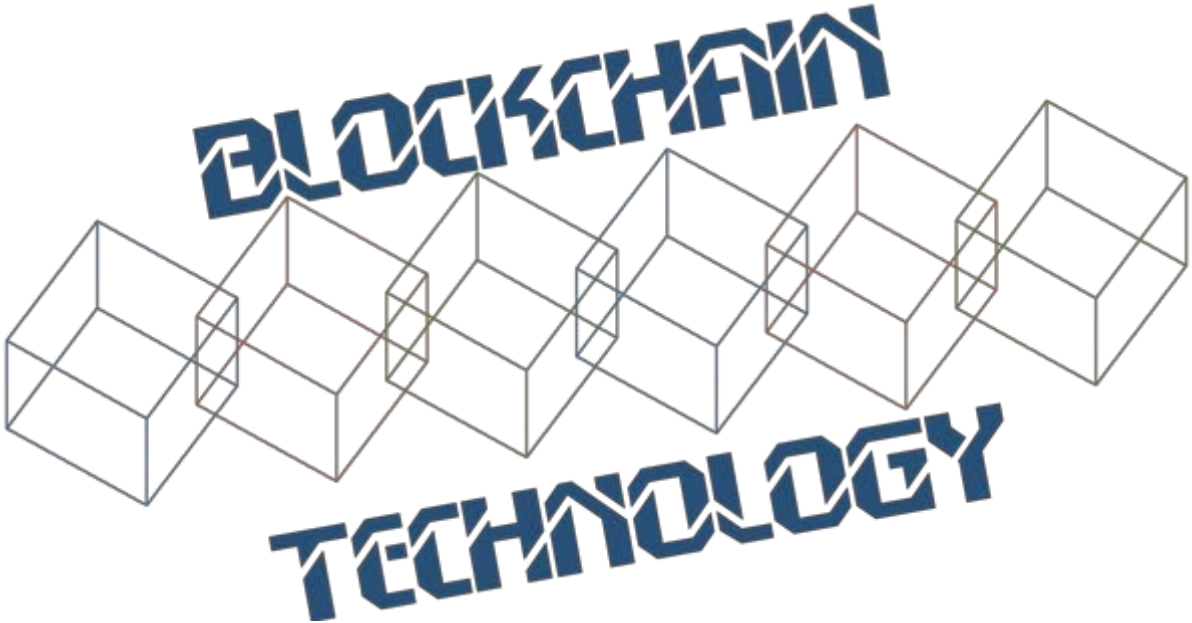


Image courtesy: http://beetfusion.com/

POW AND BEYOND

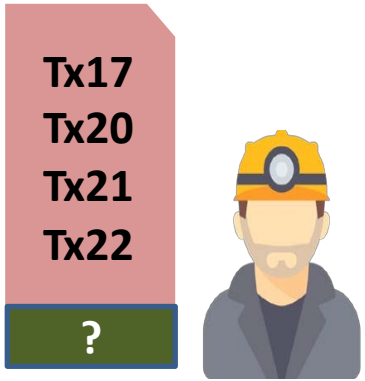
Outline of this lecture

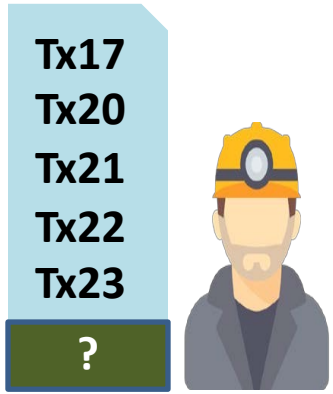
In last lecture, we have discussed about basic PoW mechanism in Hashcash. In this lecture, we will cover:

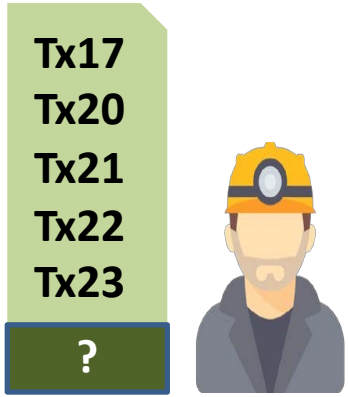
- How Bitcoin PoW extends the hashcash PoW based systems?
- How to develop a methodology to protect BC by applying distributed consensus mechanism?
- Discussion on other consensus Algorithms those are applied on permission less model of BC.
- How they utilize the concept of consensus algorithms to provide security in BC n/w?

