Notes Content

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

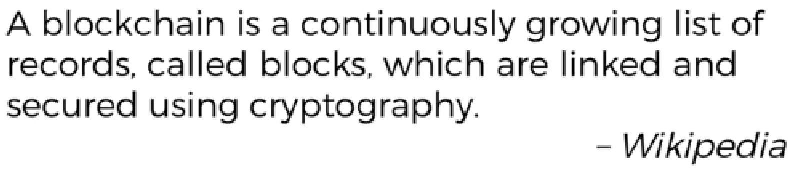
Video 2

Africa Tour and rating

Video 3

What is Blockchain?

- The concept came from Stuart Haber and W scott Stornetta in 1991.
- Paper: How to timestamp a digital document
- The concepts of blockchain came from that paper

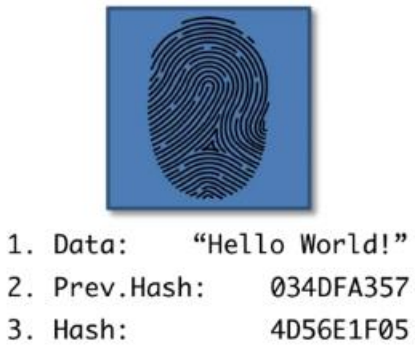


A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography.

– *Wikipedia*

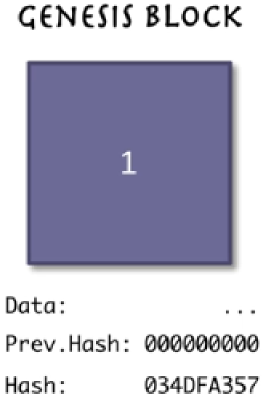
-

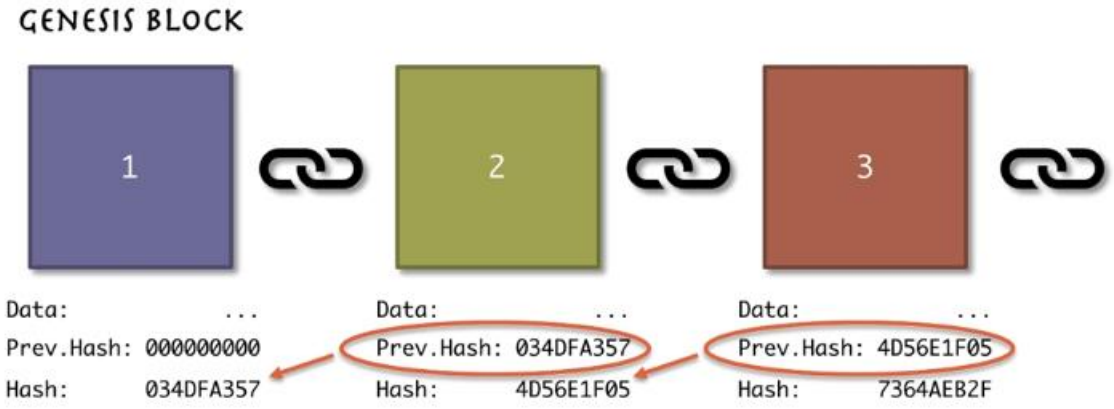
- A Block



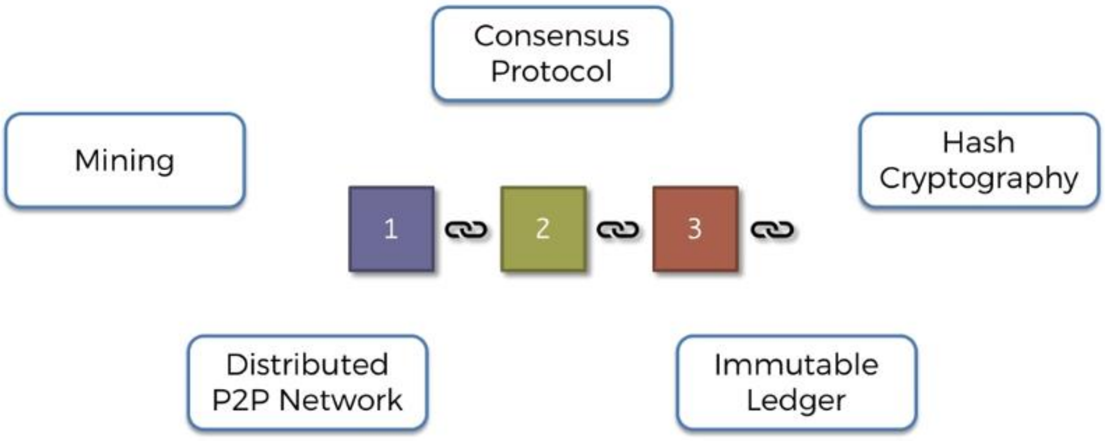
```
1. Data:      "Hello World!"
2. Prev.Hash:    034DFA357
3. Hash:         4D56E1F05
```

- Genesis block: The first block of the blockchain. The first block never going to change





- “Blocks are cryptographically linked together”
- The topics we’re going to cover in the module



