Blockchain Overview

Introduction

"Blockchain" is the generic term for BitCoin, Etherium, et. al.

A blockchain is a chain (using unique hashes as links) of blocks that contain one or more financial transactions. The blockchain is simply a public "ledger" that holds transactions and makes them immutable. Blockchain is not restricted to being a ledger financial transactions, but BitCoin specifically devotes itself to financial transactions.

The BitCoin network is essentially a peer-to-peer (P2P) network.

"Miners" are "big" nodes on the BitCoin network. "Miner" nodes are willing to do the heavy lifting and compete with each other to export a block of transactions. In BitCoin, there is a "prize" for the first miner to solve the puzzle and export its block.

BitCoin is an "unpermissioned" network, meaning that any node can join the network without permission. BitCoin needs many miners, spread across the globe, to do the real work of verifying and publishing transactions and verifying blocks or transactions published by other miners.

BitCoin uses PoW (proof of work) to solve a puzzle. The first miner to solve the puzzle gets to publish its block. A winning block contains only the transactions that the winner has chosen. Other competitors might choose a different set of transactions from the "mempool". BitCoin dynamically adjusts so that solving a puzzle takes about 10 minutes.

If a transaction sits at the bottom of the pool for <*some number of*> days, it might be dropped and never appear in a winning block. I.E. some transactions may <u>never</u> be processed ("dust").

Losers, miners, in the competition still perform computations - verifying the contents of each transaction in a published block and complaining, if something looks fishy.

PoW wastes computing resources (and electricity). Miners tend to set up their operations, geographically, in places that provide cheap electricity and cool climates (eschewing the need for air conditioning), such as northern Quebec in Canada (lots of cheap hydro, cool climate).

BitCoin is written in open-sourced C++.

The original intent of BitCoin was to use as many distributed nodes as possible, distributed over the whole world. The number of nodes can change over time (e.g. new nodes joining and some existing nodes crashing). This is called "unpermissioned" — a node does not need permission to join the network. In general, we don't know if the nodes can be trusted or if they might be fakers. The main problem in this case is BFT (Byzantine Fault Tolerance). The mathematics makes assumptions about how many nodes are fakers, and if a certain threshold of trusted nodes is attained, then the mathematics makes guarantees about the trustability of the whole network.

IBM, Linux and banks flog a "permissioned" kind of blockchain (HyperLedger). In this version, the nodes are all known and their count is determinate, i.e. no one can join the HyperLedger without permission. This is very similar to what banks (and VISA, et al) already do. It is not clear to me that this is true to the original intent of blockchain. It seems to be a marketing trick to capitalize on the buzz-word "blockchain".

It is not clear where BitCoin originated. Supposedly, "Satoshi Nakomoto" invented and open-sourced BitCoin. Who Satoshi is, is a secret. This secrecy could mean many things — that the originator is an individual or a group concerned with freedom of money and transactions, or a government group intent on removing paper money from circulation, or …

Race conditions, caused by timing and the non-locality of the mining nodes, is handled by the “longest chain is accepted” strategy, which settles out after <*some number of*> blocks have been verified (about 6-ish).

Along with BFT, so-called “Sybil attacks” are culprits that blockchains guard against. “Sybil attacks” are nodes that try to cheat the system by cloning several nodes on a single machine (multiple “personalities” on a single machine - similar to the film Sybil), and try to collude to gain control of transactions (i.e. making them pay out to the colluders). The front-line, easiest, defence against Sybil attacks is to make the PoW puzzles so onerous that only a single cpu with full power can solve the puzzle in about 10 minutes. If a single node is split into a bunch of time-shared nodes, the split, faked, nodes can never perform the full work (puzzle breaking) in less time than a full node, and a Sybil (fake) node can almost never win publishing rights for a block.

By unconscious consensus, papers that discuss blockchain algorithms tend to use the names “Alice” and “Bob” as blockchain transaction participants.

