Overview of Bitcoin

Raza Sikander
C-DAC Hyderabad

Agenda

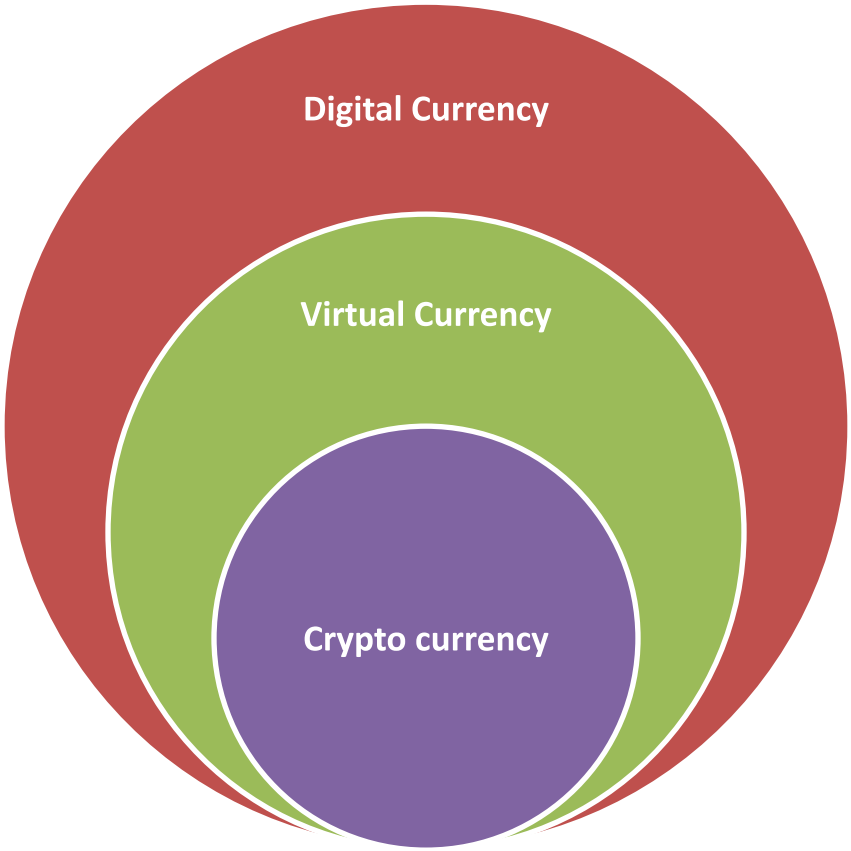
- Introduction to Cryptocurrency
- Bitcoin architecture
- Cryptocurrency Wallets
- Concept of Mining
- Proof of Work (PoW)
- Attacks on Bitcoin

Cryptocurrrency

- *A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralized networks based on blockchain technology*

  – *Investopedia*

Digital – Virtual – Crypto Currencies



- Digital currency – includes monetary assets also
  - Regulated: A country's central bank can issue a digital form of its fiat currency notes
  - Unregulated: Virtual currency
- Cryptocurrency
  - Type of Virtual currency
  - Uses cryptography to secure the transactions and for authentication

Differences between conventional and cryptocurrencies

	Fiat or conventional currency	Cryptocurrency
Type	Real	Virtual
Centralized	Yes (Central Bank)	No, distributed
Secure	Moderate (fake currency)	High - backed by cryptography
Acceptance	National level / country level	Global
Issued by	Government	Group of developers
Example	₹, $	Bitcoin/ BTC