Consensus Protocol

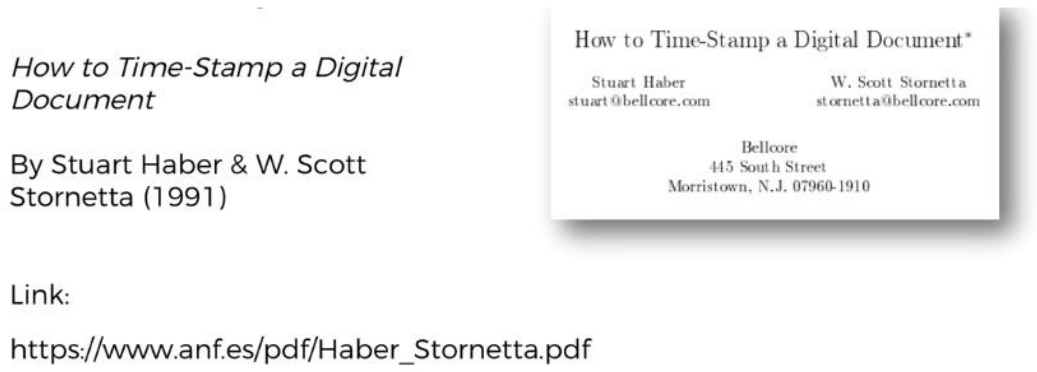
Mining

Hash Cryptography

Distributed P2P Network

Immutable Ledger

Additional Reading



How to Time-Stamp a Digital Document

By Stuart Haber & W. Scott Stornetta (1991)

How to Time-Stamp a Digital Document*

Stuart Haber
stuart@bellcore.com

W. Scott Stornetta
stornetta@bellcore.com

Bellcore
445 South Street
Morristown, N.J. 07960-1910

Link:

https://www.anf.es/pdf/Haber_Stornetta.pdf

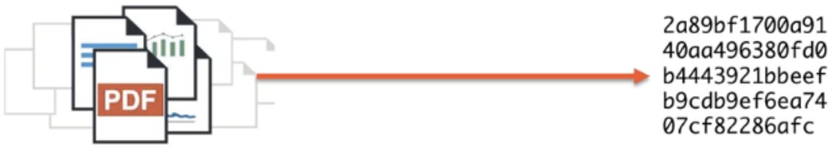
Video 4:

Hash Cryptography

Every person has a unique fingerprint. There is a small change of two people having same fingerprint that is very unlikely to be 1 in 60 million.

A fingerprint is a unique identifier of a person. Ex. Used by forensics department

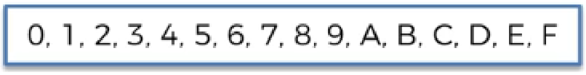
Same principal can be applied to digital documents. Using SHA256 Hashing algorithm



Developed by NSA

SHA stands for Secure Hash Algorithm and 256 is the number of bits it takes up in memory

Hash is 64 character long. It is represented in hexadecimal. Each character in the hash takes up 4 bits



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

How 16 characters can be represented using 4 bits?

- 4 bits for each character in the hash

0 = 0000

1 = 0001

2 = 0010

3 = 0011

4 = 0100

5 = 0101

6 = 0110

7 = 0111

8 = 1000

9 = 1001

10 = 1010

11 = 1011

12 = 1100

13 = 1101

14 = 1110

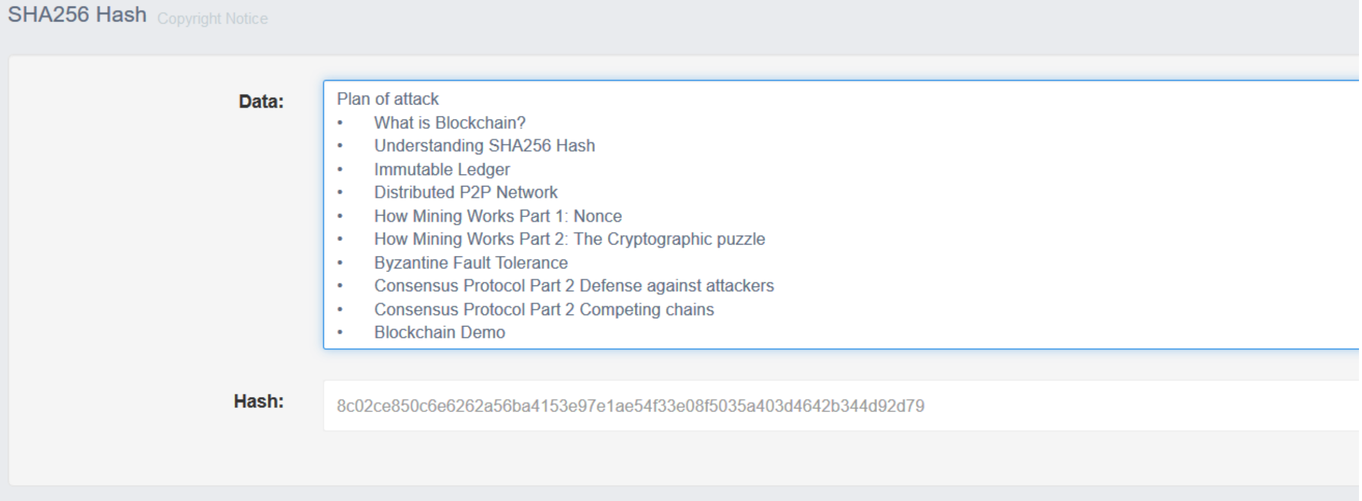
15 = 1111

- $2^4 = 16$

SHA256 not only work for text document. It works for any digital document. Like images, videos, text, audio, executable file

Demo of SHA256 hashing

https://tools.superdatascience.com/blockchain/hash



SHA256 Hash

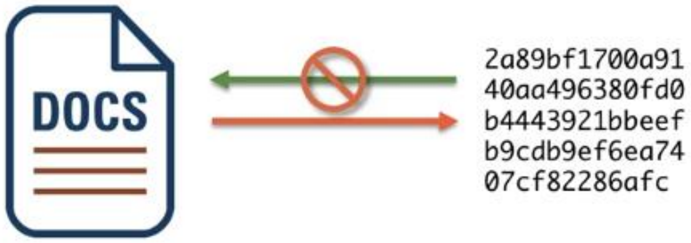
Data:

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

Hash: 8c02ce850c6e6262a56ba4153e97e1ae54f33e08f5035a403d4642b344d92d79

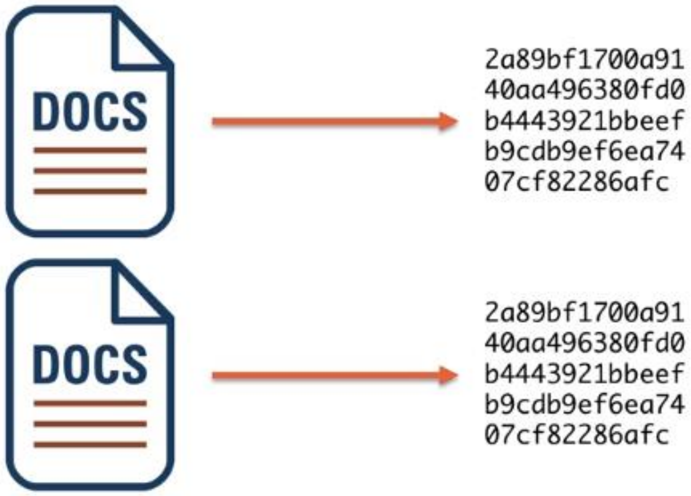
There are other algorithms other that SHA256. So the 5 requirements for a Hash Algorithm is

1. One- way



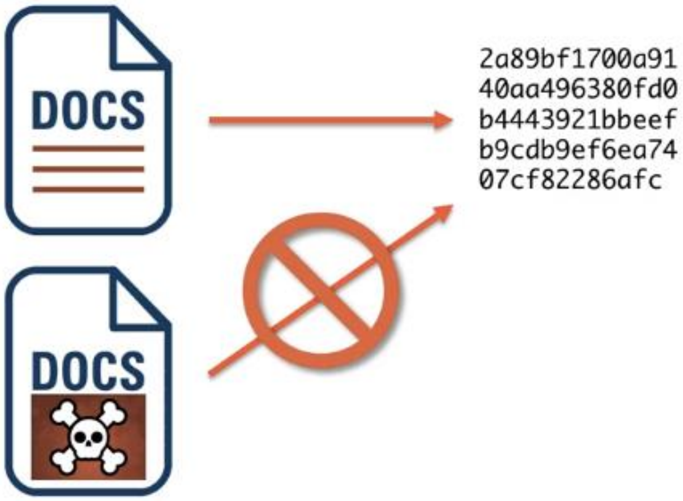
If you get the hash you cannot decode back to document. Just like fingerprint, from a fingerprint you cannot determine how the person looks like but if person is available then fingerprint can be retrieved or matched

2. Deterministic

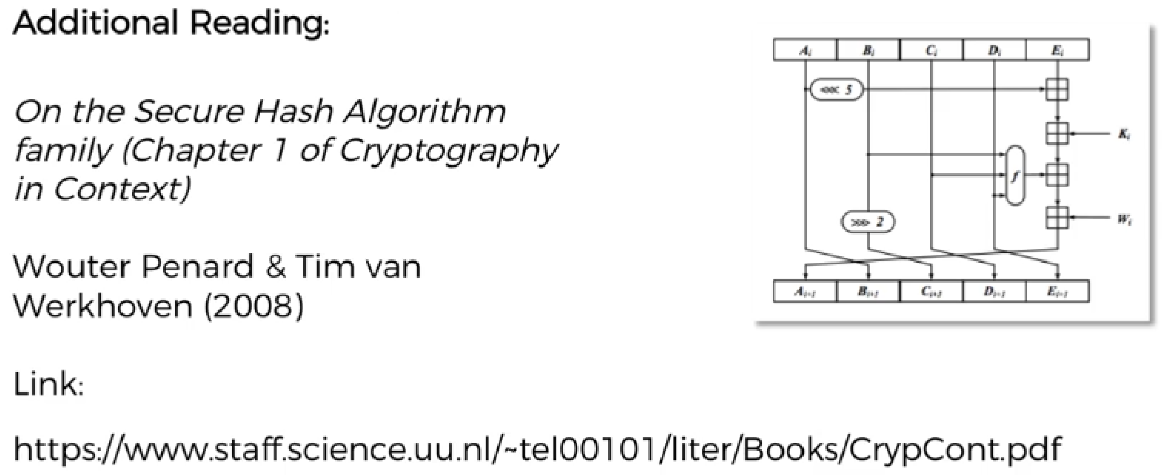


One hash generated for a document is unique and if the same document is put again same hash should be generated.

- Fast Computation
- The Avalanche Effect
  If the document is tampered or changed just even by one bit, the hash will change completely.
  See demo on https://tools.superdatascience.com/blockchain/hash
- Must withstand collisions.



