IN5420. Summary 1 Bitcoin. Ivan Shirshikov

What is a Merkle Tree?

Merkle Tree is a datastructure used in Bitcoin Blockchain. It provides scalability, maintain hash-based architecture, data integrity and the way to easily verify the integrity of data.
Merkel proof - allow data verification without nodes` hash, only based on root hash

In bitcoin Merkel Tree stores transaction in blocks. Root hash that is stored in block allows to verify transactions even in SPV (lightweight) nodes. Can be used in other blockchains (ex. Eth - Merkle Patricia Trees). Also plays a huge role in version contol systems like Git and IPFS

Hash function generate output of same size and unique on input every time. Even if difference is little. Using of cryptographic hashes without Merkle Tree is extremely unefficient and not scalable.
Structure of Merkle Tree: Data blocks are stored in leaf components and hases connects to each other to the top using hash combinations of neighbours. It can take the “N” amount of hashes and represent it with a single hash. Tree structure allows us to detect the pace where changes occured. The root hash can be used as the fingerprint for an entire dataset.

Merkle Trees in Bitcoin: Cryptographic hash function: SHA-256 alg. This stands for Secure Hashing Algorithm, whose output is a fixed 256 bits in length. In Bitcoin miners add transactions in blocks and hash them using merkle tree.
SPV nodes dont download the whole blockchain. They only download block headers and need only root hash to verify that transaction included. Because of the structure we can prune blocks (because we are saving hashes in merkle branch) so allowing storage optimizaiton.

Understanding blockchain: definitions, architecture, design, and system comparison

State Tracking approach: Bitcoin employs the unspent transactional output (UTXO) approach. Tracks only unspent (TXO - transactional output) balances. Require wallets on client side to keep track of UTXO. Bitcoin has no data-retantion policy (all data a lifetime accessible). UTXP allows for a parallel processing of transactions while account based sequensionally based on balance.
Bitcoin block size is 1MB, while Eth is limited by gas usage. In memory storage: Block index database, UTXO cache, & Merkle trees of transaction

The two available operations add transaction and get state. Bitcoin uses PoW (Proof of work) consensus alg and logest chain rule giving transaction confirmation. Longer chaing after block - stornger confirmation.
Blockchain info is stored in db like LevelDB or RocksDB. Key- value tracks. Bitcoin uses LevelDB. Blocks is stored on local disk. LevelDB for indexing. Getting blockchain data is easier than updating - no need in consensus, but is limited by db (you can not filter data or sort). Only simple operations is available in such dbs like find trak by hash. To overcome these limitations you can use thrd party libs like BlockchainSQL

PoW helps to fight with DoS attacks.

Performance in Bitcoin: Throughput : 3-7 TPS, probabalistic counts as confirmed after 6 blocks of confirmation, mining power utilization (how much energy is spent on block creating) above 99% in bitcoin

Chapter 5: Bitcoin Mining

Two types of tasks:validationg transactions and blocks, race to find blocks and profits

1. Finding a valid block (nonce). After getting nonces miner calculate if it validates using target difficulrty
2. Determining the difficulty every 2016 blocks (2 weeks) in such way that avg block creation time will be 10 mins

3. Miners uses GPU,because CPU is not profitable due difficulty. Also graphic card can be overclocked. Disadvantages of GPU mining: a lot of hardware that is not utilized for mining, cooling charachteristics, a lot of power
4. FPGA mining.Field Programmable Gate Arrays: a lot of errors and still 50 years of mining, less accessible. Only few moths until ASIC arrived
5. ASIC mining: application-specific integrated circuits- chips for bitcoin mining. Until 2015 short lifetime. Not profitalbe- profit in case of bitcoin growth.
6. Today: professional mining centers. Newer and efficient ASIC.
7. The future : future is not bright for individual miners
8. Energy consumption: you need to use some amount of joules to flip one bit unreversible. Embodied energy, Electricity, cooling. To estimate a cost of mining - Top-down(benefit to energy) or bottom-up approach (hashes to energy). Good idea- repurposing energy (heat)
9. Mining pools - few together. Mining shares. Proportional pay-per-share in pool. In 2014 50% of power was in one pool. They make mining fair for small players and one operator - easier to update the network. The main disadvantage - form of centralization, decrease of number of fully validated nodes.
10. To get more profit - implement different strategies.
11. Types of attacks: forking attack (51%), temporal block-withholding attacks (dont announce about found) attack. No way to blacklisting

Chapter 8: Alternative Mining Puzzles

Checking solution is trivial and doesnot depends on how difficult it was. Progress freeness. The chance of winning the puzzle - roughly proportional t the hash used.
Adjustable difficulty, fast verification, and progress-freeness are three crucial properties of Bitcoin mining puzzles. We want ot create ASIC resistant (reduce the gap between most used and most effective). Memory- hard puzzles. The most popular memory-hard puzzle is called scrypt. Time-memory tradeoff: halving our memory requirement increases the number of SHA-256 computations by only a

quarter (from 2N to 5N/2) example from scrypt. The ASIC honeymoon - lack of ASICs on new altcoins

Proof of Useful work - a lot of energy without any social use. Limited data availablity and limited real world impact. Permacoin - Proof of Storage. Miners stores useful data

We should limit creating of pools. Block discarding attack - not giving info to pool about success. Rewarding the sabotage. A modified mining puzzle is proposed where miners must know the private key of the pool manager to submit valid blocks. 2 choices : any of them can steal money or computing the signature(more expensive) itself
Proof of Stake: +: Lower energy need, no special devices, majority of stake to validators.- : can mince a lot of multiple forks, centralization risk (51% staked), a lot of potential attacks.
PoW is more secure and decentralized

PROOF-OF-X (POX) SCHEMES

The byzanitine generals problem: n≥ 2f + 1 to tolerate, but n≥ 3f +1 to reach the consensus

PoW: monopoly risk

Alternative PoW: Memory-bound, Primecoin, Permacoin

PoS. Coin age (amount of coin * time held)

PoA (Proof of Activity) - hybrid PoW and PoS. Miners solve PoW empty block, empty block is sending in network and N amount of people provide transactions there.
Proof of Publication. CommitCoin – Provable Commitments. Bitcoin address that codes important data and sending some bitcoins there counts as commitment

Proof of burn - burn coins to mint new one.