Blockchain Technology Discussion on MSE paper (Oct 4, 2022)

Dr Dhiren Patel

Q1 A (4 marks)

A. List and discuss role of Cryptographic Security primitives used in Blockchain?

- Hash function (cryptographic) – SHA256, Data integrity (transactions, blocks, blockchain) – Merkle tree, Stitching blocks together - immutable distributed ledger, Mining a Block (Puzzle solving - PoW)
- Encryption – SKC (DES, AES, HF construction), PKC (RSA, ECC – Secp256k1), securing transactions confidentiality
- Key management and Key exchange – Private key/Public key, ECC Secp256k1 – key generation and Wallet addresses,
- Digital signature –authentication/signing transaction

Q1 B (2 marks each)

- 1. Explain Bitcoin difficulty adjustment.
- Done approx. every 2 weeks (time it took to find the last 2,016 blocks),– difficulty (puzzle) <number of leading zeros> is increased or decreased to keep av. time between blocks to 10 min.
- 2. How crypto-currencies are different than Fiat currencies?
- Crypto currencies are digital assets designed to work as medium of exchange that uses strong cryptography to secure transactions, control the creation of units, and verify the transfer of assets in decentralized manner (community controlled), e.g. Bitcoin, universal currency (border less), censorship resistant
- Fiat - centralized currency through central banking systems (govt.), highly regulated by central authorities, financial institutions and IMF, e.g. USD
- Circulation, Max. Supply, Collateral, National currency

Q1 B

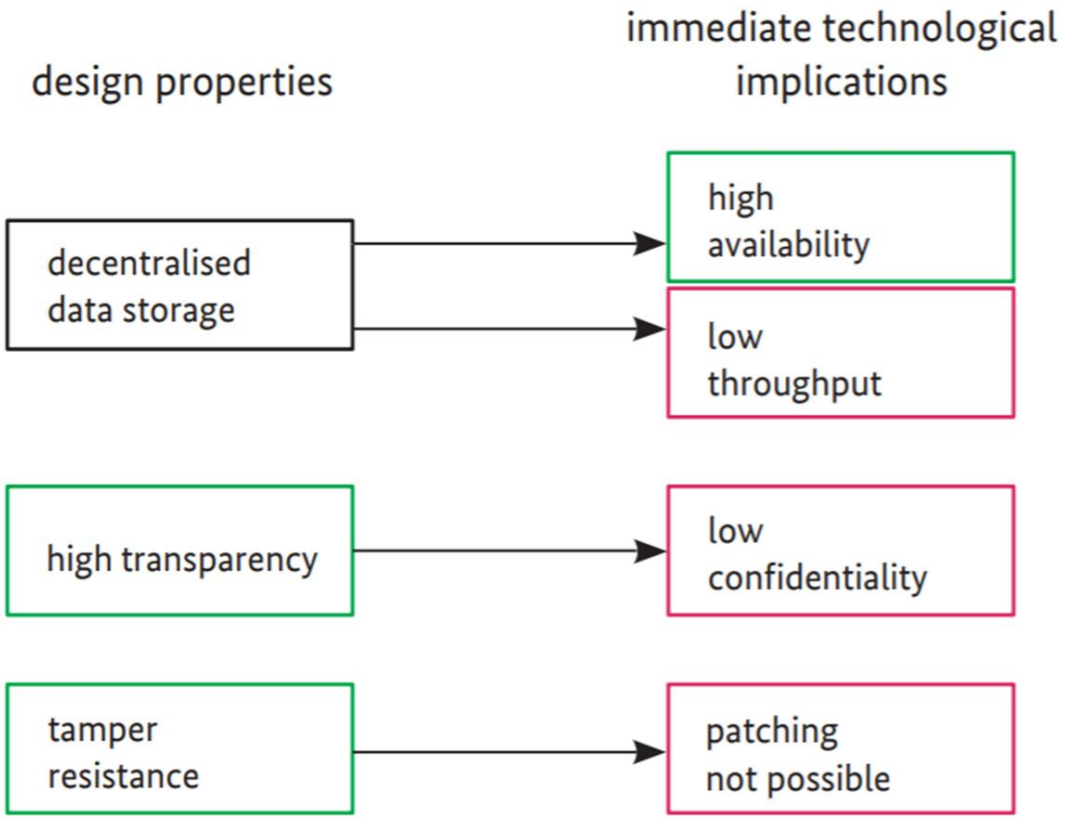
- 3. Give your comments on Bitcoin energy usage.
- Bitcoin’s energy usage depends on how many miners are operating on its network at any given time. These miners must compete against each other to win the right to add the next block to the blockchain and earn rewards. The competitive structure results in a lot of wasted energy as only one miner can add a new block every 10 minutes. At its present level (Aug 2021), Bitcoin consumes 81.51 terawatt hours (TWh) annually.
- However, Bitcoin uses less than half the energy the banking system consumes

