CRYPTOMASTER

WORKBOOK2

2023 VOLITION LABS

SESSION 2

01 STARTING AS A BITCOIN OPERATOR

To start as a Bitcoin or other cryptocurrency operator, the operator must receiving Bitcoin to their Bitcoin address. Bitcoin is received either as a mining block award via a coinbase transaction or as Bitcoin sent from another Bitcoin wallet.

To receive Bitcoin to the wallet the operator prompts the wallet to produce a private key from a range of 2^256 possible permutations. It is this degree of entropy that protects assailants from being able to brute force (guess) the private key.

From the private key a public address is cryptographically produced. This is presented to the sender to receive an amount of crypto.

The private key must always be kept secret from any other party. However the Bitcoin public address can be freely distributed without fear of compromizing the account. Only by presenting the private key can an operator command the blockchain to transfer assets to another address. This is called asymmetric public-private key cryptography.

There are examples of artists putting their Bitcoin address within their street art in order to receive Bitcoin tips. Although the address is highly public, there is no way for a third party to access the account.

SESSION 2

02 TRANSACTIONS

When a transaction is sent, the sender's wallet constructs the transaction, containing information regarding the transaction amount and fee. It also contains a certificate of authenticity which is cryptographically created by hashing the private key with the transaction data and the public address.

By sending the certificate in this way the sender is able to demonstrate cryptographically to the network that they are in possession of the private key without revealing the private key to either the network or the recipient.

This cryptographic protocol is called elliptic curve digital signature algorithm or ECDSA.

03 THE MEMPOOL

In the fiat system there is the need for the bank to centrally apply checks and balances to the transactions in order to maintain a trusted system.

Equally, Bitcoin transactions sent to the network do not automatically get recorded and approved on the blockchain. First they are checked for authenticity.

On being sent, transactions first appear in waiting room held in the collective network memory called the memory pool or mempool. From here they are packaged into 1mb blocks (data folders) with the transactions offering the highest transaction fees given priority over transactions with lower transaction fees.

SESSION 2

04 TIMESTAMPING OF TRANSACTIONS

The timestamping or verification process in blockchain is conducted by the mining nodes operating in incentivized competition (gamification) against each other to win block rewards.

The first miner to find the Nonce (the key) to unlock the block is rewarded with the native currency, in this case, Bitcoin. This mechanism, known as the Coinbase transaction, also serves as the method of currency issuance.

Once transactions are timestamped into blocks on the blockchain they are immutably recorded on the blockchain ledger. With each subsequent block that it is mined, the greater the level of immutability. Hence transactions are not usually considered completed until two subsequent blocks are mined.

05 TRANSACTION FEES

For transactions to be processed by the network fees much be attached. This is designed to prevent DOS attacks on the network as well as to add additional incentives for the miners. After 21m Bitcoin are mined, there will be no more mining rewards and miners will receive transaction fees only.

Miners select transactions to put into blocks according to the size of the fee attached to the transaction. Once a 1bm block is full of transaction data, no more transactions can be processed into that block and the abandoned transactions must wait in the Mempool (memory pool) for inclusion in a later block.

If the fee is too low it is possible that the transaction will not be processed into a block and instead become stuck in the Mempool for several days before being returned to the sender's wallet.

SESSION 2

If confirmation speed is a priority, a competitive transaction fee should be included. This is calculated by monitoring the level of traffic on the network and identifying the current competitive fee level. Wallet applications provide this service to the user and make an automatic recommendation regarding the fee size.

Once a block is confirmed, the transactions will appear on the blockchain to be audited via a blockchain explorer.

Unless a majority of the Bitcoin nodes conspire to change that transaction data (a 51% attack), which they are strongly incentivized not to do, that transaction data will remain timestamped on the blockchain for ever. With each subsequent blocked mined, the computational difficulty of changing the transaction data becomes exponentially difficult. This is why wallet applications require transactions to appear in at least 3 blocks before being considered 'confirmed.

06 TOKENOMICS

Tokenomics refers to the science of token economics within crypto currencies, including elements such as the method of currency issuance and incentivization architecture.

In Bitcoin the mechanism of mining also serves as the method of currency issuance. While many cryptocurrencies schedule an initial coin offering (ICO) to create an upfront supply of tokens as part of a fundraising initiative, Bitcoins are only produced on average every ten minutes via a mining reward (coinbase transaction) to the successful miner.

Compare this to fiat banks where money is created via the issuance of national loans to governments, thereby creating an instant debt liability.

The currency issuance protocol set by Bitcoin is capped at 21m Bitcoin. To date over 19 Bitcoin have been issued as mining rewards and are currently in circulation.

However due to the Bitcoin mining reward 'halving' event every 210000 blocks (roughly 4 years), the number of Bitcoin issued logarithmically decreases, resulting in all Bitcoin being mined by 2140.

After this point transaction fees will be the only reward given to miners.

07 MINING

Mining is the gamification process that incentivizes node operators to lend their computer processing power to secure the network. Bitcoin does not exist outside of nodes, therefore it incentivizes node operators to be Bitcoin host nodes by rewarding them with Bitcoin.

