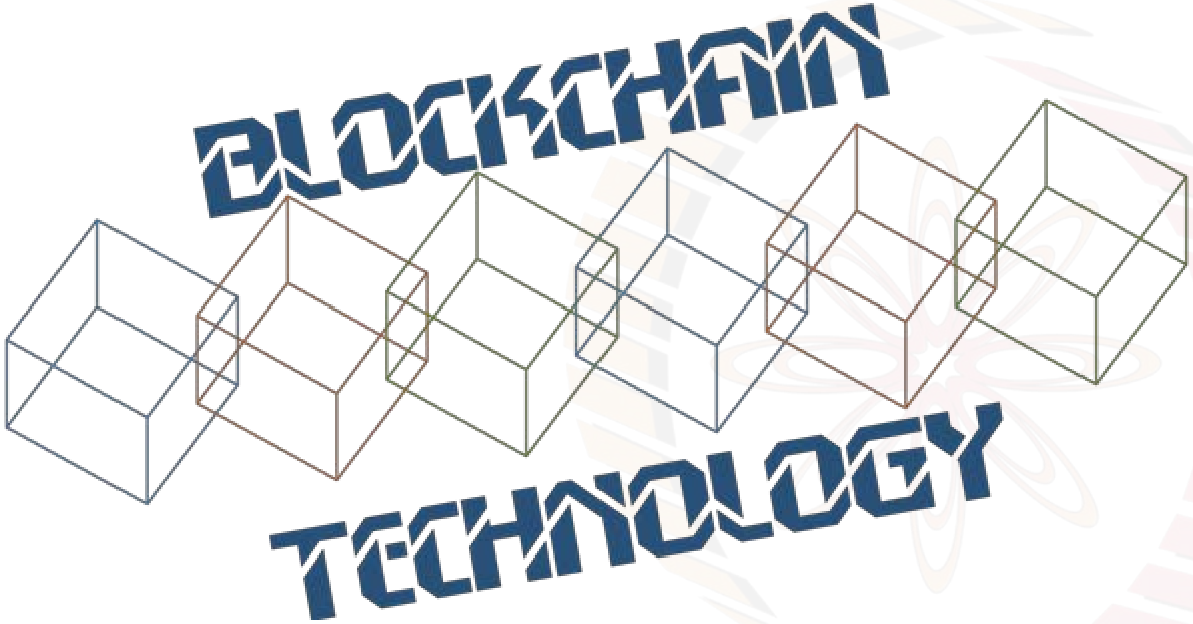
BLOCKCHAINS

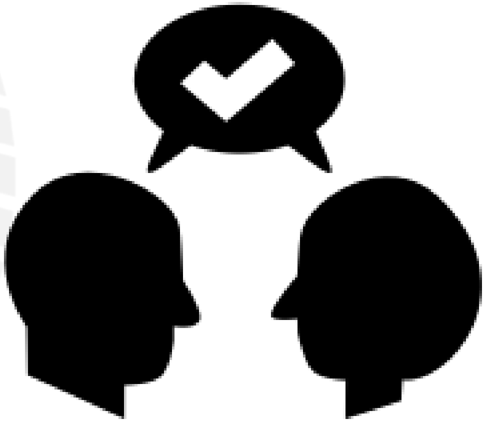
ARCHITECTURE, DESIGN AND USE CASES

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

PRAVEEN JAYACHANDRAN
IBM RESEARCH,
INDIA

Image courtesy: http://beetfusion.com/

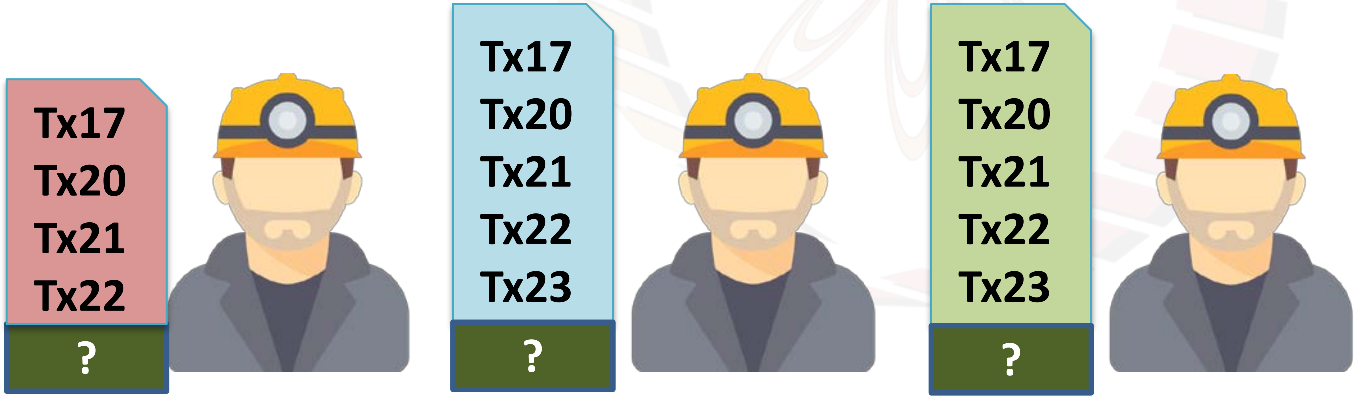




POW AND BEYOND

Bitcoin Proof of Work (PoW)

- Based on Hashcash PoW system
  - The miners need to give a proof that they have done some work, before proposing a new block