Q1 B

- 4. Discuss Forks in blockchain.
- Forks are for Handling exceptions. Forks are mechanisms that add to the robustness of the blockchain framework.
- A **Soft Fork** is a fork where updated versions of the protocol are backwards compatible with previous versions.
- •A **Hard Fork** is a change of the protocol that is not backwards compatible with older versions of the client. Participants would absolutely need to upgrade their software in order to recognize new blocks.
- Soft Fork - a minor process adjustment has to be carried out typically by bootstrapping a new software to the already running processes
- Hard fork implies a major change in the protocol (sort of – a new version of operating system)

Q1 B

- 5. List design properties of Blockchain and their technology implications



Q2 A

- **Answer the following (Choose only one correct answer out of A,B,C,D)**
- 1. What is genesis block?
- A. The first transaction of a blockchain B. The first block of a blockchain
- C. The last block of a blockchain D. A block created by Founder
-
- 2. What is the coinbase blockc reward for miners currently in Bitcoin blockchain.
- A. 6.25 BTC B. 12.5 BTC C. 25.00 BTC D. 50.00 BTC
-
- 3. Which of these fields is present in Bitcoin Blockchain summary?
- A. Gas limit B. Difficulty C. Private key of Sender D. None of the above
-
- 4. What is the smallest denomination of crypto-currency ether?
- A. Satoshi B. Wei C. Uni D. Luna

