IB Case Study Vocabulary

A local economy driven by blockchain (2020)

Websites

Merkle Tree: https://blockonomi.com/merkle-tree/

Blockchain: https://unwttng.com/what-is-a-blockchain

Mining: https://www.buybitcoinworldwide.com/mining/

Attacks on Cryptocurrencies: https://blockgeeks.com/guides/hypothetical-attacks-on-cryptocurrencies/

Bitcoin Transaction Life Cycle: https://ducmanhphan.github.io/2018-12-18-Transaction-pool-in-blockchain/#transaction-pool

51 % attack - a potential attack on a blockchain network, where a single entity or organization can control the majority of the hash rate, potentially causing a network disruption. In such a scenario, the attacker would have enough mining power to intentionally exclude or modify the ordering of transactions.

Block - records, which together form a blockchain. ... Blocks hold all the records of valid cryptocurrency transactions. They are hashed and encoded into a hash tree or Merkle tree. In the world of cryptocurrencies, blocks are like ledger pages while the whole record-keeping book is the blockchain. A block is a file that stores unalterable data related to the network.

Blockchain - a data structure that holds transactional records and while ensuring security, transparency, and decentralization. You can also think of it as a chain or records stored in the forms of blocks which are controlled by no single authority.

Block header – main way of identifying a block in a blockchain is via its block header hash. The block hash is responsible for block identification within a blockchain. In short, each block on the blockchain is identified by its block header hash. Each block is uniquely identified by a hash number that is obtained by double hashing the block header with the SHA256 algorithm. One important aspect to note here is the fact that the header hash is NOT stored in the block structure. Instead, it's calculated by each node as the block is "received" through the network.

The block header is an 80-byte long string. It is comprised of the 4-byte long Bitcoin version number, 32-byte previous block hash, 32-byte long merkle root, 4-

byte long timestamp of the block, 4-byte long difficulty target for the block, and 4-byte long nonce used by miners.

Candidate block - a block that a mining node (miner) is trying to mine in order to receive the block reward. So, a candidate block may be described as a temporary block that will be either validated or discarded by the network. Miners compete with each other to validate the next block and add it to the blockchain, but first, they have to create a candidate block to participate in the mining competition.

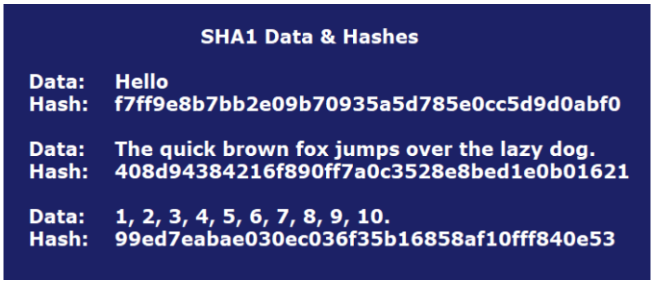
Candidate blocks - created by miners by collecting and organizing multiple unconfirmed transactions from the memory pool. The transactions are then hashed to form a Merkle tree structure, which will eventually produce a Merkle root (or root hash).

Collision resistance - is a property of cryptographic hash functions. A hash function is considered collision resistant if it is hard to find two inputs that hash to the same output.

Why do collisions matter? Because when you're creating a block in a blockchain, if you can get the same hash from different input, that means you can legitimately change data in a previous block without anyone noticing because the history doesn't rearrange. The hash remains the same, so the history remains the same, but suddenly someone has a lot more bitcoin in his wallet.

Cryptocurrency - a type of digital or virtual money. It serves as ordinary money, such as dollars, pounds, euros, yen, etc. But it has no physical counterparts — banknotes or coins that can be carried around, that is, the cryptocurrency exists only in electronic form. It uses cryptography for security and anti-counterfeiting measures.