  - The attackers will be discouraged to propose a new block, or make a change in the existing blocks

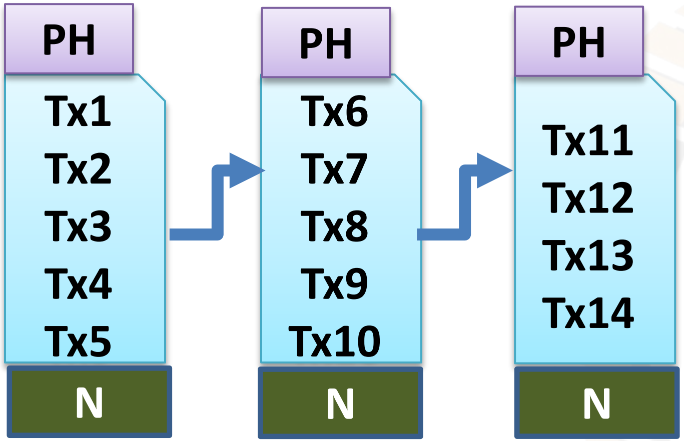


Tx17
Tx20
Tx21
Tx22
?

Tx17
Tx20
Tx21
Tx22
Tx23
?

Tx17
Tx20
Tx21
Tx22
Tx23
?

Bitcoin Proof of Work System

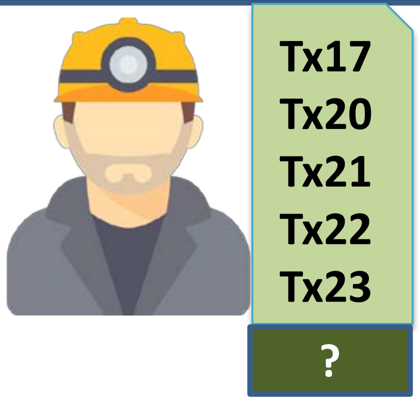


PH
Tx1
Tx2
Tx3
Tx4
Tx5
N

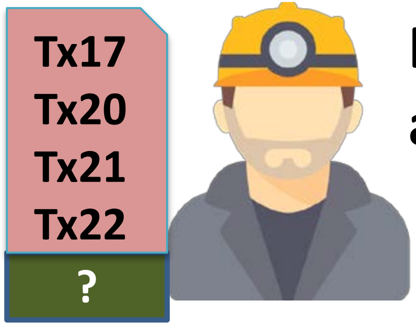
PH
Tx6
Tx7
Tx8
Tx9
Tx10
N

PH
Tx11
Tx12
Tx13
Tx14
N

BH: Block Hash
PH: Previous Block Hash
MR: Merkle Root
N: Nonce



Tx17
Tx20
Tx21
Tx22
Tx23
?