Mining nodes compete to find the NONCE (number only once). This is a number which, when hashed together with the block header produces a block hash with a specificed amount of zeros. The number of zeros the miners are required to find is dictated algorithmically by the difficulty rating which is dictated by the amount of hash power on the network at any one time.

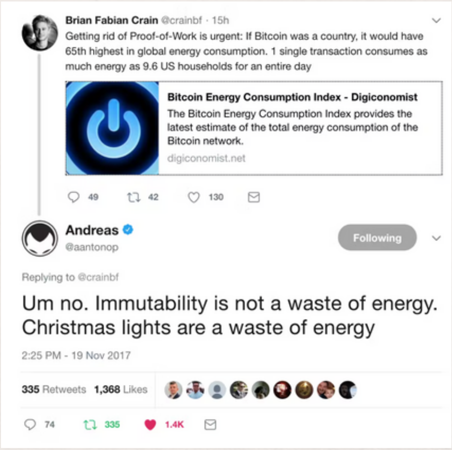
When the genesis block was mined the difficulty rating was 1. Now the difficulty rating is several billion. As the amount of hash power (the ability for nodes to compute hashes per second) on the network increases, so the need for CPU power increases, requiring participants to either build increasingly large mining farms or participate in mining pools that collectivize the hash rate and mining dividends.

SESSION 2

08 BITCOIN ENERGY CONSUPTION

According to the Cambridge Center for Alternative Finance (CCAF), Bitcoin currently consumes around **110 Terawatt Hours per year** — 0.55% of global electricity production, or roughly equivalent to the annual energy draw of small countries like Malaysia or Sweden.

This has led to criticism of Bitcoin by green campaigners. However it should be noted that 70% of Bitcoin energy use is from renewable sources. Furthermore, when considering Bitcoin's environmental footprint, the relative use of energy by global fiat monetary system should also be considered.



Brian Fabian Crain @crainbf · 15h

Getting rid of Proof-of-Work is urgent: If Bitcoin was a country, it would have 65th highest in global energy consumption. 1 single transaction consumes as much energy as 9.6 US households for an entire day

Bitcoin Energy Consumption Index - Digiconomist

The Bitcoin Energy Consumption Index provides the latest estimate of the total energy consumption of the Bitcoin network.

digiconomist.net

49 42 130

Andreas @aantonop

Following

Replying to @crainbf

Um no. Immutability is not a waste of energy. Christmas lights are a waste of energy

2:25 PM - 19 Nov 2017

335 Retweets 1,368 Likes

74 335 1.4K

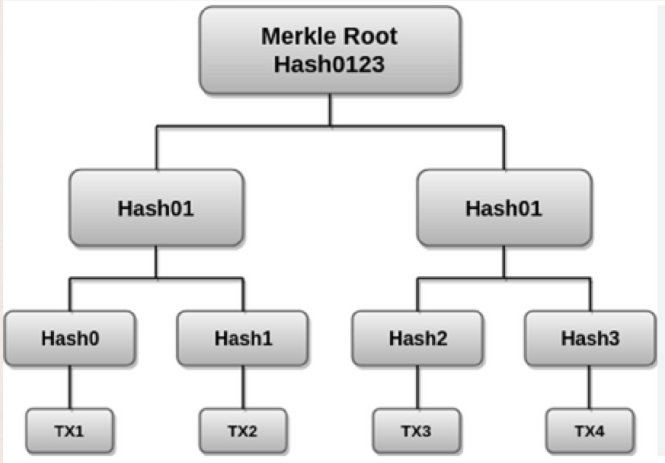
https://qz.com/1988503/bitcoin-miners-and-fracking-companies-are-working-together
https://hackernoon.com/the-bitcoin-vs-visa-electricity-consumption-fallacy-8cf194987a50

09 HASHING

Bitcoin uses a hashing function called SHA256. This is an algorithm that outputs any length of data input into a data string of 256 bits, expressed as base64 hash of 64 bytes.

Algorithmic hashing comprises a significant part of the bitcoin data structure. The Bitcoin database is a chain of blocks that are concatenated via a series of linked hashes. Transaction data is hashed into a transaction hash. Transaction hashes are hashed together via a Merkle tree to form a Merkle root. The Merkle root is hashed along with the block header to form a block hash.

Each block header hash also contains the block hash from the previous block. In this way, if any information is changed at any previous point in the blockchain by a malicious node, all subsequent block header hashes will be instantly altered. This enables other nodes in the network to identify and reject nodes acting maliciously without large computational requirements. This process ensures the immutable nature of the blockchain.



A Merkle tree is used in Bitcoin as part of its hashed data architecture.

10 ATOMIC STRUCTURE

The hashing structure creates a number of dynamic bonds in a similar way as gold in that it has an immutable atomic structure that is extremely difficult, if not impossible, to reproduce but easy to verify.

In this way Bitcoin can be seen as a digital form of gold. While it is impossible to alter in terms of its structure, its authenticity can be easily and quickly verified.