Bitcoin Proof of Work (PoW)

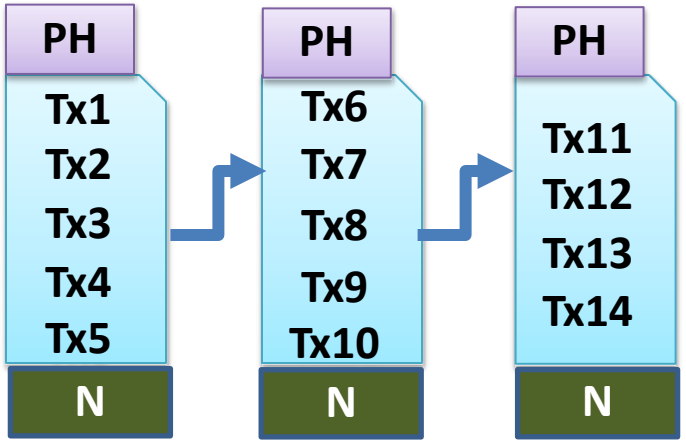
- Based on Hashcash PoW system
  - The miners need to **give a proof** that they have done some work, before proposing a new block
  - The attackers will be discouraged to propose a new block, or make a change in the existing blocks



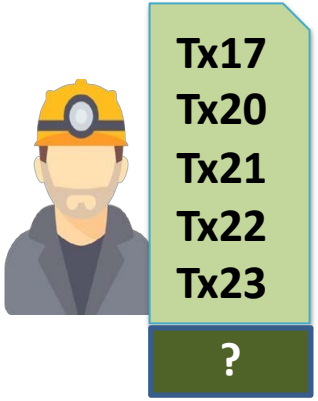


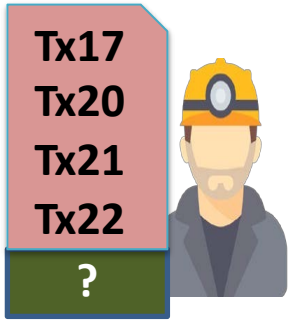


Methodology for Bitcoin PoW System



BH: Block Hash
PH: Previous Block Hash
MR: Merkle Root
N: Nonce (which is included in every block) Every miner is trying to find out this Nonce value, which will satisfy certain **Hash Equation**



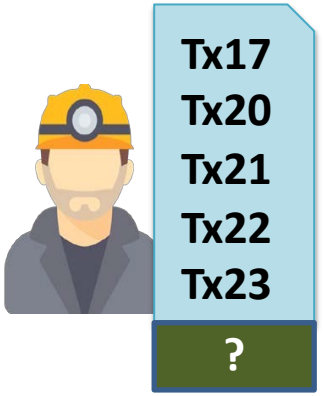


BH should have certain zeros (difficulty) at the beginning

BH = Hash(PH:MR:N)

N = ?

- Miners tries with **different values of N** to satisfy the difficulty
- Miners who will **first find out the value of N** for his own block then his/her own block will be added to the existing blockchain.



