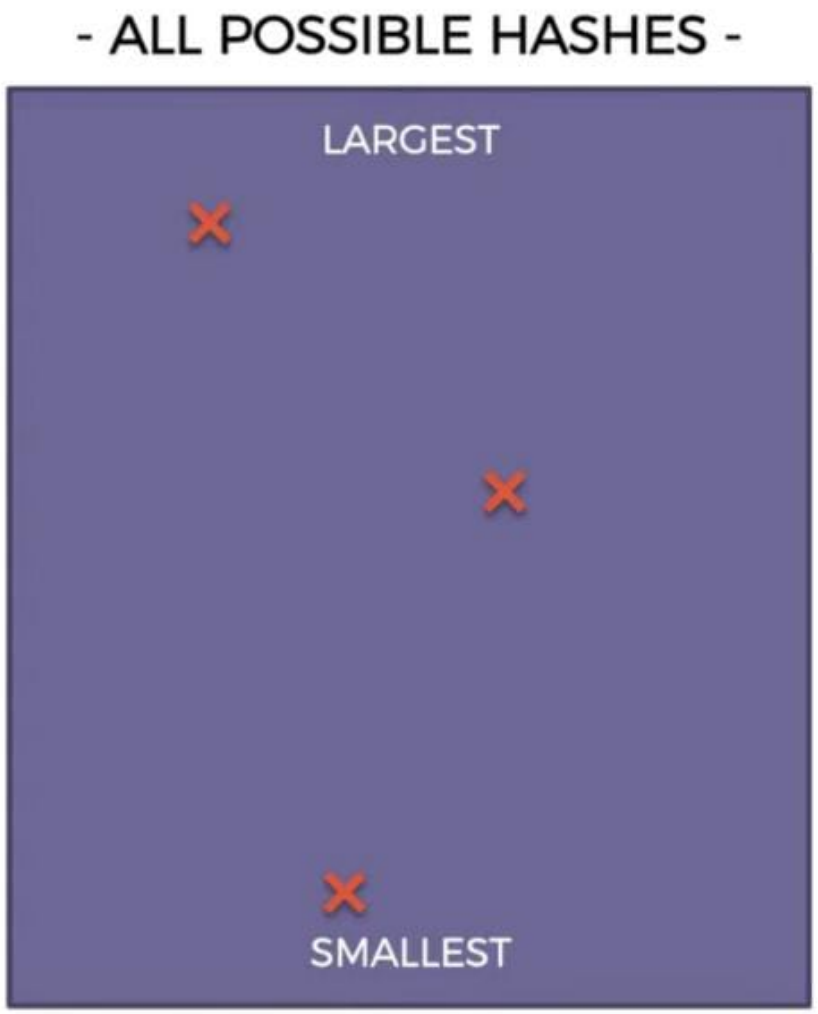
How mining works? (The cryptographic puzzle)