Bitcoin: A Peer-to-Peer Electronic Cash System

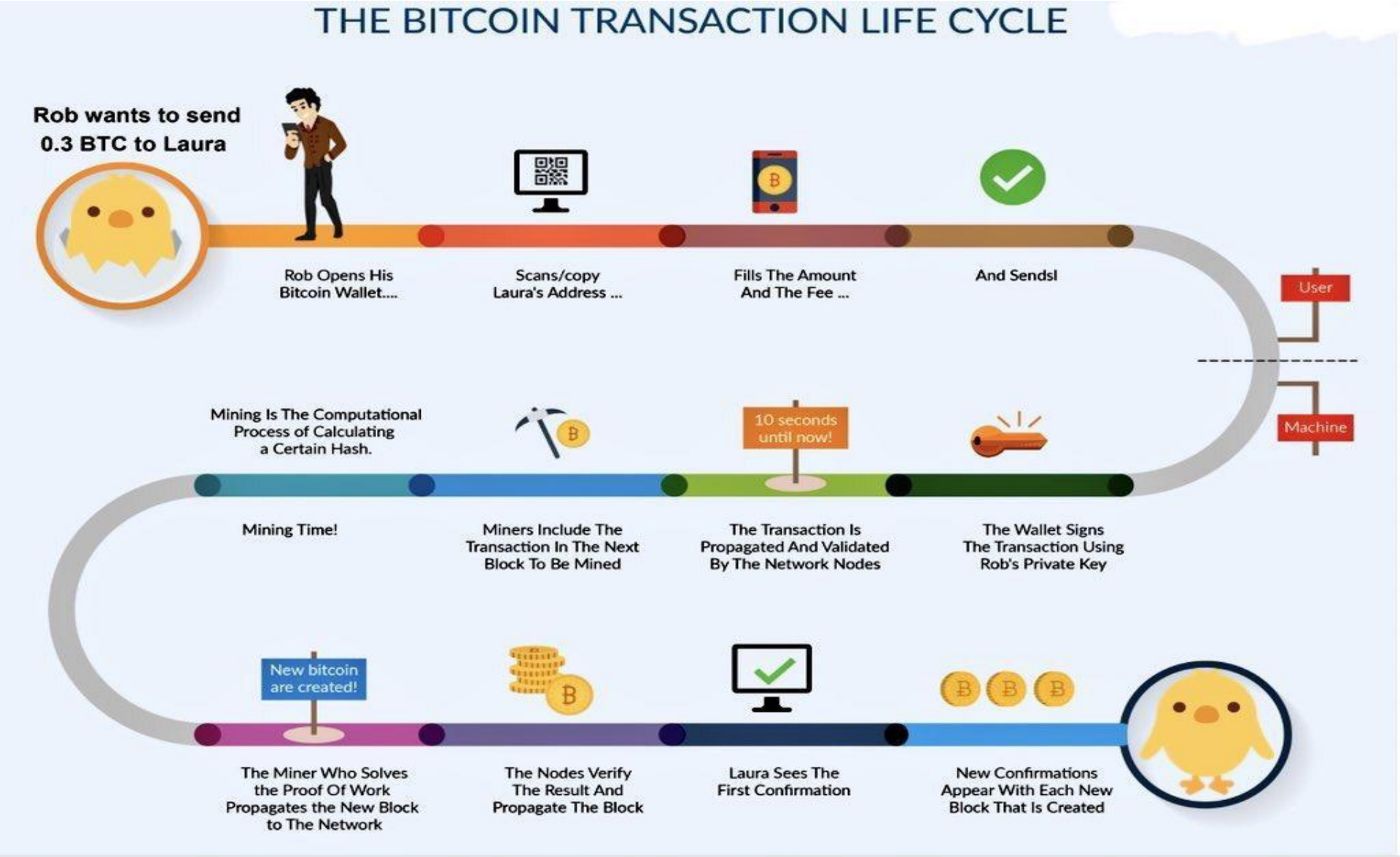
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

What is Bitcoin?

- Bitcoin is a completely decentralized, peer-to-peer, permissionless cryptocurrency put forth is 2009
  - No central party for ordering or recording anything
  - Software that runs on machines of all stakeholders to form the system
  - **No identity**; no need to signup anywhere to use; no access control - anyone can participate in any role

The Bitcoin Transaction Life Cycle



Source: https://twitter.com/btc/status/1009159861379260416

Bitcoin Transaction

- Sequence of steps that happen to transfer 0.3 BTC from Rob to Laura are:
  - Wallet
    - Initiate the transaction
  - Network
    - Validate the transaction
  - Mining
    - Build the block that is to be added to the ledger
  - Wallet
    - Receive the money