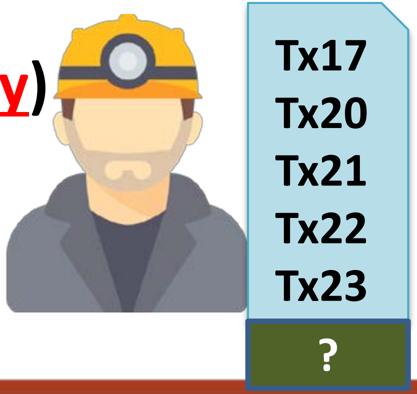


Tx17
Tx20
Tx21
Tx22
?

BH should have certain zeros (<u>difficulty</u>) at the beginning

BH = Hash(PH:MR:N)

N = ?



Tx17
Tx20
Tx21
Tx22
Tx23
?

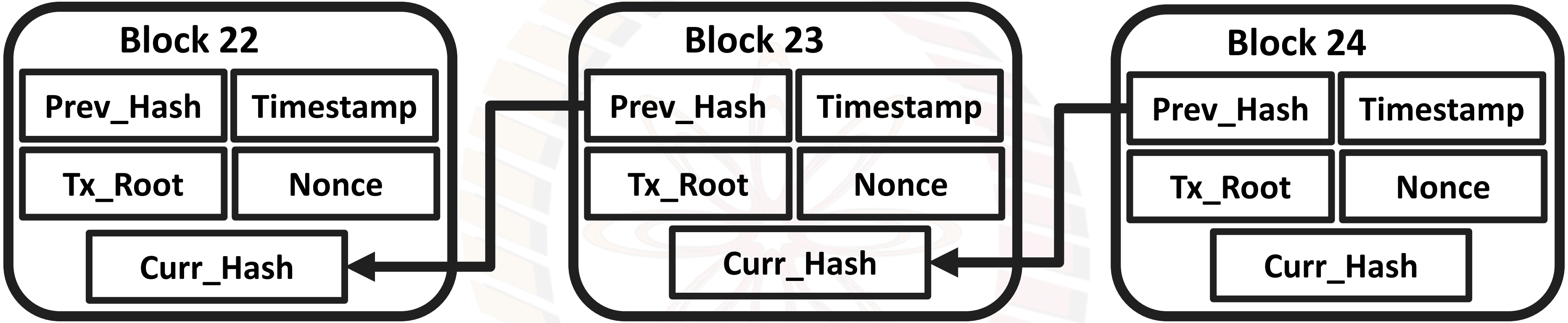
Bitcoin Proof of Work (PoW) System

- Most implementations of Bitcoin PoW use double SHA256 hash function

- The miners collect the transactions for 10 minutes (default setup) and starts mining the PoW

- The probability of getting a PoW is low – it is difficult to say which miner will be able to generate the block
  - No miner will be able to control the bitcoin network single handedly