Cryptographic hash - a method of cryptography that converts any form of data into a unique string of text. Hashing is a mathematical operation that is easy to perform, but extremely difficult to reverse. (The difference between hashing and encryption is that encryption can be reversed, or decrypted, using a specific key.) The most widely used hashing functions are MD5, SHA1 and SHA-256. Some hashing processes are significantly harder to crack than others.



```
             SHA1 Data & Hashes

Data:   Hello
Hash:   f7ff9e8b7bb2e09b70935a5d785e0cc5d9d0abf0

Data:   The quick brown fox jumps over the lazy dog.
Hash:   408d94384216f890ff7a0c3528e8bed1e0b01621

Data:   1, 2, 3, 4, 5, 6, 7, 8, 9, 10.
Hash:   99ed7eabae030ec036f35b16858af10fff840e53
```

The average user encounters hashing daily in the context of passwords. For example, when you create an email address and password, your email provider likely does not save your password. Rather, the provider runs the password through a hashing algorithm and saves the hash of your password. Every time you attempt to sign into your email, the email provider hashes the password you enter and compares this hash to the hash it has saved. Only when the two hashes match are you authorized to access your email.

Determinism – a property of a Blockchain that states that the same operation performed across different nodes should return the same result. All operations on the Blockchain should be deterministic. That is, no matter how many times you run the function on the same input, the output will always be the same.

Digital signature - A digital signature refers to a set of algorithms and encryption protections used to determine the authenticity of a document or software.

In simpler terms, a digital signature is a complicated way to verify that a document hasn't been tampered with during transit between sender and signer.

Distributed consensus - protocols that make sure all nodes (device on the blockchain that maintains the blockchain and (sometimes) processes transactions) are synchronized with each other and agree on which transactions are legitimate and are added to the blockchain.

Double-spend problem - occurs when a blockchain network is disrupted and cryptocurrency is essentially stolen. The thief would send a copy of the currency transaction to make it look legitimate or might erase the transaction altogether. Although it is not common, double-spending does occur.

Entropy - In cryptography, entropy is a measure of true randomness. An n-bit number chosen uniformly at random with a perfect random number generator has n bits of entropy, and entropy of other things can be computed in comparison to this case.

Genesis block - the first block in any blockchain. It is the foundation on which additional blocks are sequentially added to form a chain of blocks, resulting in the term, blockchain being coined. The genesis block is also referred to as block zero.

Immutable transactions - Immutable simply means **unchangeable**. Immutable transactions are transactions in a blockchain ledger that remain a permanent, indelible, and unalterable history of the ledger.

Why does immutability matter? One reason is that it provides complete data integrity. Ledgers that deploy blockchain technology can guarantee the full history and data trail of an application: once a transaction joins the blockchain, it stays there as a representation of the ledger up to that point in time. The integrity of the chain can be validated at any time by simply re-calculating the block hashes—if a discrepancy exists between block data and its corresponding hash, that means the transactions are not valid. This allows organizations and its industry regulators to quickly detect data tinkering.

Key pair generation - In the Public key protocol, two keys are used one key is used for encryption and another key is used for decryption. One key (public key) is used for encrypting the plain text to convert it into cipher text and another key (private key) is used by receiver to decrypt the cipher text to read the message.

Ledger - At its core, a blockchain is a ledger through which data is added and updated in real-time via consensus of the different nodes running the software in the network. However, once the data is added to the ledger, it cannot be removed or edited like with a database. This is a product of the overall design of blockchains.

Merkle proof – technique used to verify that the hashing of data in a Merkle tree is consistent all the way up the tree and in the correct position without having to actually look at the entire set of hashes. Instead, they can verify that a data chunk is consistent with the root hash by only checking a small subset of the hashes rather than the entire data set.

Merkle tree - A Merkle tree is a **hash-based data structure** that is a generalization of the hash list. It is a tree structure in which each leaf node is a hash of a block of data, and each non-leaf node is a hash of its children. Typically, Merkle trees have a branching factor of 2, meaning that each node has up to 2 children.

Merkle trees are used in distributed systems for efficient **data verification**. They are efficient because they use hashes instead of full files. Hashes are ways of encoding files that are much smaller than the actual file itself. Currently, their main uses are in peer-to-peer networks such as Tor, Bitcoin, and Git.