The Bitcoin Transaction Life Cycle - The Network

Step 1) The wallet constructs the transactions, sign using senders private key, broadcasts it to the network

Step 2) The network nodes validate the transactions based on the existing Blockchain, and propagate the transaction to the miners

Step 3) The **miners include the transaction** to the next block to be mined

The Bitcoin Transaction Life Cycle - The Miners

Step 1) The miners collect all the transactions for a time duration, say for 5 mins

Step 2) Miners construct a new block and tries to connect it with the existing blockchain, through a cryptographic hash computation - The mining Procedure

Step 3) Once the mining is over and the hash is obtained, the block is included in the existing blockchain - The updated blockchain is propagated in the network

The Bitcoin Transaction Life Cycle - The Receiver

Step 1) Sender opens his Bitcoin Wallet and refreshes, the Blockchain gets updated

Step 2)The transaction reflects at Senders wallet

Wallet

- A wallet is a software program that
  - stores the public and the private keys
  - Signs the transactions with the private key of the owner
  - Acts as a medium to send or receive cryptocurrency
  - Helps to check the balance

Bitcoin wallets

https://bitcoin.org/en/choose-your-wallet?step=1 80%

Mobile wallets

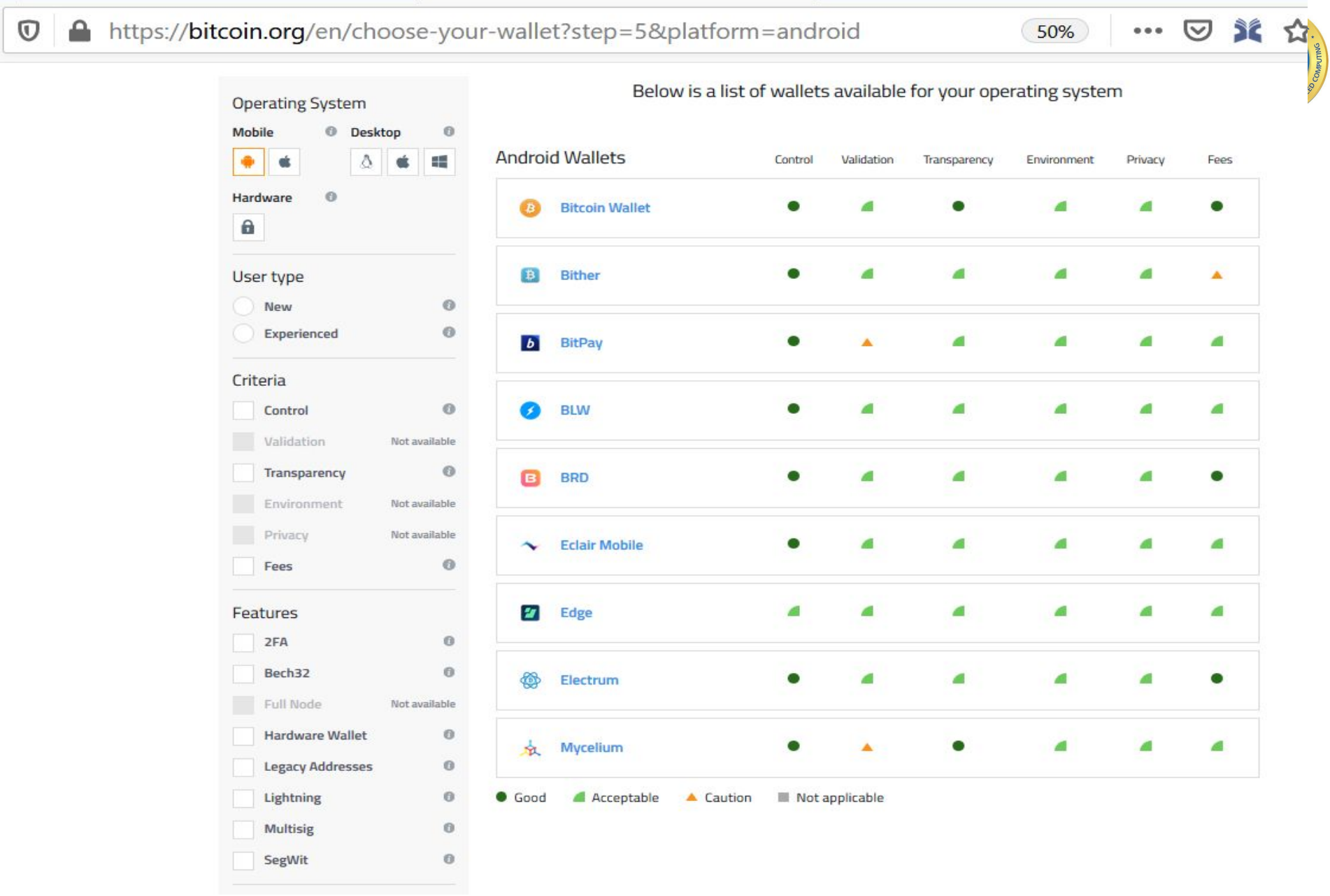
- Portable and convenient; ideal when making transactions face-to-face
- Designed to use QR codes to make quick and seamless transactions
- App marketplaces can delist/remove wallet making it difficult to receive future updates
- Damage or loss of device can potentially lead to loss of funds