Additional Reading



Additional Reading:

On the Secure Hash Algorithm family (Chapter 1 of Cryptography in Context)

Wouter Penard & Tim van Werkhoven (2008)

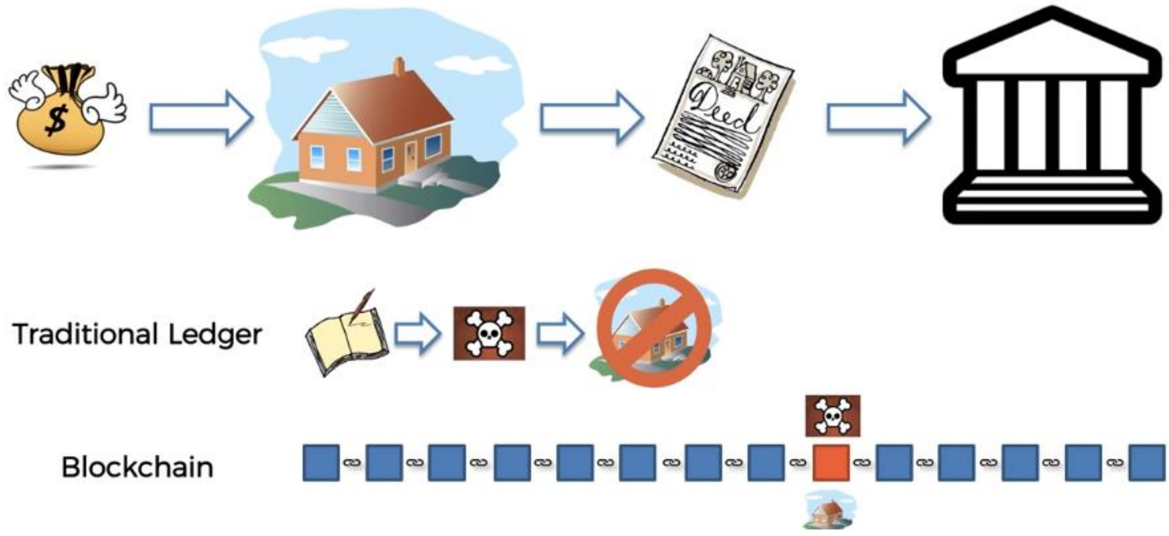
Link:

https://www.staff.science.uu.nl/~tel00101/liter/Books/CrypCont.pdf

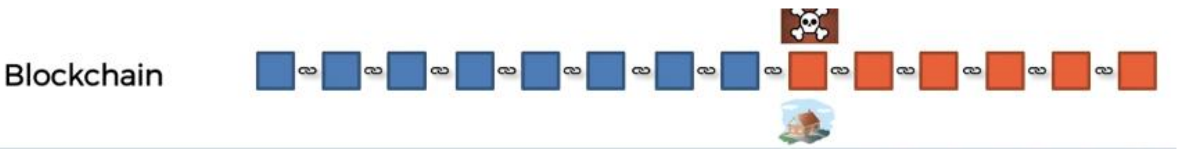
A_i
B_i
C_i
D_i
E_i
<<< 5
K_i
f
>>> 2
W_i
A_{i+1}
B_{i+1}
C_{i+1}
D_{i+1}
E_{i+1}

Video 5:

Immutable Ledger



All the block following the tampered block will become invalid, and it is very difficult to change all the blocks of the chain.



Video 6

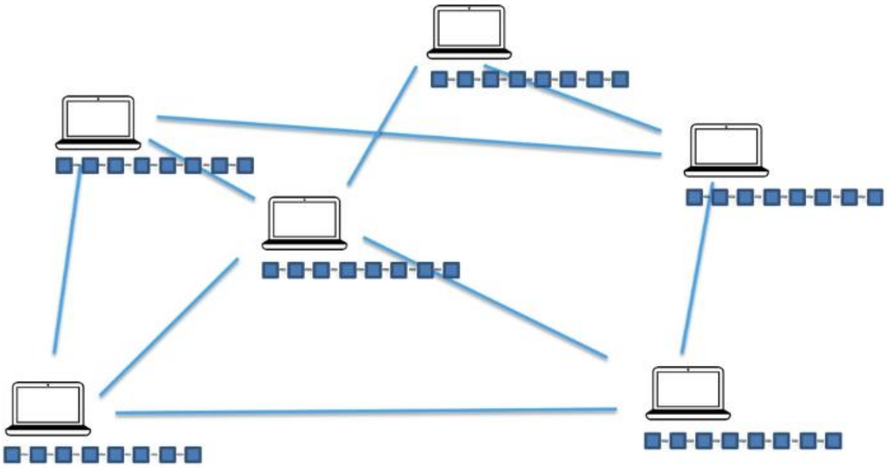
Distributed P2P Network

We solve 2 problems from distributed P2P network. That is,

1. What if someone get time to change all the invalid blocks of the blockchain, and change it successfully?
2. If the blocks of the chain are tampered how to recover the original information?

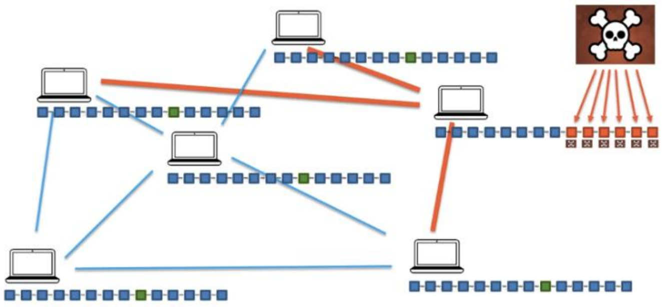
Both the questions are solved by distributed P2P network

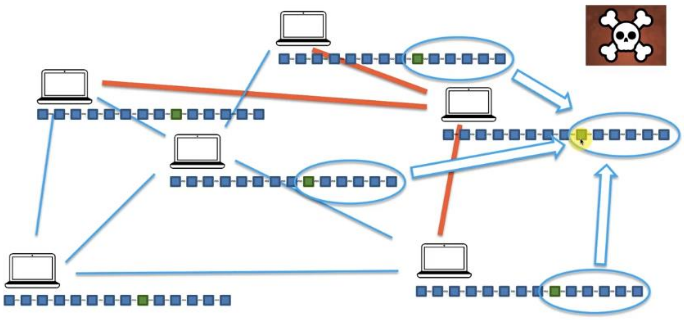
The blockchain is distributed across the network on different computers.



