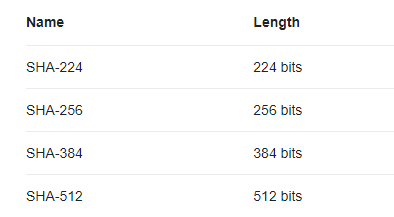
1. explain some of the ways hashing functions enable blockchain technology.

A hash is a function that meets the encrypted demands needed to solve for a blockchain computation.

Hash functions are commonly used to protect the integrity of data. Given a trusted hash of the data, it is possible to calculate the hash of the data and compare the two values. If they match, then the data has likely not been modified since the original hash was created.

Hashes are of a fixed length since it makes it nearly impossible to guess the length of the hash if someone was trying to crack the blockchain. The same data will always produce the same hashed value.



SHA-0

Sha-0 was the initial SHA series hashing algorithm. It has a digest size of 160-bits. It was soon replaced by SHA-1 that although also 160-bits, was more secure. SHA-0 is not used anymore in cryptographic keys

SHA-2

SHA-2 came very soon after the SHA-1 release and started standardizing different output sizes. From SHA-224, SHA-256, SHA-12 and others.

SHA-256

SHA-256 allows a bigger maximum message size which is 2⁶⁴ bits, digest size of 256 bits, block size of 512 bits and word size of 32 bits.

The SHA-256 hard limit allows inputs up to 2097152 Terabytes. SHA-256 has a 32-bits output. Normal computers use SHA-256 all the time, and this is also one of the foundational hashing algorithms behind Bitcoin and many other blockchains.

SHA-384 and SHA-513

These two SHA have a maximum message size of 2¹²⁸ bits that is better than SHA-256, and requires more computing power. The maximum block size is 1024 bits, and the word size of 64 bits. They compute with 64-bits and use pretty much the same operations as SHA-256 and SHA-224, and they perform 80 rounds.

SHA-3

SHA-3 was created in 2015, and it allows different sizes from 224, 256, 384 and 512 bits. The Keccak algorithm used in Ethereum is part of the SHA-3 family. SHA-3 can provide an output in different sizes according to the needs, and block sizes vary based on the digest size, from 576 to 1152 bits. The SHA-3 performs 24 rounds.

1. briefly explain Bitcoin's UTXO model of transaction validation (separate from POW).

The UTXO model allows Bitcoin nodes to efficiently verify every transaction on the blockchain. When a node receives a transaction, either in the mempool or as part of a block, it can verify whether the UTXOs being spent are valid and unspent.

In short, The UTXO model is a verification model. This means users submit transactions that specify the results of the state transition, defined as new transaction outputs spendable by the receiver(s). Nodes then verify if the consumed inputs are unspent and if the signature(s) satisfy the spending conditions.

1. what is the structure of a Block in bitcoin and how does it relate to the 'blockchain' (merkle tree vs merkle list of merkle trees)

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.

A block is a container data structure that aggregates transactions for inclusion in the public ledger, the blockchain. The block is made of a header, containing metadata, followed by a long list of transactions that make up the bulk of its size.

A blockchain is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block a timestamp, and transaction data.

1. what problem/s are POW/POS trying to solve? discuss/compare (byzantine fault tolerance, reaching a single consensus on a p2p network)

Byzantine Fault Tolerance is a computer system's ability to continue operating even if some of its nodes fail or act maliciously.

The term comes from a hypothetical called the Byzantine Generals Problem.

With any computer system that has multiple nodes, each node could be considered a general. The system's Byzantine Fault Tolerance refers to whether it can keep working even when some nodes go down or intentionally try to deceive it.

With proof-of-stake (POS), cryptocurrency owners validate block transactions based on the number of coins a validator stakes. Proof-of-stake (POS) was created as an alternative to Proof-of-work (POW), the original consensus mechanism used to validate a blockchain and add new blocks.

With proof-of-stake (POS), cryptocurrency owners validate block transactions based on the number of coins a validator stakes.

Proof-of-stake (POS) was created as an alternative to Proof-of-work (POW), the original consensus mechanism used to validate a blockchain and add new blocks.

Proof-of-stake (POS) is seen as less risky in terms of the potential for an attack on the network, as it structures compensation in a way that makes an attack less advantageous.

Proof of work (PoW) is a decentralized consensus mechanism that requires members of a network to expend effort solving an arbitrary mathematical puzzle to prevent anybody from gaming the system.

Proof of work is used widely in cryptocurrency mining, for validating transactions and mining new tokens.

Due to proof of work, Bitcoin and other cryptocurrency transactions can be processed peer-to-peer in a secure manner without the need for a trusted third party.

Proof of work at scale requires huge amounts of energy, which only increases as more miners join the network.

Proof of Stake (POS) was one of several novel consensus mechanisms created as an alternative to proof of work.