Desktop wallets

- Environment enables users to have complete control over funds
- Some desktop wallets offer hardware wallet support, or can operate as full nodes
- Difficult to utilize QR codes when making transactions
- Susceptible to bitcoin-stealing malware/spyware/viruses

Hardware wallets

- One of the most secure methods to store funds
- Ideal for storing large amounts of bitcoin
- Difficult to use while mobile; not designed for scanning QR codes
- Loss of device without proper backup can make funds unrecoverable

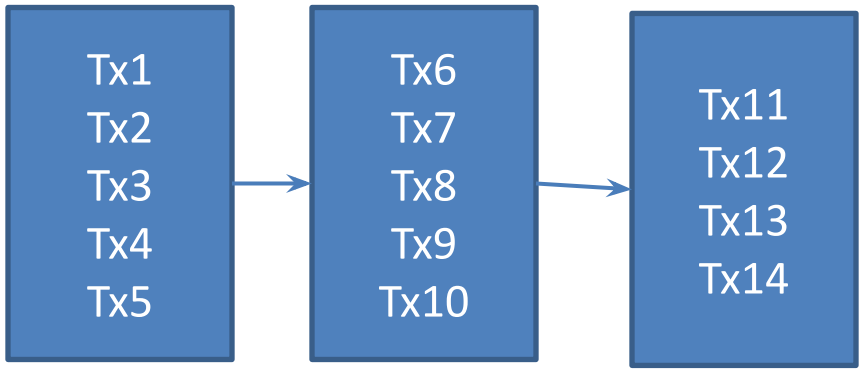


https://bitcoin.org/en/choose-your-wallet?step=5&platform=android

Consensus in a Bitcoin Network

- Every node does two things
  - Validates the transactions
  - Verifies the transactions in a block that is received from the Miner.
- Consensus procedure is
  - Validate the transactions – by the nodes
  - Apply consensus over the entire block of transactions – by the miners
  - Verify the transactions – by the nodes

Consensus in Bitcoin network



Whose block is to be added?

Possible solution: Broadcast and then apply a choice function

But how much time we will wait?
FLP – impossibility result !!

Tx15
Tx16
Tx18
Tx19

Miner - 1

Tx15
Tx16
Tx17

Miner - 2

Tx15
Tx16
Tx17
Tx18

Miner - 3

Miners doesn't know each other

Solution

- Each of the miner tries to solve a challenge independently
- Response: Who ever solves the challenge and proves first, their block is accepted
  - Solving the challenge is to be difficult and complex
- Solution is sent to other miners for verification
  - Verification should be easy
- If any of the txs are not included in the block, they are considered by the minors in the next block
- In parallel, Mining continues

Challenge-Response to Permission-less Consensus

- Bitcoin - PoW - Works on Challenge-Response
  - To achieve consensus, each node in a network must solve a complex, resource-intensive cryptographic problem called a proof of work to ensure all are in sync.