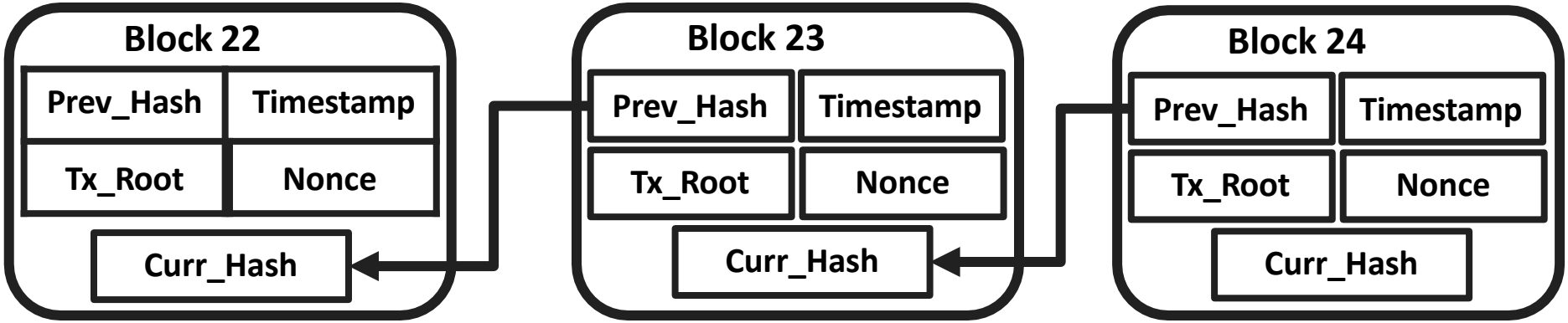
Bitcoin PoW System

- Most implementations of Bitcoin PoW use double **SHA256 hash function.**

- The miners collect the transactions for approximate **10 minute (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. Ideally it will not happen.
- **PoW also termed as "Nakamoto consensus"**

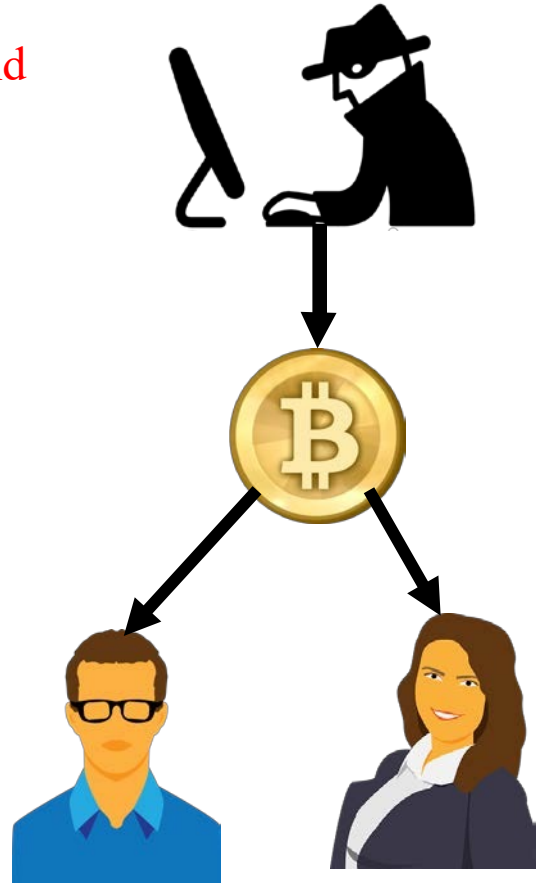
Why Bitcoin PoW is Tamperproof



- The blockchain together contain a large amount of work
  - The attacker needs to perform more work (greater than the total collective work done by all miners) to tamper the blockchain
  - This is **difficult** with the current hardware.
  - **But not impossible**, if the attacker can do the work by investing a huge hardware, which can compute the hash very fast and will be able to change the hash value of all blocks in the BC.

