Dr. Philippe J.S. De Brouwer

Applications of Quantum Computers in Banking

Strategic Innovation and Artificial Intelligence - Velvet Edition

May 13, 2024

Table of Contents

Contents

1 The Bitcoin Blockchain

The Blockchain

- is a database of transactions secured by encryption and validated by peers.
- The blockchain is not stored on multiple computers and systems within a network (these systems are called nodes).
- Every node has a copy of the blockchain, and every copy is updated whenever there is a validated change to the blockchain.
- The blockchain consists of blocks, which store data about transactions, previous blocks, addresses, and the code that executes the transactions and runs the blockchain.

The Blocks

When a block on the blockchain is opened, the blockchain creates the block hash, a 256-bit number that encodes the following information:

- The block version: the Bitcoin client version
- The previous block's hash: the hash of the block before the current one
- The coinbase transaction: the first transaction in the block, issuing the bitcoin reward
- The block height number: how far away numerically the block is from the first block
- Merkelroot: A 256-bit number that stores the information about all previous blocks
- Timestamp: the time and date the block was opened
- The target in bits: the network target
- The nonce: a randomly-generated 32-bit number

Queued transactions are entered into the block, the block is closed, and the blockchain creates the hash. Each block contains information from the previous blocks, so the blockchain cannot be altered because each block is "chained" to the one before it. Blocks are validated and opened by a process called mining.

Bitcoin Mining

Definition
Mining is validating transactions and creating a new block on the blockchain.

- Miners try to find a number that matches the block hash. The programs randomly generate a hash and try to match the block hash, using the nonce as the variable number, increasing it every time a guess is made. The number of hashes a miner can produce per second is its hash rate.
- The miners who first solves the hash receives the bitcoin reward,
- A new block is created, and the process repeats for the next group of transactions.

Mining Difficulty

Difficulty
There is no way of predicting what nonce will work, so mining is randomly trying all possible numbers. The difficulty is then the average number of tries it takes to verify the hash.

Notes

- Bitcoin's protocol requires a longer string of leading zeroes depending on the number of miners, adjusting the difficulty to hit a rate of one new block every 10 minutes.
- The difficulty has been increasing since Bitcoin was introduced, reaching tens of trillions of attempts these days.
- Mining is expensive and competition is intense. This is why mining farms and mining pools were created.
- Mining uses ca. 0.55

Halving of Rewards

- At start, the mining reward was 50 BTC for solving the hash.
- Every four years, or 210,000 blocks, the reward is cut in half. (So, rewards were cut to 25 in 2012, 12.5 in 2016, and 6.25 in 2020. The next halving is expected to occur in 2024 when the reward will reduce to 3.125, followed by a reduction to 1.5625 around 2028)

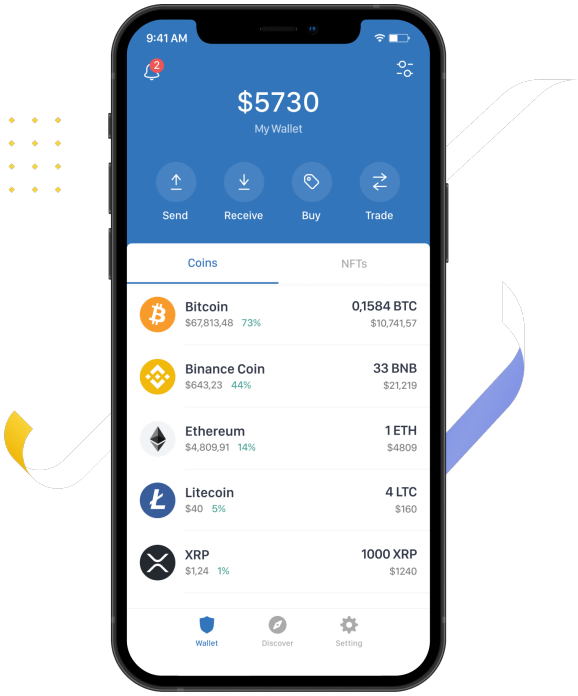

Figure 1: The wallet app of `trustwallet.com`.

- The last bitcoin is expected to be mined somewhere around 2140. All 21 million bitcoins will have been mined at that time, and miners will depend solely on fees to maintain the network.

Keys and Wallets

- Ownership of BTC is in the block-chain
- To view balance, use a wallet and keys

Keys

- When bitcoin is assigned to an owner via a transaction on the blockchain, that owner receives a number, their **private key**.
- The wallet has a public address—called -
- the **public key** -
- that can be used to send BTC

Note
A bitcoin is data with ownership assigned. Data ownership is transferred when transactions are made.

Wallets

- A wallet is a software application used to view your balance and send or receive bitcoin.
- The wallet interfaces with the blockchain network and locates your bitcoin for you. The blockchain is a ledger with portions of bitcoin stored on it.
- The transactions are are scattered all over the blockchain. Your wallet application finds all previous transactions, totals the amount, and displays it.

Custodial Wallets
A trusted entity, like an exchange, holds your keys for you. eg. Coinbase

Noncustodial wallets
The user takes responsibility for securing the keys, such as in your wallet application on your mobile phone.

Storage of the Keys

Hot Storage
Storing keys in an application connected to the internet is referred to as hot storage. However, hot storage is the vulnerability most often exploited.

Cold storage
is any method that is not connected to the internet. e.g a removable USB drive or a piece of paper with your keys written on it (this is called a paper wallet).

Deep cold storage
is any cold storage method that is secured somewhere that requires additional steps to access the keys beyond removing the USB drive from your desk drawer and plugging it in. e.g. a personal safe

Bitcoin Transactions

- To send a coin, you enter the receiver's address in your wallet application, enter your private key, and agree to the transaction fee.
- press "send"
- The receiver waits for the transaction to be verified by the mining network, which can take up to 30 minutes because transactions wait in a mining queue called the "mempool."

2 Other Blockchain applications

A Blockchain is

A Blockchain is
a way to securely transact in an environment that lacks trust

A Blockhain is
a de-centralized register where security built in

Banks

- **Payments**: less verification needed, speed(?), cost(?)
- **de-centralised ledgers**: settlement could be faster, transaction matching is part of the payment, etc.
- **Clearing and Settlement**: drop in replacement for SWIFT(?)
- **other assets**: bonds, stocks, options, etc.
- **IPOs and raising of capital**
- **Loans**: bonds on distributed ledger, credit bureau information, home ownership and mortgage registers, etc.
- **Trade Finance**: letters of credit, invoices, bills, etc.
- **Identity verification**: secure re-use of trusted verification (e.g. Zero Knowledge Proof = proof that you know x without disclosing x) + users can decide who to share ID proof with
- **as an asset** ... for hedge funds(?)
- **P2P transfers**

Crypto Currencies

Question:

How many crypto currencies are there?

.....

.....

.....

.....

Source: https://coinmarketcap.com/all/views/all/

Crypto Currencies: definitions

Ponzi scheme

```
_noun_

a form of fraud in which belief in the success of a non-existent
enterprise is fostered by the payment of quick returns to the first
investors from money invested by later investors.
```

3 Conclusions

Key Takeways

- A **blockchain is a secured distributed ledger**, a database shared between multiple users who can make changes.
- **Mining** is the process of validating transactions -
- miners are rewarded in bitcoin.
- Access your bitcoin using a **wallet**, a **public key**, and **private keys**.
- Bitcoin users pay small transaction fees in bitcoin to miners for transaction processing.
- The Bitcoin blockchain has **(not yet) been compromised**.
- The real **opportunities** arise where a centralized ledger is not obvious