Tampering PoW Blockchain

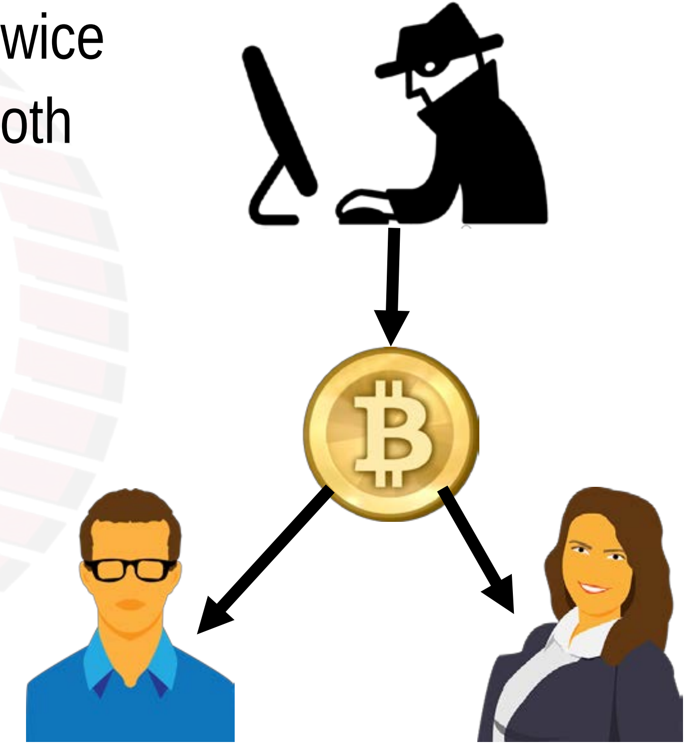


- The blockchain together contain a large amount of work
  - The attacker needs to perform more work to tamper the blockchain
  - This is **difficult** with the current hardware

Solving the 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



Sybil Attacks

- Attacker attempts to fill the network with the clients under its control
  - Refuse to relay valid blocks
  - Relay only attacked blocks – can lead to double spending

- Solution:
  - Diversify the connections – Bitcoin allows outbound connection to one IP per /16 (a.b.0.0) IP address

Denial of Service (DoS) Attacks

- Send lot of data to a node – they will not be able to process normal Bitcoin transactions

- Solutions:
  - No forwarding of orphaned blocks
  - No forwarding of double-spend transactions
  - No forwarding of same block or transactions
  - Disconnect a peer that sends *too many* messages
  - Restrict the block size to 1 MB
  - Limit the size of each script up to 10000 bytes
  - …

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

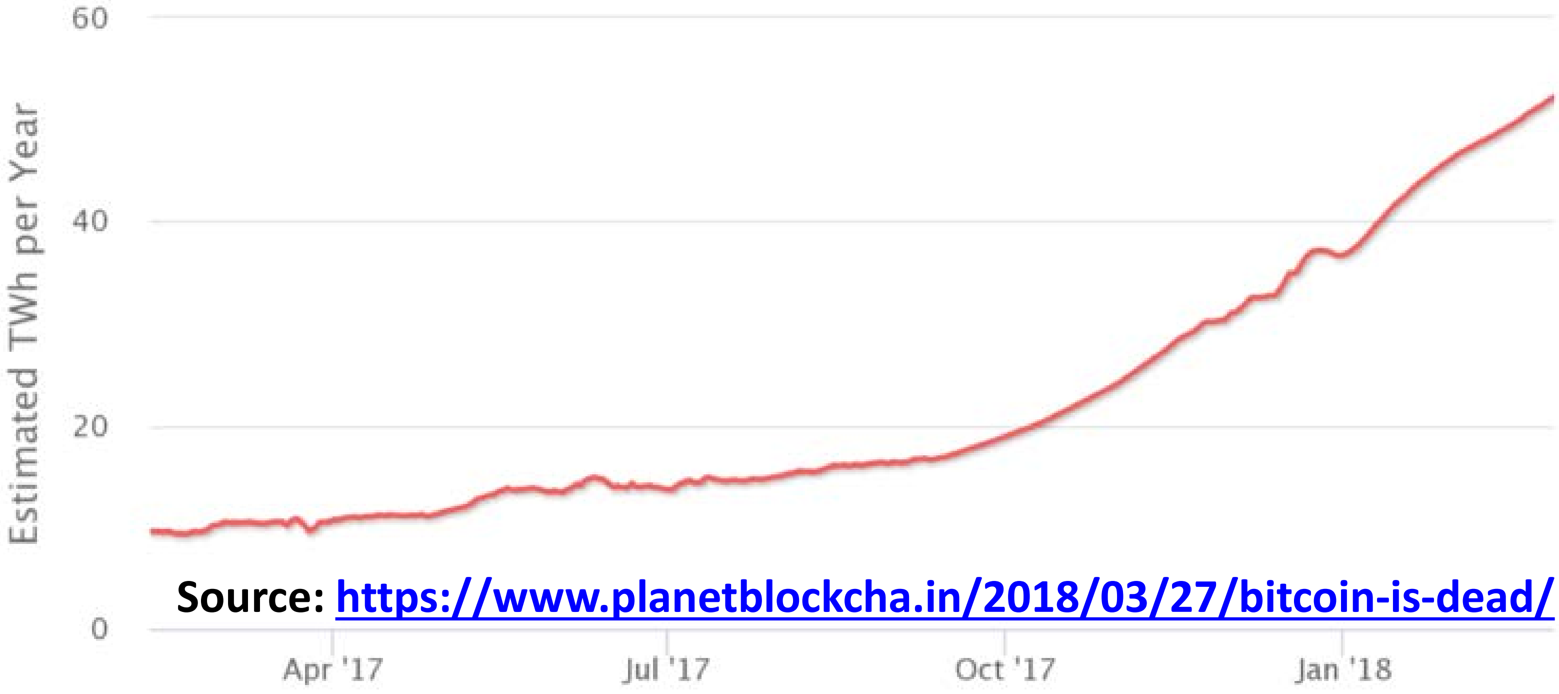
- A known case of successful double-spending
  - (November 2013) “it was discovered that the GHash.io mining pool appeared to be engaging in repeated payment fraud against *BetCoin Dice*, a gambling site” [Source: https://en.bitcoin.it/]