18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

00000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

0000000000000000000000000000000000000159CAA4B1EDA0FED66CB5E915C8F

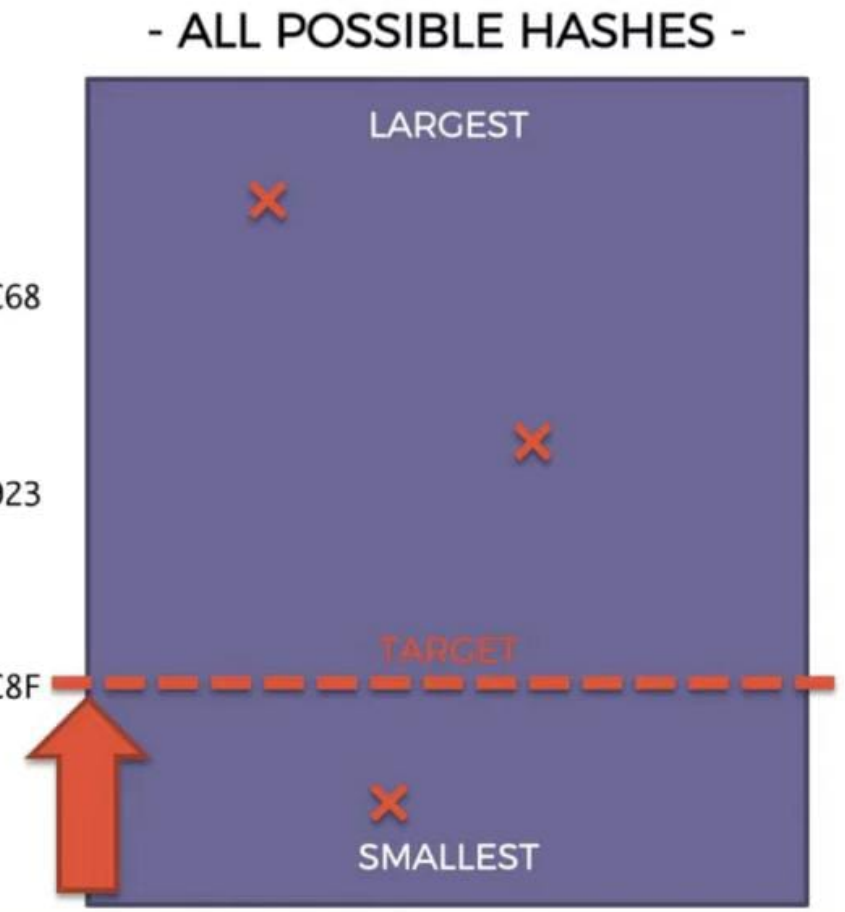


Network arbitrary selects the target for the miners

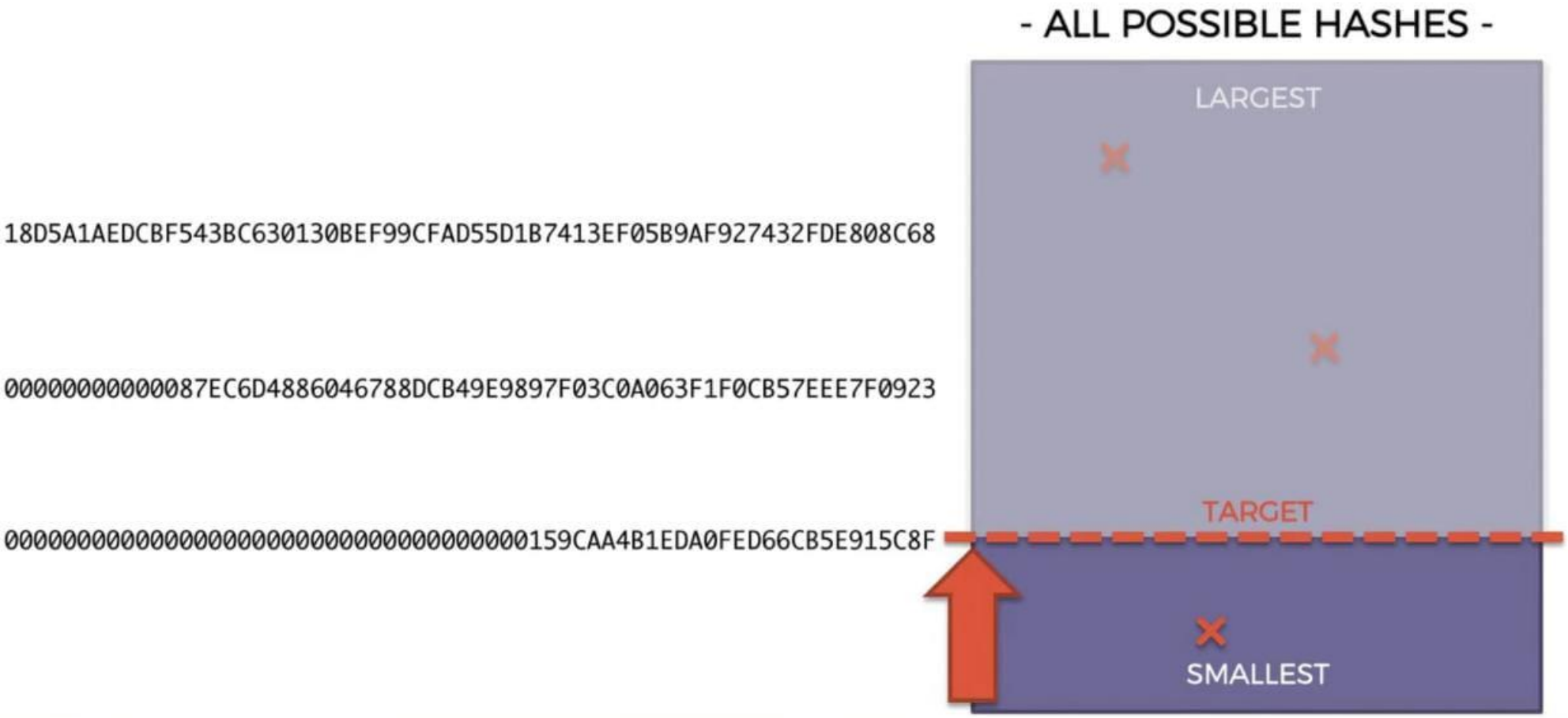
18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