BitCoin uses a puzzle that consists of hashing something (e.g. the proposed block of transactions plus a kludge factor — the “nonce”) until the hashcode has a requisite number of zero’s at its front. This kind of puzzle can only be solved by brute force, and it takes a random amount of time to solve. On the other hand, once solved (and published) the hashcode can be easily (and cheaply) verified, hence, all other nodes can verify the puzzle solution, to verify that the winning node did, indeed win.

The winning miner node gets to create a certain amount of BitCoins and to insert them into the published block (payable to the winning node). That is how new BitCoins come into existence. The amount of new BitCoins granted to the winning miner, drops over time, and at some point (a few years away, from 2019) the grant amount will drop to zero, hence, the BitCoin supply has an upper limit (which might affect future quantitative easing using BitCoin).

Each transaction gives a fee to the winner, who also collects the BitCoin grant (prize). When the grant drops to zero, winning miners will only receive transaction fees.

Users (human) of the BitCoin network own a “wallet” that holds one-half of a public/private key (they hold the private, or “secret” key). The wallet generates public keys which are used in transactions as destination addresses to which BitCoins (or fractions of BitCoins) can be sent.

All transactions are visible forever in the blockchain. Each block contains a hashcode to the previous block. If any transaction in the chain is tinkered with, the whole chain will not verify.

Using multiple public keys can make the chain harder to read, but ultimately, with enough horse-power, the chain can be unravelled, traced and viewed. In a BitCoin-only world, a black market or “cash deals” cannot exist.

BitCoin also defines light weight nodes. Light weight nodes (e.g. smart phones) can participate in the network (generating transactions, holding wallets), but don’t do the heavy lifting (mining).

BitCoin uses Merkle trees to reduce memory usage - not every node needs to hold the complete chain at all times. Merkle trees are a subset of ADS (Authenticated Data Structures). Validation nodes, still, must visit and verify each published block.

The “value” of BitCoins is purely speculative and changes over time according to market whims.

Improvements to BitCoin are the subject of heated research. Improvements include: improving the transaction rate (BitCoin publishes a block of verified transactions every 10 minutes (at best 2700 transactions https://cryptoslate.com/bitcoin-transactions-per-block-at-all-time-highs/), whereas permissioned networks, e.g. VISA, process 1,000’s of transactions per second), scaling improvements such as CoSi and sharding (BitCoin slows down as the number of nodes/miners increases), better (cheaper) anti-cheating methods (e.g. PoS - proof of stake ; Randhound protocols), alternative data structures (e.g. Etherium), “smart contracts” (e.g. Etherium), etc.

There are 100’s, if not 1,000’s, of digital currencies in existence. Which currency will win market share? Currently, BitCoin has the most market share, Etherium is a far second.

We already know that first-to-market holds a distinct advantage - e.g. Intel won the cpu battle in the face of, later, “better” cpu’s (Motorola, National Semiconductor), VHS won the battle, over Beta, etc.

Permissioned networks are, currently, massively faster than unpermissioned networks.

Experiments / product offerings are being made, using non-monetary transactions, e.g. storing digital handles to physical objects (e.g. deeds, etc.) in the immutable ledger.

Surprises

BitCoin doe not provide anonymity.

BitCoin does NOT guarantee that every transaction will be processed. Transactions are dropped from the “mempool” if they sit at the bottom for <*some*> days.

Transactions cost money. Miners can grab and commit transactions based on fees plus mining rewards.

Pederson commitments can provide anonymity, but are very expensive (time-wise) to compute and anonymity must start at the beginning of time (at the genesis, beginning, of the blockchain).

All BitCoin transactions are fully consumed. If you want to receive “change” back from a transaction, then you must split the transaction into two parts - one that goes to the vendor and one that goes to yourself.

A miner that wins publishing rights for a block, gets to keep any "leftovers" (i.e. amounts that remain after the transaction has been processed. All transactions are fully consumed, some transactions may not sum to zero, the unclaimed difference goes to the winning miner).

Declaration of a winning miner is done in a as-random a method as possible (determined by the puzzle).

The winning miner collects all the transaction fees from the winning block, all leftovers from the winning block and the mining prize (as it stands at that moment in time).

A losing miner gets nothing. One must amortize the random, non-frequent, wins against frequent losses.