PoW also Solves the **Double Spending Problem**

- **The attack: means** "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
  - So, to make the system tamper proof PoW ensures that Double Spending problem not occurred



Next attack that can be occurred in PoW based systems Sybil Attacks

- Here, the attacker attempts to fill the network with the clients under its control then the attacker gets the control or monopoly of the n/w
  - 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
  - Example, if you have IP series of 172.16.--.--/16 then in this entire n/w you can have at most one peer that means if you diversify the n/w then it is expected that attacker may not generate multiple false miners (means they will be in the cluster within the same subnet). So, forward the block to multiple nodes rather than cluster of nodes in the same n/w.
  - BC makes the Sybil attack hard to implement on a distributed n/w.
  - It is always possible that multiple attacker's attacks on multiple subnet then collectively they launch the attack in a distributed way. But in real n/w hard to do it.

Attack that can be occurred in PoW based systems: **Denial of Service (DoS) Attacks**

- Here, the attacker send lot of data to a particular node then nodes will not be able to process normal Bitcoin transactions

- **Solutions: Set of Rules**
  - No forwarding of orphaned blocks (Orphan blocks are valid and verified blocks but have been rejected by the chain due to a time lag in the acceptance of these block)
  - No forwarding of double-spend transactions
  - No forwarding of same block or transactions twice
  - Disconnect a peer that sends *too many* messages
  - Restrict the **block size to 1 MB** because larger block becomes difficult to verify by the normal nodes. In less block size, it is easier to forward the block to many peers in the n/w.
  - Limit the size of each script up to **10000 bytes** (means how to match the output of a TX with the input of the next TX). Higher size open the door for attackers

Is it possible to Break the Bitcoin PoW ?

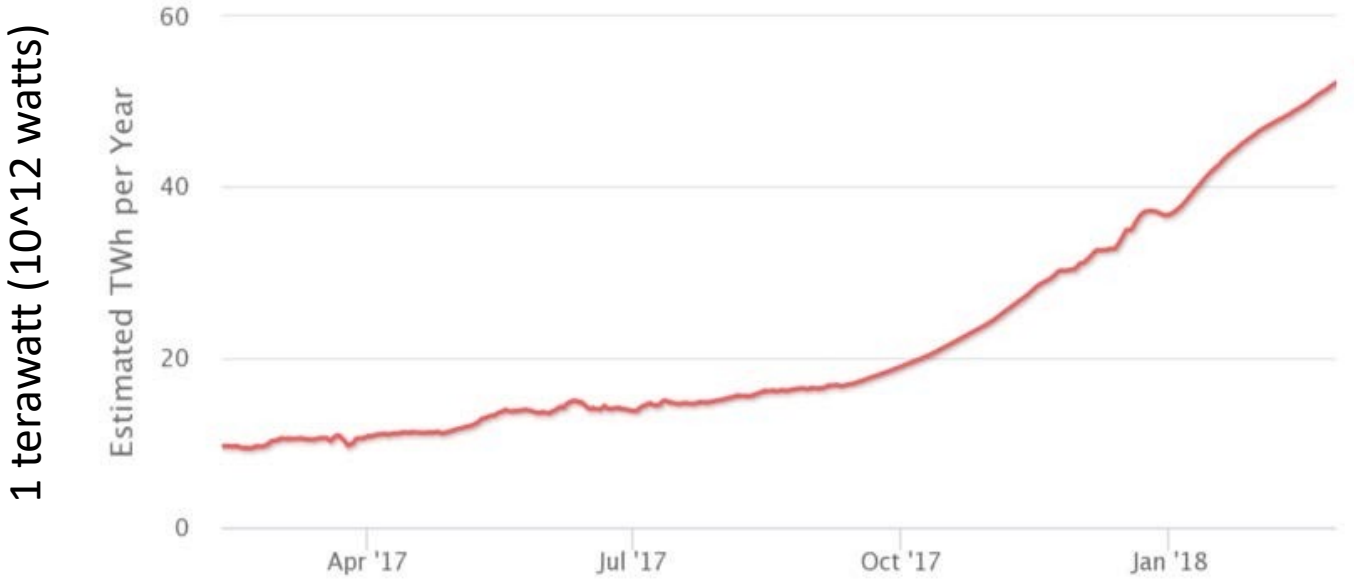
- Bitcoin PoW is **computationally difficult** to break, but not **impossible**
- Attackers can deploy **high power servers** to do more work than the total work of the blockchain.
- A known case of successful double-spending. **Example**
  - (November 2013) “it was discovered that the **GHash.io mining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

