Blockchain: Utopia or U-turn?
Glossary

Block

Block are synonymous with digital pages in a ledger, also known as a record keeping book. These files store unalterable data related to the network. A block is an archive in the blockchain, which contains and verifies several pending transactions. A new block containing transactions is attached to the blockchain through mining approximately every ten minutes (per average).

Block Height

The block height is the number of individual blocks in a blockchain. The first block is Height 0. It is also known as the Genesis Block.

Blockchain

Is a distributed ledger that records all the transactions and smart contracts for a cryptocurrency or platform. The blockchain is replicated on several thousand nodes all around the world. A blockchain is a public archive of BItcoin transactions, placed in chronological order. The blockchain is distributed among all Bitcoin users and it is used so as to verify the permanence of Bitcoin transactions and prevent double spending.

Bitcoin

Bitcoin is a branded cryptocurrency that most people are familiar with. This cryptocurrency works as a decentralized global peer to peer network with no issuer or acquirer. This means that no single entity can control it, as a central authority is bypassed. The coin is open source, meaning it has wallet and transaction verification. And best part - it can be used by anyone with a smartphone or a computer. Bitcoin was created by Satoshi Nakamoto in 2008 as the first application of the blockchain and as the first cryptocurrency. It is still the dominant cryptocurrency now. The supply of bitcoins is fixed at 21 million. That’s the market cap on all bitcoins.

Cypherpunk

Cypherpunk is any activist advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change. Originally communicating through the Cypherpunks electronic mailing list, informal groups aimed to achieve privacy and security through proactive use of cryptography. Cypherpunks have been engaged in an active movement since the late 1980s.

Charlie Lee

Charlie Lee is the creator of Litecoin, and formerly Coinbase's Director of Engineering. Although he is the creator of Litecoin, Lee remains focused on a number of Bitcoin-specific projects as well. Prior to Lee's forays into the world of cryptocurrency, he held various engineering positions at companies like Google and Guidewire Software.

David Lee Chaum
David Lee Chaum is an American computer scientist and cryptographer. He is famous for developing ecash, an electronic cash application that aims to preserve a user's anonymity. He has also invented many cryptographic protocols and founded DigiCash, an electronic money corporation. His 1981 paper, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", laid the groundwork for the field of anonymous communications research.

Cryptocurrency
Is a decentralized digital currency that can be used for goods, services, and transfer of assets. The first cryptocurrency was Bitcoin. It went live in January 2009.

Cryptocurrency Exchange
Cryptocurrency Exchange are websites or services that let you exchange digital cryptoassets and cryptocurrencies between one another or exchange fiat currencies such as the US dollar for cryptoassets. Two of the most prominent examples of these exchanges are Coinbase and Binance.

Cryptocurrency Wallets
Cryptocurrency Wallets are ways of storing your private and public keys to your cryptoassets. A wallet is a safe you can access to then get your keys. In general, a Bitcoin Wallet is the equivalent of a physical wallet in the Bitcoin network. The wallet actually contains your own private key(s) that allow(s) you to spend the bitcoins that are distributed in a specific block chain. Each Bitcoin wallet can display the total balance of the bitcoins it controls; moreover, it allows the user to make a payment to a natural person – exactly as it happens with a physical wallet. This differs from credits cards, where you are charged by the vendor.

Decentralization
Is a measure of how much authority is held by a central holder. You can argue that blockchains are naturally more decentralized than other methods of distributing data because there is (at least in public chains) no gatekeeper on who can join: as long as you have the computing power, you can participate in the blockchain.

Digital Signature
Is a digital code generated by public key encryption that is attached to an electronically transmitted document to verify its contents and the sender's identity.
A digital (encrypted) signature is a mathematical device that permits the user a proof-of stake (PoS). In the case of Bitcoin, a Bitcoin wallet and its private keys are connected through some sort of mathematical witchcraft. Once a Bitcoin software signs a transaction through the appropriate private key, the whole network can witness that the signature coincides with the bitcoins spent. However, there is absolutely no way for someone to guess your private key and steal your hard-earned bitcoins.

Distributed ledger

Distributed ledger is an analogy often made about blockchains. Instead of a centralized bank ledger, blockchains offer the promise of distributing balances throughout a network of computer servers.

Ethereum
Ethereum is a blockchain-based decentralised platform for apps that run smart contracts, and is aimed at solving issues associated with censorship, fraud and third party interference.

Escrow
Escrow is a financial arrangement where a third party holds and regulates payment of the funds required for two parties involved in a given transaction. It helps make transactions more secure by keeping the payment in a secure escrow account which is only released when all of the terms of an agreement are met as overseen by the escrow company.