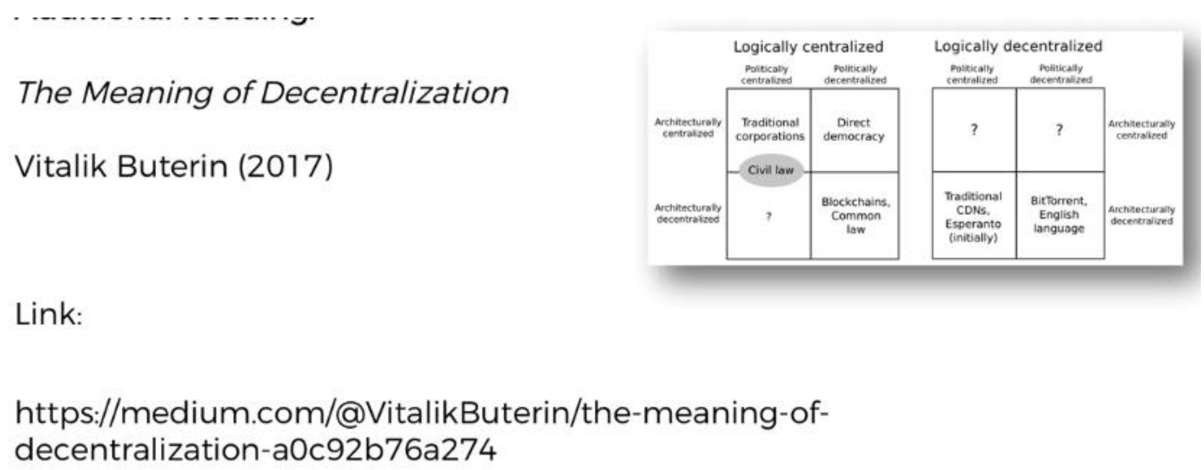
Blockchain is copied across all the network and updated regularly.

If the blocks on one blockchain is changed the computers connected to it will update the blockchain notifying the blockchain is not valid.





Additional Reading



The Meaning of Decentralization

Vitalik Buterin (2017)

Link:

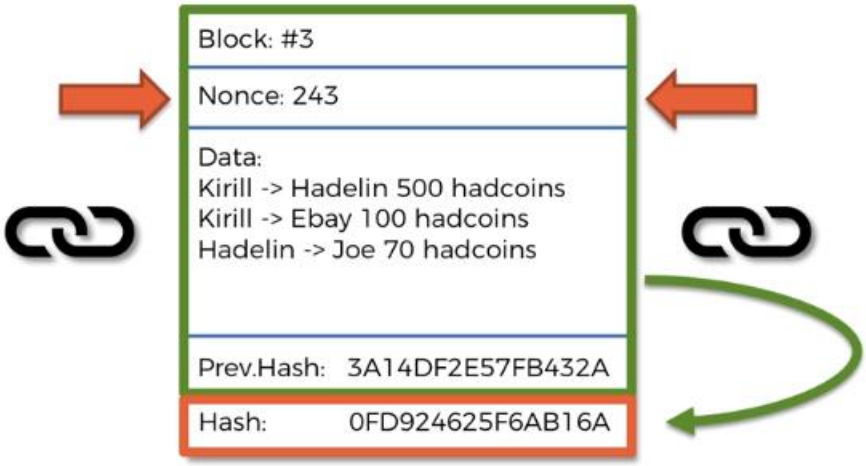
https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

	Logically centralized		Logically decentralized		
	Politically centralized	Politically decentralized	Politically centralized	Politically decentralized	
Architecturally centralized	Traditional corporations	Direct democracy	?	?	Architecturally centralized
	Civil law				
Architecturally decentralized	?	Blockchains, Common law	Traditional CDNs, Esperanto (initially)	BitTorrent, English language	Architecturally decentralized

Video 7

How Mining Works

The Original Block structure:



Block: #3

Nonce: 243

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

Prev.Hash: 3A14DF2E57FB432A

Hash: 0FD924625F6AB16A

Block number, Data and previous hash is fixed. There is an extra field added i.e. Nonce. So to calculate the hash of the current block, nonce is changed continuously that matches with the golden hash.