Here the double spending attack launched over the Bitcoin n/w

The Monopoly Problem in PoW based systems

- PoW depends on the computing resources available to a miner
  - Miners having more resources have more probability to complete the work
  - Like with GPU servers, they can do parallel computing of Hashing.
- Monopoly can increase over time (*Tragedy of the Commons-Statistical theory*)
  - 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.
  - This type of problem may arise in the existing Bitcoin n/w.

Another problem in PoW-based system is **Power Consumption**



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

To Handle 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. So, adding new block depends upon the computing resources of the miners
  - **PoS:** Amount of bitcoin that the miner holds – Miner holding 1% of the Bitcoin can mine 1% of the PoS blocks. It will break monopoly.

Proof of Stake (PoS)

- It provides increased protection
  - Executing an attack is **expensive**, you need more Bitcoins, if you want to generate more blocks.
  - **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 or wealth"
  - 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*)
  - Also, you have to hold the Bitcoins for certain durations.

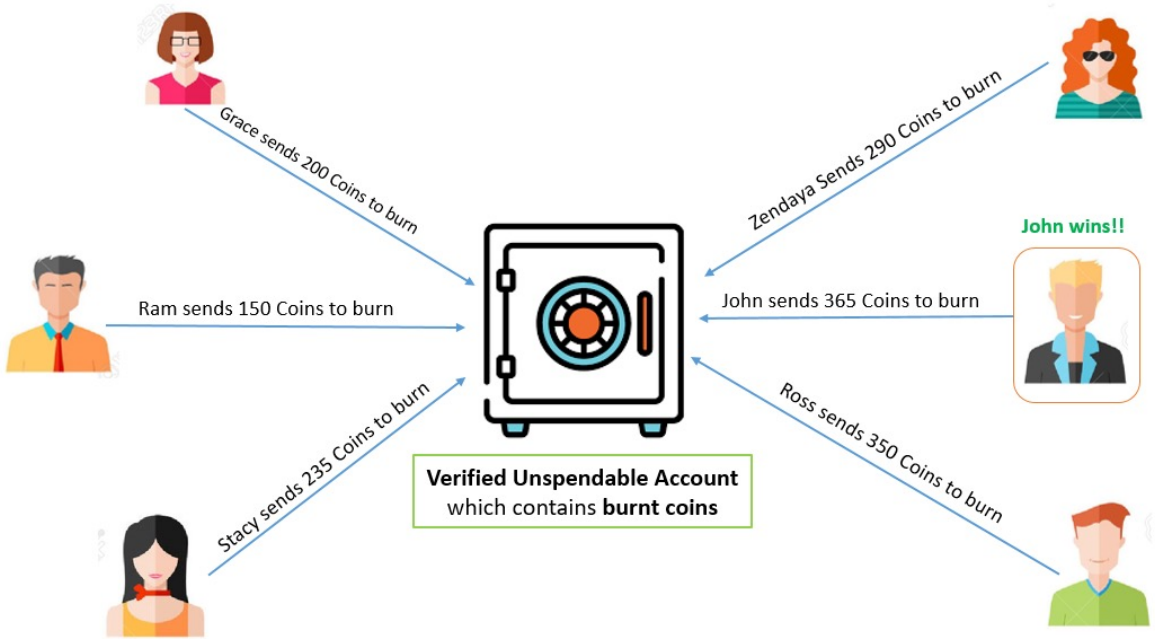
Proof of Burn (PoB)

- Miners should show a proof that they have *burned* some coins
  - Burned means that they have sent them to a verifiably un-spendable address (where no one will be able to spend Bicoins)
  - Expensive just like PoW, but no external resources are used other than the burned coins (spend only digital or virtual resources, which are the Bitcoins). **Attackers have huge loss of Bitcoins**
  - **PoB-based systems are power efficient?** because you are not utilizing physical hardware to do the work but spending digital currencies for the same. That's why it is efficient in terms of the power consumption.