Miner - The role of miners is to secure the network and to process every transaction. Miners achieve this by solving a computational problem which allows them to chain together blocks of transactions (blockchain).

Mining - Cryptocurrency mining is a process in which transactions for various forms of cryptocurrency are verified and added to the blockchain digital ledger. Each time a cryptocurrency transaction is made, a cryptocurrency miner is responsible for ensuring the authenticity of information and updating the blockchain with the transaction. The mining process itself involves competing with other crypto miners to solve complicated mathematical problems with cryptographic hash functions that are associated with a block containing the transaction data.

The first cryptocurrency miner to crack the code is rewarded by being able to authorize the transaction, and in return for the service provided, crypto miners earn small amounts of cryptocurrency of their own. In order to be competitive with other crypto miners, though, a cryptocurrency miner needs a computer with specialized hardware.

Nonce - A nonce is an abbreviation for "number only used once," which is a number added to a hashed—or encrypted—block in a blockchain that, when rehashed, meets the difficulty level restrictions. The nonce is the number that blockchain miners are solving for. When the solution is found, the blockchain miners are offered cryptocurrency in exchange. The world of crypto mining is challenging, and one often needs excellent computational power to even begin to try and solve the nonce.

Non-invertibility – a property of a hashing algorithm that says that it should be impossible, or at least prohibitively difficult, to work out the input that led to any given hash. Ideally, it should be easy to transform data into a hash, and practically impossible to go the other way.

Nonrepudiation – Nonrepudiation is a method of guaranteeing message transmission between parties via digital signature and/or encryption. It is often used for digital contracts, signatures and email messages.

Imagine receiving a harassing email from someone who denies sending the message. How do you determine the truth? Digital signatures prove the delivery and receipt of email transmissions, guaranteeing nonrepudiation.

Thus, nonrepudiation protects the recipient and the sender when a recipient denies receiving an email. Without nonrepudiation, an essential pillar of IA, information security would be significantly flawed.

One-way function - A one-way function is a mathematical function that is significantly easier to compute in one direction (the forward direction) than in the opposite direction (the inverse direction).

Proof of work - The initial concept of Proof of Work was developed in 1993, as a way to prevent denial of service attacks and other service abuse (such as spam on a network). It consisted of requiring some kind of work from the users, usually involving computer processing.

In 2009, Bitcoin introduced an innovative way of using Proof of Work, as a **consensus algorithm**. In this case, PoW is used to validate transactions that are gathered into blocks, which are linked together to form a blockchain.

Since then, PoW has spread to become a widely used consensus algorithm and is now deployed by many cryptocurrencies. It works by having miners compete against each other in solving complex computational puzzles. These puzzles are difficult to solve, but when solved, the solutions can be quickly verified. So, once a miner finds the solution to a new block, they can broadcast that block to the network. All other miners will then verify that the solution is correct, and the block will likely be confirmed.

PuTTYgen - is a program that can generate SSH key pairs (public and private), which are special files you can use for encryption, authentication, and so on.

Self-referential data structure - are those structures that have one or more pointers which point to the same type of structure, as their member. In other words, structures pointing to the same type of structures are self-referential in nature. Examples of self-referential data structures include linked lists, stacks, queues, trees, graphs, and heaps.

SHA256 - (**Secure Hash Algorithm**) is a one-way function that converts a text of any length into a string of 256 bits. In this case, it is a cryptographically secure hashing function, in that knowing the output tells you very little about the input. A cryptographic hash is like a signature for a data set.

Takeover attack – not sure about this one. I guess the 51% attack is an example of a takeover attack. There is something called an Account Takeover Attack (ATO), but it does not have anything to do with cryptocurrency.

Transaction pool – place where all unconfirmed transactions reside. A transaction pool is stored on a special device and its contents can be accessed, observed in real time by any node on the network.

Before adding a transaction to their block, a **miner** needs to check if the transaction is eligible to be executed according to the blockchain history. If the sender's wallet balance has sufficient funds according to the existing blockchain history,
the transaction is considered valid and can be added to the block.