Solution – Proof of Work

- Challenge should be hard enough to be solved
- But, at the same time, it should be easy to verify
  - Hash is puzzle friendly
  - Y = H(A||X)
  - Given A and Y, find X
  - Finding X is a challenge, but when A and X are known, verification is easy

Solution: Proof of Work

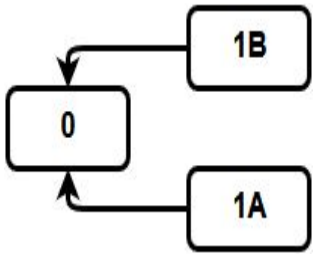
- Y = H(A||X)
- Block Hash = Hash(Previous Block Hash: Merkle Root: Nonce)
- challenge:
  - Block Hash: should have certain zeros (difficulty) at the beginning
  - For what value of Nonce, this can be achieved
- The miners need to give a proof that they have done some work, before proposing a new block

Mining Difficulty

- The difficulty changes for every 2016 blocks
  - Desired rate – one block each 10 minutes
  - Two weeks to generate 2016 blocks
  - The change in difficulty is in proportion to the amount of time over or under two weeks the previous 2016 blocks took to find (en.bitcoin.it)
  - current_difficulty = previous_difficulty * (2 weeks in milliseconds)/(milliseconds to mine last 2016 blocks)
  - The offset for difficulty D is 0xffff * 2208/D

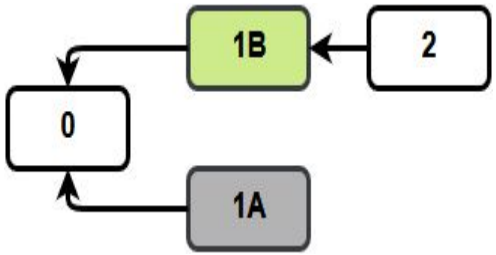
Which block to accept?

- Mining starts for block at height 1
- 2 miners mine the block at same time
- Half network mines on 1A and another half of 1B
- No transactions are final yet



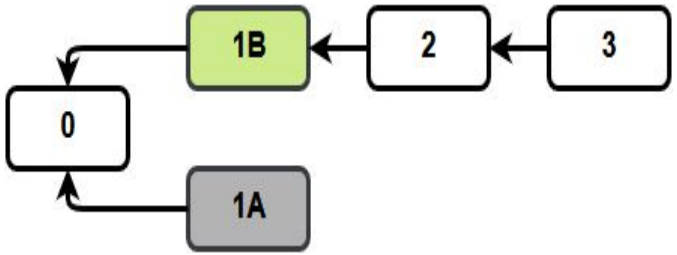
Which block to accept? contd.

- A miner mines block at height 2
- All miners work on finding block at height 3 and transactions in block 1A are now back not in a block



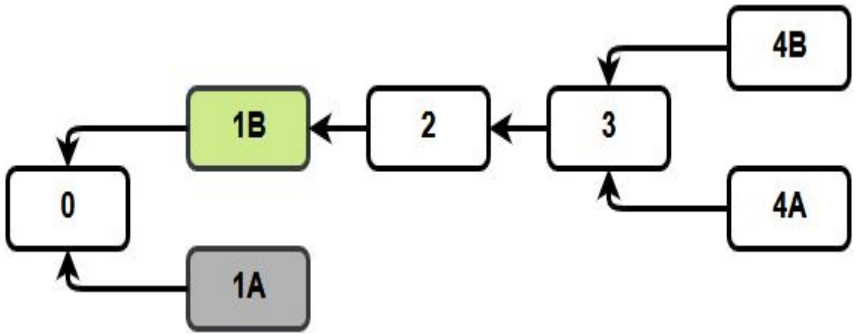
Which block to accept? contd.