- **Difference b/w PoW vs PoB** – Real resource vs virtual/digital resource

- **PoB** works by burning PoW mined cryptocurrencies means through PoW every one have some currencies then you can apply PoB.

PoB


Grace sends 200 Coins to burn
Zendaya Sends 290 Coins to burn
John wins!!
Ram sends 150 Coins to burn
John sends 365 Coins to burn
Stacy sends 235 Coins to burn
Ross sends 350 Coins to burn
Verified Unspendable Account
which contains burnt coins

Broad Differences PoW vs PoS vs PoB

PoW

- Do some work to mine a new block (means find Hash function)
- Consumes physical resources, like CPU power and time
- Power hungry

PoS

- Acquire sufficient stake to mine a new block (means prove you have certain Bitcoins to participate)
- Consumes no external resource, but participate in transactions
- Power efficient

PoB

- Burn some wealth to mine a new block (you have to spend certain Bitcoins rather than the physical currency to participate)
- Consumes virtual or digital resources, like the coins
- Power efficient because you are burning virtual currency not physical

Proof of Elapsed Time (PoET)

- Proposed by Intel, as a part of Intel Blockchain environment, which is called as **Hyperledger Sawtooth**– a blockchain platform for building distributed ledger applications
- **Basic idea:**
  - Here, each participant in the blockchain network waits a random amount of time
  - The first participant to finish becomes the leader for the new blocks
  - Means makes the randomization among the miners so the miner who complete this random waiting first that miner will be able to propose the new block first

PoET over Trusted Environments

- **Challenge-** How will one verify that the proposer has **really waited** for a **random amount of time**?
- If it is a software-controlled system, then attacker may do change in the code and may claim that I have waited for say 120 sec before participating in the mining procedure.
  - **To verify it,** Intel utilize a special CPU instruction set – *Intel Software Guard Extension* (SGX) – a trusted execution platform, which is a hardware code, where you can write:
  - The trusted code is private to the rest of the application, **so it is hardware controlled not software controlled**
  - The specialized hardware provides an attestation that the trusted code has been set up correctly.
  - It works for both permission less and permissioned environment, but PoW, PoB, and PoS they are primarily for permission less environment

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 (PoB) - https://peercoin.net/assets/paper/peercoin-_paper.pdf
- Hyperledger Sawtooth Platform - https://www.hyperledger.org/projects/sawtooth

Question: How longest chains are determined in Bitcoin?

- Longest chains are not determined by the maximum number of blocks in the chain.
- It is determined by the total work done (in terms of Proof of Work mining) for mining all the blocks in the chain.
- Note that the work done is a **function of the mining difficulty.**
- The intuition behind selecting the chain with the maximum work is that because such a chain will be more difficult to tamper as you have to do more work.

Question: What are orphaned blocks and how to remove them?

- The block from one of the miners (who will pass the difficulty posed by the network) will be the part of the longest chain, others will be marked as orphaned block and **will not be used.**
- Moreover, If there is a transaction inside an orphan block, then it should also be there in one of the valid block.
- The miners look whether the broadcasted transactions have been included in one of the valid blocks (nor the orphaned blocks);
- if not, they include them in the next mined block. The orphaned blocks can be removed afterwards.

Question: Can a miner propose an invalid block?

The miners are normal nodes, so it is highly possible that a miner is an adversary and it proposes an invalid block (a block with invalid transactions).

Question: What if a miner proposes an invalid block?