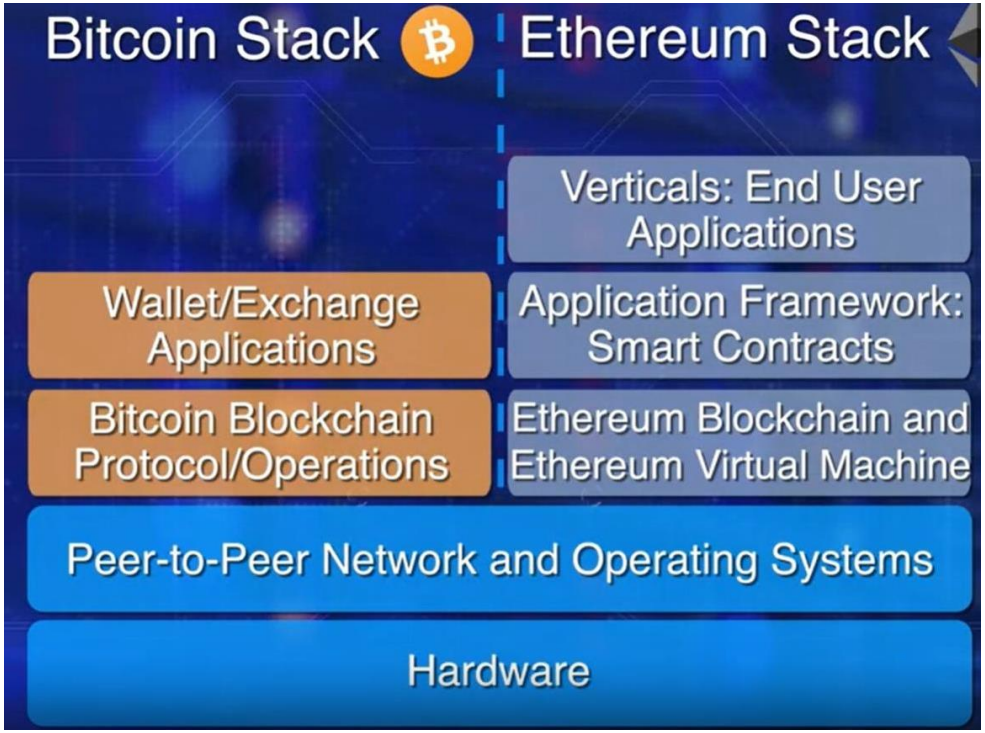
Q2 B

- 1. Discuss DeFi and NFT.
- Decentralized finance is an exit from traditional banking services and norms. Smart contracts in DeFi are facilitating the exchange of goods, services, data, funds and so on. Users of centralized financial institutions, such as banks and credit unions, rely on intermediaries to execute a transaction. Whereas, DApps are using smart contracts to ensure that each action is genuine, transparent, and free of human error.
- NFT – Non Fungible Tokens, represent unique assets that are not further divided. A smart contract is a tool that allows implementing a sale agreement between the NFT owner and the buyer. The smart contract contains information on the NFT, such as the work's creator, other parties who are entitled to royalties each time the NFT is sold, and the work's ownership history.

Q2 B

- 2. Compare Bitcoin and Ethereum – as currency, as blockchain, and transaction components.

Currency – BTC (1 BTC ~20K USD)
Eth – 1 Eth ~1300 USD
As Blockchain – both uses PoW consensus mechanism, Eth2 is now PoS.
BTC – store of value,
Eth – exchange of value, platform for smart contracts
Transaction components – gas price (for computations), contract address,

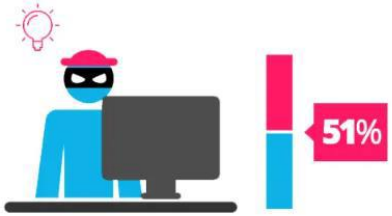


Q2 B

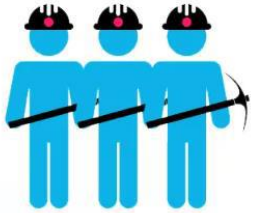
- 3. What is Mining and what is Validation? Discuss Proof of Work and Proof of Stake.
- validation involves checking the time-stamp and the nonce combination to be valid and the availability of sufficient fees for execution
- mining is the process used to secure the network by validating the computations, collecting them to form a block, verifying them, and broadcasting it
- PoW – consumes lot more computation due to winner takes it all competition (miners) (energy)
- PoS – designated stake holders (verfiers) – much less energy
- PoW - bad actors are cut out thanks to technological and economic disincentives
- PoS - a bad validator may lose deposit

Proof of Work vs. Proof of Stake

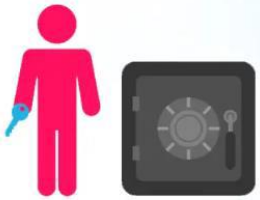
To add each block to the chain, miners must compete to solve a difficult puzzle using their computers processing power.



In order to add a malicious block, you'd have to have a computer more powerful than 51% of the network.



The first miner to solve the puzzle is given a reward for their work.



There is no competition as the block creator is chosen by an algorithm based on the user's stake.

In order to add a malicious block, you'd have to own 51% of all the cryptocurrency on the network.

There is no reward for making a block, so the block creator takes a transaction fee.

More…

- UST callapse –
  "stablecoin“ that was not very stable
- NFTs Will Disrupt Any Industry That Lacks Transparency
- Web3
- use cases for NFTs are beyond art, and NFT memberships and rewards programs are with high potential