- A miner mine block at height 3



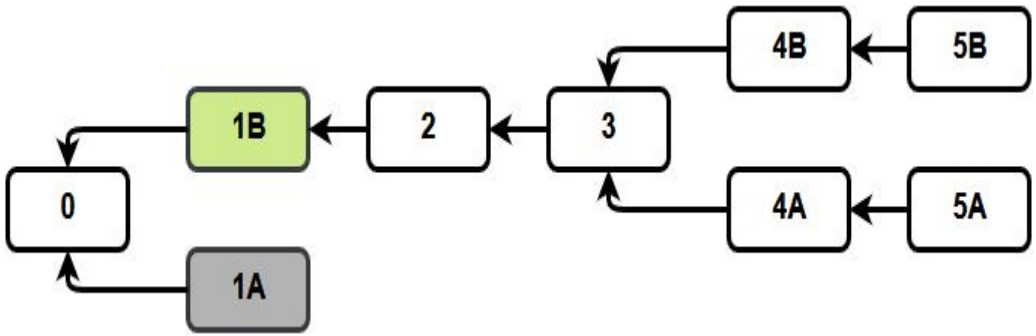
Which block to accept? contd.

- At height 4, 2 miners mine the block at same time



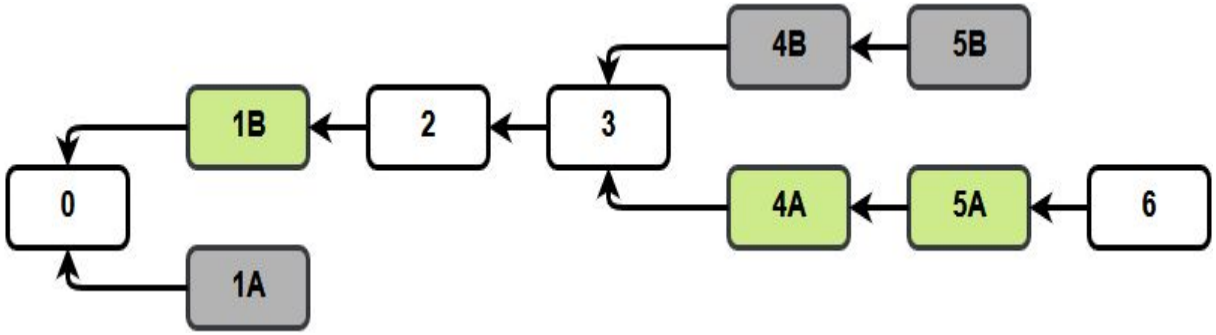
Which block to accept? contd.

- Again at height 5, 2 miners mine the block at same time



Which block to accept? contd.

- A miner working on height 6 mines a block
- All miners start mining for block at height 7 and all transactions in blocks 4B and 5B are back not in a block
- Thus the longest chain wins
- Eg. In bitcoin, the current default is wait for 6 confirmations for anything to have value



Double Spending Problem

- The attack: Successful use of the same fund twice
  - A transaction is generated with BTC10 to both Bob and Carol at the same time
- The solution:
  - The transactions are irreversible (computationally impractical to modify)
  - Every transaction can be validated against the existing blockchain

Breaking Bitcoin PoW

- Bitcoin PoW is computationally difficult to break, but not impossible
- Attackers can deploy high power servers to do more work than the total work of the blockchain
- A known case of successful double-spending – (November 2013) “it was discovered that the GHash.io mining pool appeared to be engaging in repeated payment fraud against BetCoin Dice, a gambling site” [Source: https://en.bitcoin.it/]

The Monopoly Problem

- PoW depends on the computing resources available to a miner
  - Miners having more resources have more probability to complete the work
- Monopoly can increase over time (Tragedy of the Commons)
  - Miners will get less reward over time
  - Users will get discouraged to join as the miner
  - Few miners with large computing resources may get control over the network

References

- Bitcoin
- Investopedia
- Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system Bitcoin: A Peer-to-Peer Electronic Cash System." *Bitcoin. org. Disponible en https://bitcoin. org/en/bitcoin-paper* (2009).
- Mastering Bitcoin, Oreilly Publications

THANK YOU