The invalid block gets propagated to the network. Whenever a node receives a new block, it does the followings before including it in the Blockchain - (a) validate all the transactions in the block, (b) ensure that the block does not have any double-spend transactions, (c) check the block is not a replay and is signed by the originator, (d) check the hash and the nonce of the block (verify the proof).
So, if a block contains an invalid transaction or a double-spend transaction, then the block is simply discarded.
[Again, this is the reason that you need sufficient transparency - you need to store the old transactions in your local machine].

Question: How does the first node in the blockchain get created?

It has been created manually, called the genesis block - https://www.investopedia.com/terms/g/genesis-block.asp

Question: How is it possible to have the copy of Public Ledger (which is increasing day by day) for every client? [Similar question: If the size of the Blockchain is few hundred GBs, then how do everyone store the blockchain in local machines?]

For reducing the size of the block, **several compaction techniques** are used. One such technique is called “Sharding".

Sharding is a technique in blockchain that achieve scalability within a blockchain network. It split a blockchain network into separate shards, that contain their own data, separate from other shards

Check this link for more details - https://medium.com/edchain/what-is-sharding-in-blockchain-8afd9ed4cff0

Question: Can the attacker tamper the last block?

- The hypothesis is as follows.
- Mining requires some time. Say the last block has been propagated in the network. When the miners observe a new block, they start working on the next block to be mined. So, by the time the attacker makes an alternation in the last block and propagate an altered copy of that block, a correct new block has been mined and added to the blockchain with the correct last block.
- So, the adversary has to change this new block as well, and the procedure goes on.
- Therefore**, it would be extremely difficult** (although, theoretically, not impossible) for an attacker to make a change even in the last block.

Question: How is the difficulty determined in bitcoin?

- In every 2016 blocks, the elapsed time between the first and last block is computed. Ideally, the value is nearly 2 weeks.
- If the actual value is less than 2 weeks, then the difficulty is increased at most 300%.
- If the actual value is greater than 2 weeks, then the difficulty is reduced by at most 75%.

Question: How is the mining incentive provided to the miners?

- All the miners who have solved the puzzle receive the equal incentive as in case of a single miner solve the puzzle.
- However, in every case, that incentive amount cannot be used for at least 100 blocks for confirming that the block is not an orphan block.
- The miners of an orphan block do not get any incentive.

Question: How is the Merkle tree root computed for the non-even transactions?

- The last transaction id is concatenated with a copy of itself and performed the hash.
- **For example,** the transaction ids are 1,2, and 3. Then, the combined hash will be formed as {1, 2}, and {3, 3}.

Question: What is the difference between transaction fees and block reward? Which one of them goes to the miner?

- Transaction fees are the amount that the spenders provide for the transaction.
- The block reward is the combination of the transaction fees and the block subsidy. The block subsidy is the incentive for creating the new block. Total block reward goes to the miner.
- However, as the block reward gets reduced gradually, the transaction fees can be increased to provide equal incentives to the miners all the time.

How does PoS solve monopoly?

- It is expected that when PoS is deployed, there is a uniform wealth share among the users.
- Monopoly can increase if the number of participants decreased.

How will the block hash be calculated in PoS and PoB?

You do not have a target hash in this case. Just calculate the block hash from the Merkle Root, Timestamp and previous block hash. The objective is to show that you have spend some resources. In **PoW,** the resource is the **physical computing resources** and computing power, in PoS, it is the stake that the miners have (coin-age), and in PoB it is the coins - the virtual resources. Spending computing powers, blocking stakes or burning coins can be thought of like the miners are investing some resources, and they can gain more coins after successful mining from the coinbase transactions and/or the transaction fees.

M1 can find more that one hash value with near optimal solution . Will he paid for all those solution ? Can he not abuse this technique to gain more pay?

Only the closest hash to the target is considered. And the miner has to give a proof by forwarding that hash value to the pool organizer.

What is the benefit of finding near optimal solutions ? The challenge is solved iff the complete solution is achieved?