Video 8

Part 2 How Mining Works

A hash is a number represented in hexadecimal

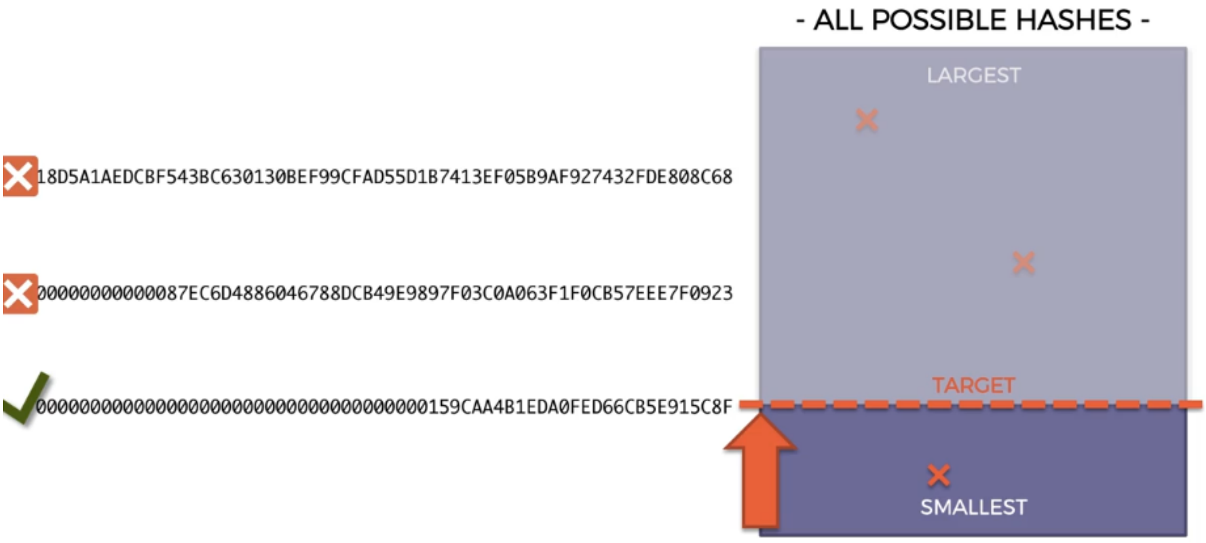
18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

0000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

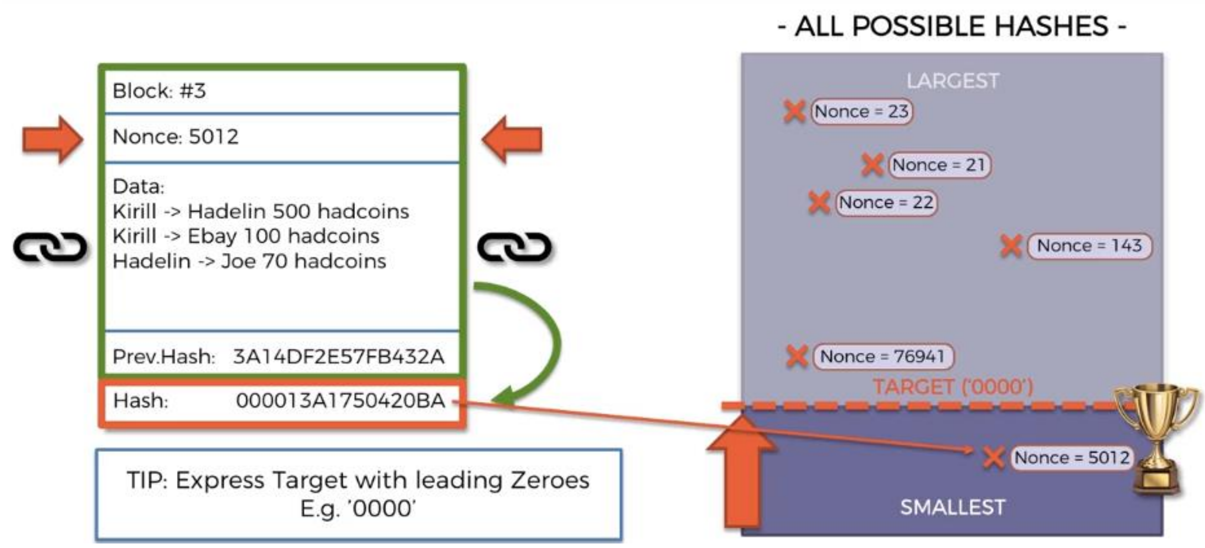
Mining:

The blockchain algorithm sets a target. There is a target set for miners to accomplish a certain hash.

Any Hash calculated by changing the nonce, if it is greater than the target hash doesn’t count. In order to be included in the blockchain the block should have a hash less than the target hash.


- ALL POSSIBLE HASHES -
LARGEST
18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68
00000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923
000000000000000000000000000000000000159CAA4B1EDA0FED66CB5E915C8F
TARGET
SMALLEST

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



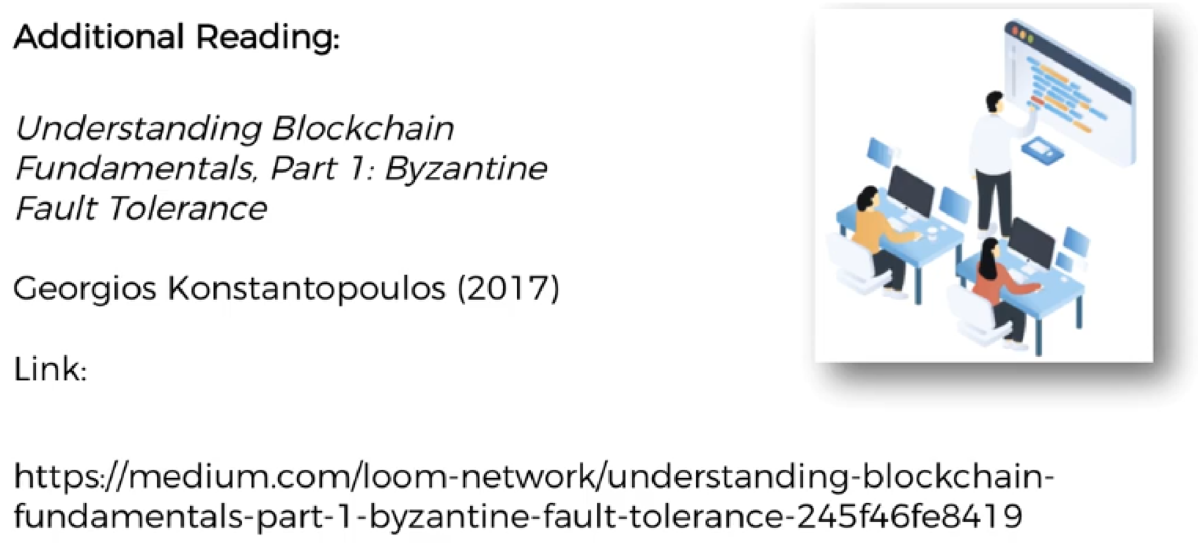
Video 9

Byzantine Fault Tolerance

https://drive.google.com/open?id=1CHKrUinTyveXo9E7PRgBM5_DCZF8d7OH

https://www.youtube.com/watch?v=VWG9xcwjxUg

Additional reading



Additional Reading:

Understanding Blockchain Fundamentals, Part 1: Byzantine Fault Tolerance

Georgios Konstantopoulos (2017)

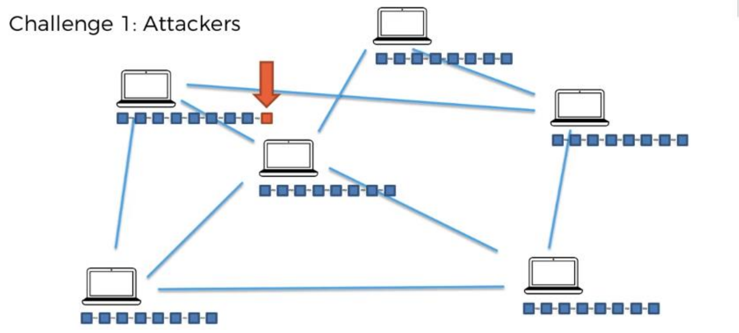
Link:

https://medium.com/loom-network/understanding-blockchain-fundamentals-part-1-byzantine-fault-tolerance-245f46fe8419

Video 10

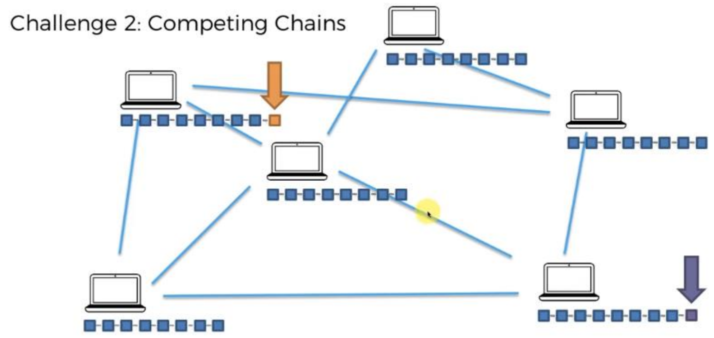
Consensus Protocol

Challenge 1: Attackers



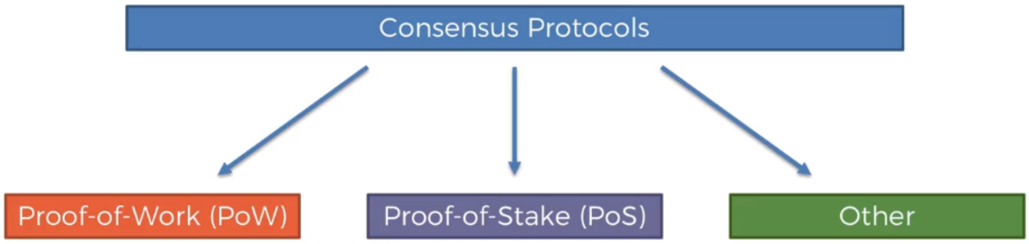
Challenge 1: Attackers

Challenge 2: Competing Chains (Lag between nodes, and can successfully mine different block at the same time)



Challenge 2: Competing Chains

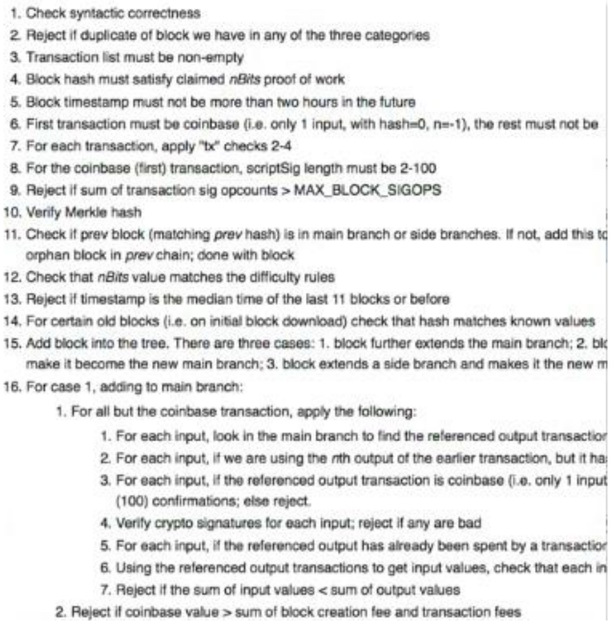
Other Types of Consensus Protocol



Proof of work is used in Blockchain network

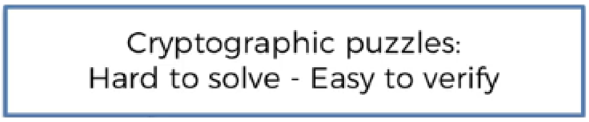
Challenge 1:

When miner mines a new block and gets the reward. If the miner tries to add a malicious block in the chain, he'll not get the reward. There are a series of checks/rules that the block has to pass to proof that it is correct.