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

PoW Power Consumption



Source: https://www.planetblockcha.in/2018/03/27/bitcoin-is-dead/

Handling Monopoly and Power Consumption - Proof of Stake (PoS)

- Possibly proposed in 2011 by a Member in Bitcoin Forum - https://bitcointalk.org/index.php?topic=27787.0
  - Make a transition from PoW to PoS when bitcoins are widely distributed

- PoW vs PoS
  - PoW: Probability of mining a block depends on the work done by the miner
  - PoS: Amount of bitcoin that the miner holds – Miner holding 1% of the Bitcoin can mine 1% of the PoS blocks.

Proof of Stake (PoS)

- Provides increased protection
  - Executing an attack is expensive, you need more Bitcoins
  - Reduced incentive for attack – the attacker needs to own a majority of bitcoins – an attack will have more affect on the attacker

- Variants of “stake”
  - Randomization in combination of the stake (*used in Nxt and BlackCoin*)
  - Coin-age: Number of coins multiplied by the number of days the coins have been held (*used in Peercoin*)

Proof of Burn (PoB)

- Miners should show proof that they have *burned* some coins
  - Sent them to a verifiably un-spendable address
  - Expensive just like PoW, but no external resources are used other than the burned coins

- PoW vs PoB – Real resource vs virtual/digital resource

- PoB works by burning PoW mined cryptocurrencies

PoW vs PoS vs PoB

PoW

- Do some work to mine a new block
- Consumes physical resources, like CPU power and time
- Power hungry

PoS

- Acquire sufficient stake to mine a new block
- Consumes no external resource, but participate in transactions
- Power efficient

PoB

- Burn some wealth to mine a new block
- Consumes virtual or digital resources, like the coins
- Power efficient

Proof of Elapsed Time (PoET)

- Proposed by Intel, as a part of Hyperledger Sawtooth – a blockchain platform for building distributed ledger applications

- Basic idea:
  - Each participant in the blockchain network waits a random amount of time
  - The first participant to finish becomes the leader for the new block

PoET over Trusted Environments

- How will one verify that the proposer has **really waited** for a **random amount of time?**
  - Utilize special CPU instruction set – *Intel Software Guard Extension* (SGX) – a trusted execution platform
  - The trusted code is private to the rest of the application
  - The specialized hardware provides an attestation that the trusted code has been set up correctly

Interesting Reads ...

- Analysis of hashrate-based double-spending, by Meni Rosenfeld - https://bitcoil.co.il/Doublespend.pdf
- The proposal of PoS - https://bitcointalk.org/index.php?topic=27787.0
- The Peercoin protocol - https://peercoin.net/assets/paper/peercoin-paper.pdf
- Hyperledger Sawtooth - https://www.hyperledger.org/projects/sawtooth

thank you!