Just a method to attract the miners to a pool. One miner from the pool will win, but then what is the gain for others.
Here, the miners know that the reward will be divided, and they will get at least some share - this attracts them to join in the pool.

PoB works by burning PoW mined blocks. Does that mean that PoB does not exist on its own , I mean it has to be implemented along with PoW to control the power and Monopoly problem that may arise from PoW.

- PoB or PoS will come into play once the mining strategy based on PoW won't suffice.
- And as we know that the inflow of bitcoins in the network is due to the mining activity people will spend the bitcoins that they have earned earlier because of the mining scheme that followed PoW.
- Thus the sentence comes as "PoB works by burning PoW mined cryptocurrencies".

Question: What if Alice wants to send two same transactions intentionally. I mean A to B 10 BTC , she wants to send twice. How will the other peers get to know that this is not a redundant transaction?

- Every transaction input must refer to previous unspent transaction outputs. In other words, Alice must point to one or more previous transactions where she was the recipient of bitcoins and that transaction output must not be the input of any other transaction.
- There are no balances in bitcoin, just coins. Alice must show which coins she is spending for each transaction.
- She would be double spending if she sends the same transaction inputs in 2 transactions and the network will reject duplicates.
- However, if she sends 10 BTC to Bob in 2 different transactions where she proves that she is the owner of 20 BTC, all of which is unspent, then this will not be a double spend.

Who decides what would be near optimal solution and how?

- Depends on the target hash.
- You can use a reverse calculation to compute the difficulty for a given hash.
- Say, there are three miners in a mining pool.
- Miner M1 generates a hash H1, M2 generates a hash H2 and M3 generates a hash H3. H1, H2, and H3 are the closest hash values of the target hash (these are near-optimal hashes) that the miners generate.
- Let D(H) is the difficulty of a hash value.
- Let D = D(H1)+D(H2)+D(H3).
- Then, M1 gets a share of D(H1)/ D,
- M2 gets D(H2)/D,
- and so on.

Transaction validation: for every transaction validation does previous blocks are cross-checked for verifying validity.. also based on the public address of sender can we also check/refer all transactions from previous blocks for that particular sender/receiver.

The actual validation process is pretty simple and does not require a check of all the previous transactions. To understand this, first note that in Bitcoin, there is no "balance", there are only "coins" in form of Satoshis (unit of Bitcoin, 1 BTC = 100,000,000 Satoshis). Now it all depends on individual transactions. Let in a transaction, you have received 200 Satoshis, so you can spend those 200 Satoshis. You may divide it into two transactions - 150 Satoshis to your friend Jerry and 50 Satoshis to your another friend Tom. So, we use something called Bitcoin scripts that just check whether these 150 Satoshis (to Jerry) and the 20 Satoshis (to Tom) are corresponding to the 200 Satoshis that you had received from a previous transaction. This also helps in preventing double-spending - you cannot send same Satoshi (the same coin) to two different transactions.

Question: In my car understanding the maximum possible hash values is when all the 256 bits are 1 or in other words in decimal it is 2^256-1. if this is chosen as the target no matter what the nonce is Everytime the block hash will be less than the target hash. Then why is this not chosen as difficulty 1?
How is the difficulty of 1 defined? Is it something having 48 zeroes and rest ones. Please clarify.

The total hash is 256 bits. Typically the target hash for "difficulty 1" is 32 bits as 0's and then (256-32)=224 bits are 1's (called pdiff) - this is the target hash for "difficulty 1" when the first block was mined by Nakamoto.

Now 32 bits 0s and 224 bits 1s can be represented as 0xffff * 2**208. Check this number. 0xffff means 16 1's and then you are making a shift of 208 bits (through 2**208) - so you have (208+16)=224 ones and the remaining 32 bits at the prefix are all zeros. So, this number 0xffff * 2**208 is called the offset for difficulty 1 - how many shifts you have to do over 0xffff to get the target hash for "difficulty 1".