00000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

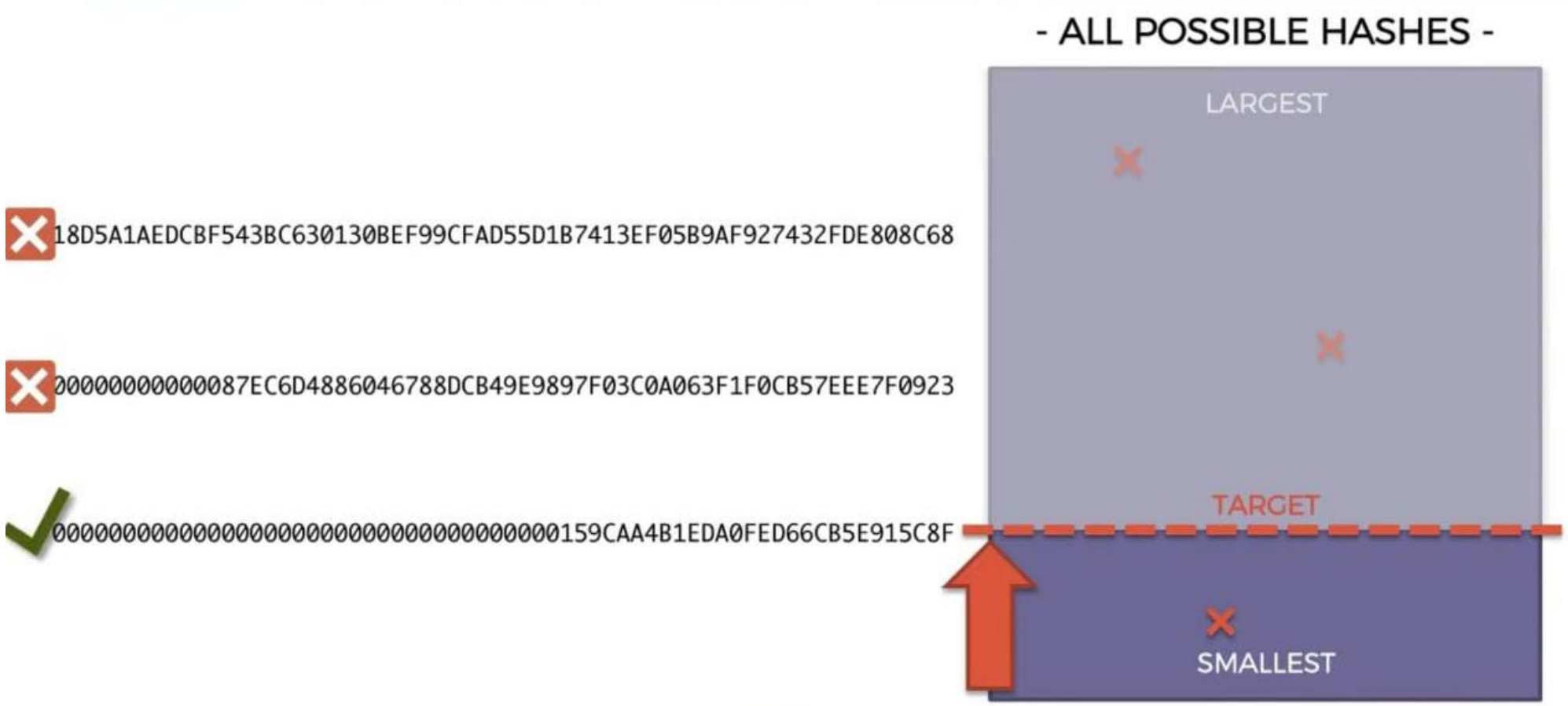
0000000000000000000000000000000000000159CAA4B1EDA0FED66CB5E915C8F