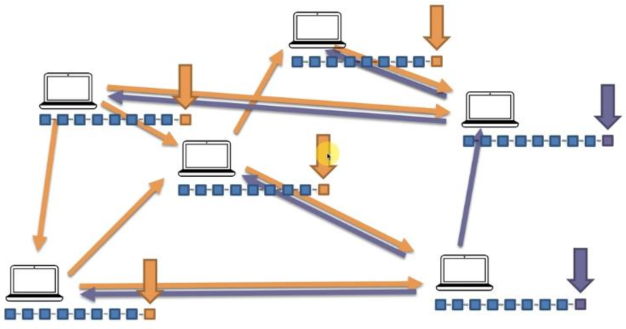
1. Check syntactic correctness
2. Reject if duplicate of block we have in any of the three categories
3. Transaction list must be non-empty
4. Block hash must satisfy claimed *nBits* proof of work
5. Block timestamp must not be more than two hours in the future
6. First transaction must be coinbase (i.e. 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 orphan block in *prev* chain; done with block
12. Check that *nBits* 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. blc make it become the new main branch; 3. block extends a side branch and makes it the new m
16. For case 1, adding to main branch:
    1. For all but the coinbase transaction, apply the following:
        1. For each input, look in the main branch to find the referenced output transactior
        2. For each input, if we are using the *n*th output of the earlier transaction, but it ha
        3. For each input, if the referenced output transaction is coinbase (i.e. only 1 input (100) confirmations; else reject.
        4. Verify crypto signatures for each input; reject if any are bad
        5. For each input, if the referenced output has already been spent by a transactior
        6. Using the referenced output transactions to get input values, check that each in
        7. Reject if the sum of input values < sum of output values
    2. Reject if coinbase value > sum of block creation fee and transaction fees

Challenge 1 is solved because nobody is able to add malicious block in the blockchain



Cryptographic puzzles:
Hard to solve - Easy to verify

Challenge 2:

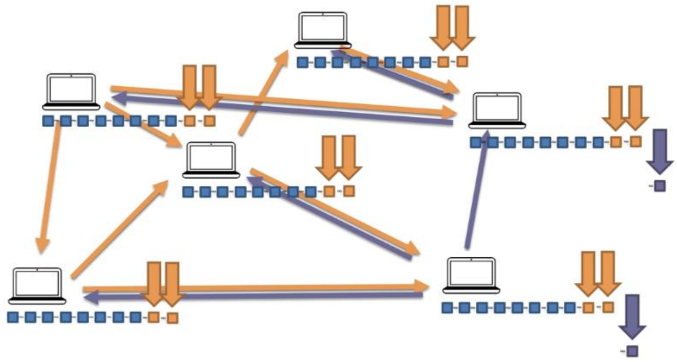


Above we have 4 nodes (orange) carrying a different blockchain than 2 nodes (purple)

Problem similar to Byzantine Fault Tolerance.

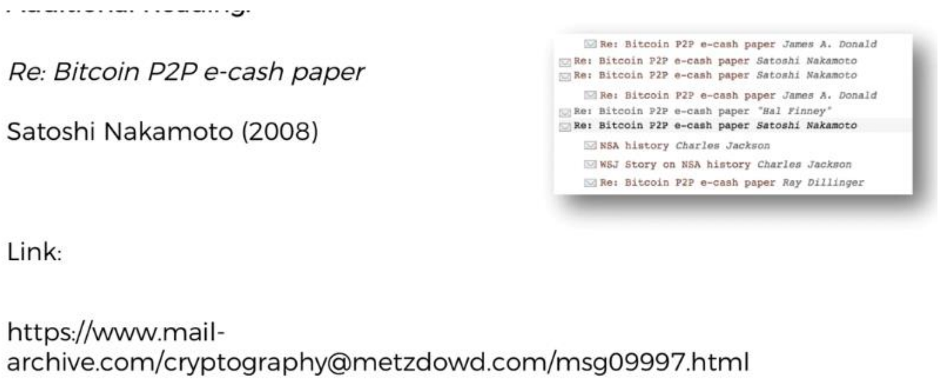
The problem is solved by the rule that whichever blockchain is the longest will be the king. In the above system where due to some lag in the network, if a block is added to the blockchain at the same time at two different nodes, the blockchain system is going to wait and let both the blockchain stay until the next block is added. Now whoever among the two different blockchains nodes mine a new block first, that blockchain is valid and get copied around all the nodes.

It means that the part of the network that has the highest hashing power will generate the longest chain.



The purple block are orphaned blocks do not get the reward

Additional Reading



Re: Bitcoin P2P e-cash paper

Satoshi Nakamoto (2008)

Re: Bitcoin P2P e-cash paper *James A. Donald*
Re: Bitcoin P2P e-cash paper *Satoshi Nakamoto*
Re: Bitcoin P2P e-cash paper *Satoshi Nakamoto*
Re: Bitcoin P2P e-cash paper *James A. Donald*
Re: Bitcoin P2P e-cash paper *"Hal Finney"*
Re: Bitcoin P2P e-cash paper *Satoshi Nakamoto*
NSA history *Charles Jackson*
WSJ Story on NSA history *Charles Jackson*
Re: Bitcoin P2P e-cash paper *Ray Dillinger*

Link:

https://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html

Additional Reading:

A (Short) Guide to Blockchain Consensus Protocols

Amy Castor (2017)

Link:

http://www.coindesk.com/short-guide-blockchain-consensus-protocols

https://tools.superdatascience.com/blockchain/blockchain