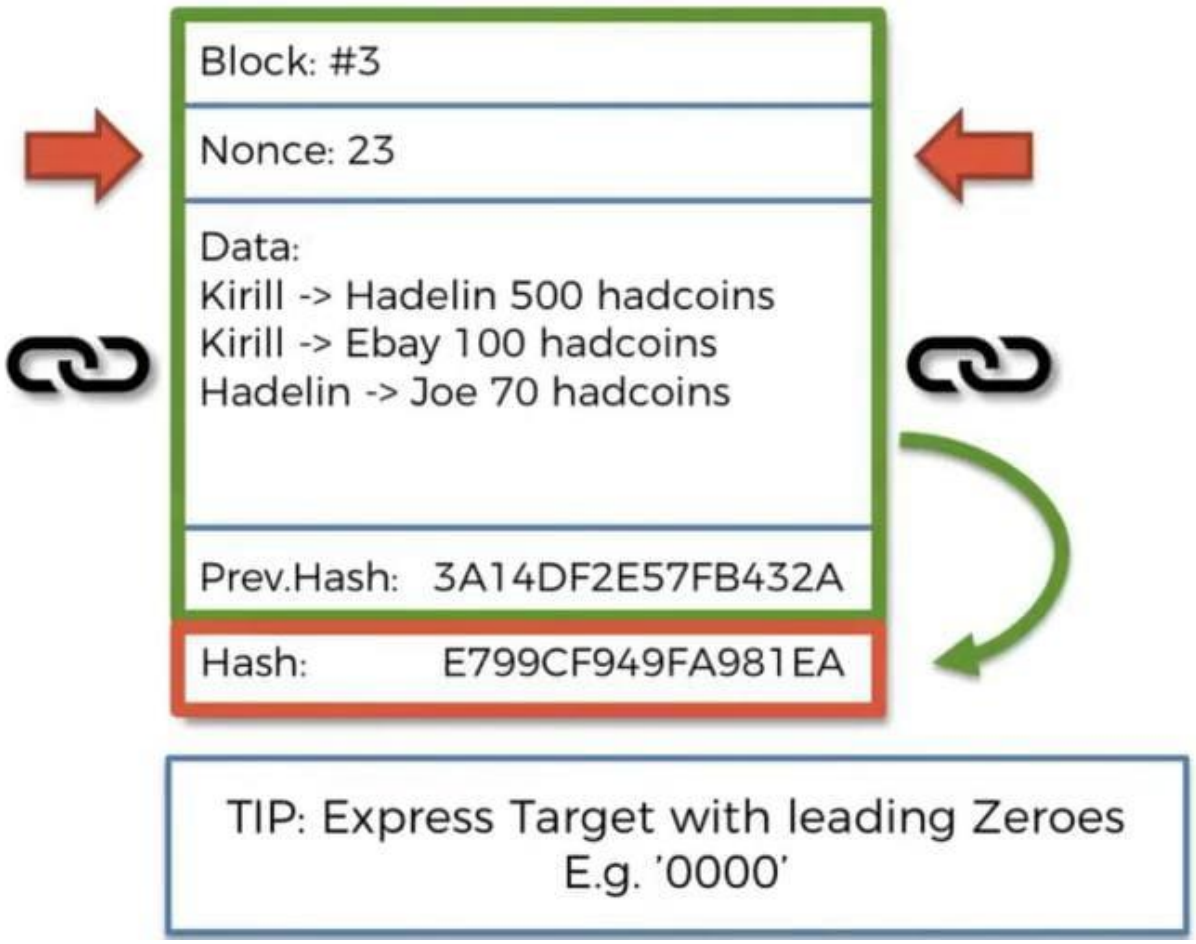


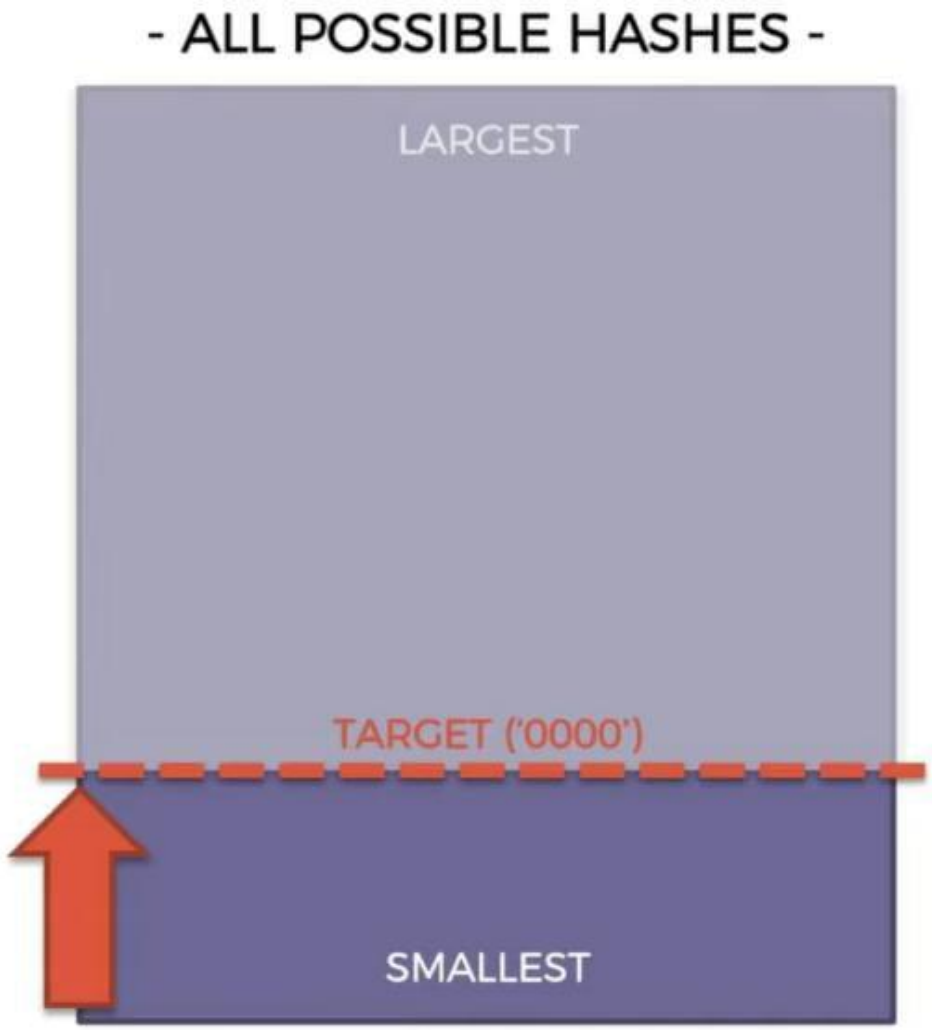
Any hash above the target doesn't count



The only reason for it is to create a hurdle for the miners

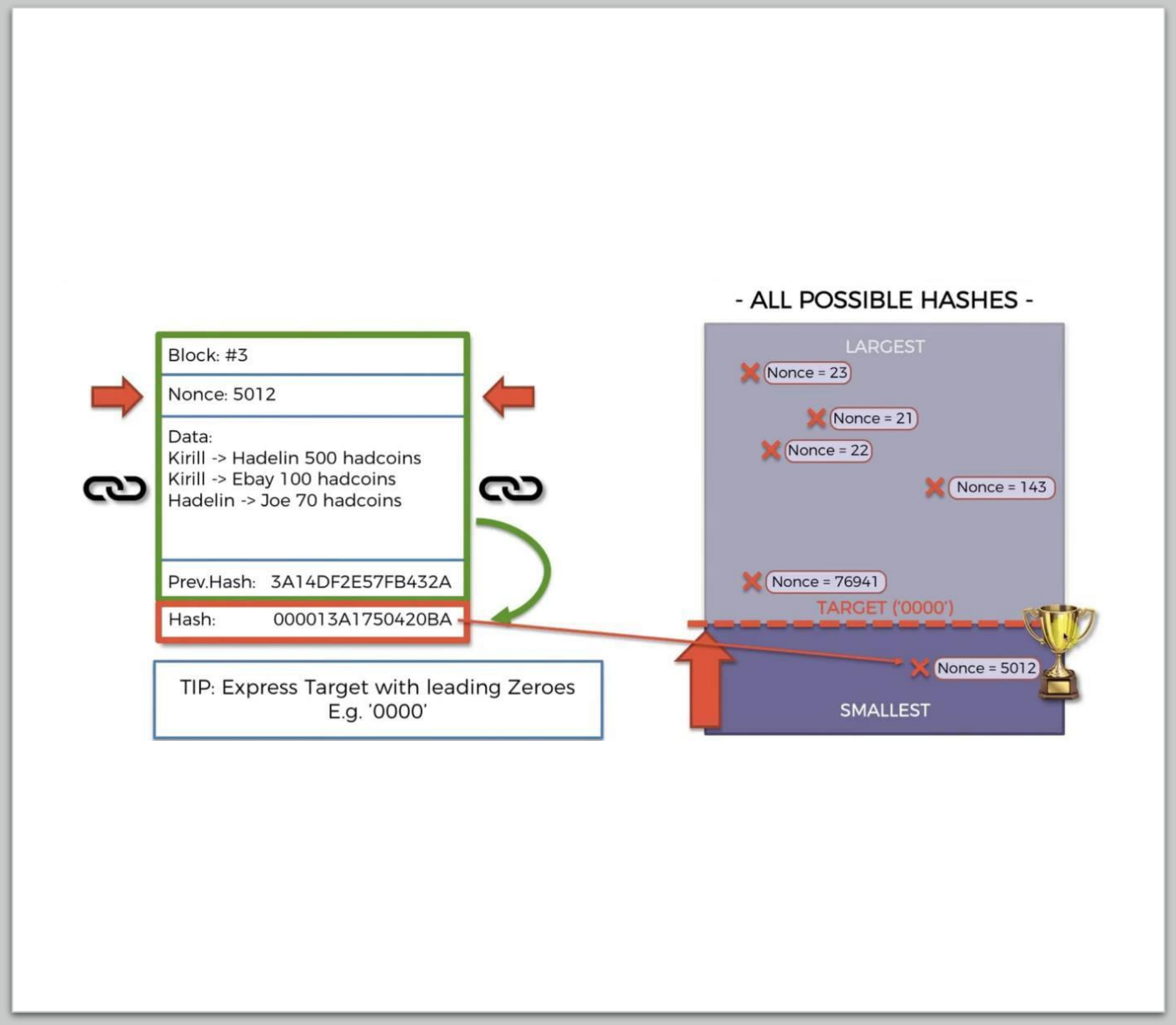


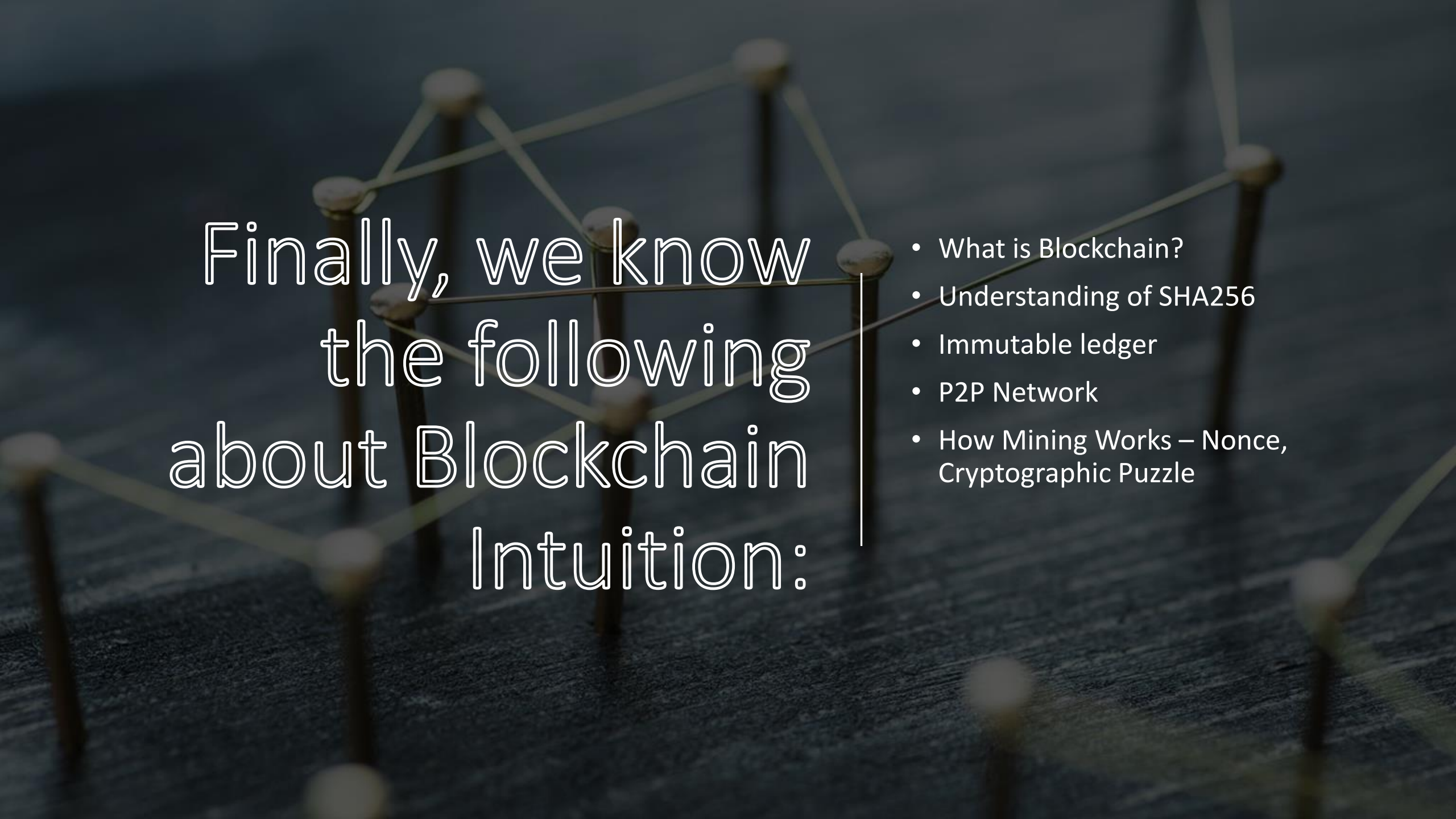

Block: #3
Nonce: 23
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 3A14DF2E57FB432A
Hash: E799CF949FA981EA
TIP: Express Target with leading Zeroes
E.g. '0000'


- ALL POSSIBLE HASHES -
LARGEST
TARGET ('0000')
SMALLEST

Found Golden Nonce:

- If you find a hash below the target, you will be allowed to create a block
- Miners just guess the nonce to generate a hash which is below the target
- Nonce = 5012 (Golden Nonce) was able to generate a hash that is below the target and hence gets to create a block in the blockchain





Finally, we know the following about Blockchain Intuition:

- What is Blockchain?
- Understanding of SHA256
- Immutable ledger
- P2P Network
- How Mining Works – Nonce, Cryptographic Puzzle

Acknowledgement and Source:

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