James Dalton Bell
James Dalton Bell is an American crypto-anarchist who created the idea of arranging for anonymously sponsored assassination payments via the Internet, which he called "assassination politics". In April 1995, Bell authored the first part of a 10-part essay called "Assassination Politics", which described an elaborate assassination market in which anonymous benefactors could securely order the killings of government officials or others who are violating citizens' rights. In 2001, *Wired* called Bell "one of the Internet's most famous essayists" and "the world's most notorious crypto-convict".

Fiat
Fiat currency is regular national currency like the U.S. dollar, British pound, and the euro. It is declared legal tender by a government but is not backed by physical assets like gold.

Fork
Forks create an alternate version of the blockchain, leaving two blockchains to run simultaneously on different parts of the network.

Genesis Block
Is the first or first few blocks of a blockchain.

Hodl
Hodl is a cryptocurrency meme for holding on to your crypto assets rather than selling. The meme was born in December 2013 when a user who'd drunk one too many beverages made a typo on a popular Bitcoin forum. You can still see the original thread on bitcointalk.org.

ICO or Initial Coin Offering
As cryptocurrencies grow in popularity, an increasing number of start-ups launch coins. Each of them promises to fix, address, or improve a particular aspect of the crypto landscape. These new coins are made publicly available via ICOs (initial coin offerings). They are like the crypto version of a stock market IPO.

Mining
Because of the cryptographic nature of cryptocurrencies, verifying transactions requires an enormous amount of computing power and specialized hardware. In exchange for the computing power, people who solve (and thus, authorize) a transaction receive some cryptocurrency for doing so. This process is called mining.

Mooning
In 2017, coins would explode in price seemingly overnight. The entire sector's market cap went from $15 billion in January to $600 billion in December. Ripple was the biggest winner; its price increased 28,963 percent over the 12 months. For comparison, the S&P 500 went up by 19.4 percent. The phenomenon of massive gains by a single coin is known as mooning.

Node
Node is a computing device on the blockchain. It is responsible for verifying transactions and keeping the distributed ledger up-to-date.

Peer to Peer
Peer to Peer or (P2P) refers to the decentralized interactions between two parties or more in a highly-interconnected network. Participants of a P2P network deal directly with each other through a single mediation point. Peer-to-peer connection refers to systems that function as an organized collective, allowing each user to directly interact with others. In the case of Bitcoin, the network is built in a way that permits each user to transmit other users' transactions. What is more, no bank has to be included as a third party.

Pretty Good Privacy (**PGP**)
Pretty Good Privacy is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. Phil Zimmermann developed PGP in 1991.

Proof-of-stake
Proof-of-stake pushes people who own a selection of a blockchain's tokens to make decisions on validating the chain. In practice, it's a much less energy-intensive practice than mining.

Proof-of-work
Proof-of-work is a system where blocks of transaction data on the blockchain are mined and validated by specialized computers who earn a reward for solving specific math equations.

Public/Private Keys
Keys are your way to access crypto balances and to send and receive value or data in cryptocurrency. Your public key is like your email address. It's what allows other people to send you funds. You can share your public key with the general public.

Satoshi Nakamoto
is the name used by the unknown person or people who developed bitcoin, authored the bitcoin white paper, and created and deployed bitcoin's original reference implementation. As part of the implementation, they also devised the first blockchain database. In the process, they were the first to solve the double-spending problem for digital currency using a peer-to-peer network. They were active in the development of bitcoin up until December 2010.

Smart Contracts
In addition to the cryptocurrencies (a.k.a. tokens or coins), some blockchains also support smart contracts. The most prominent smart contract network is Ethereum. Smart contracts allow non-currency assets to exchange hands on the blockchain without the need for a middleman. Assets could include membership records, insurances, or even real estate.

Nick Szabo
Nick Szabo is a blockchain and cryptocurrency pioneer. Szabo is widely regarded as the inventor of the concept of smart contracts, which are now a fundamental feature of cryptocurrencies. Szabo also is the creator of "bit gold", a decentralized precursor to bitcoin which informed the initial construction of Bitcoin's architecture.

Timothy C. May
Timothy C. May better known as **Tim May** (December 21, 1951 – December 13, 2018) was an American technical and political writer, and was an electronic engineer and senior scientist at Intel in the company's early history. May was a founding member of, and had been one of the most voluminous contributors to, the Cypherpunks electronic mailing list. He wrote extensively on cryptography and privacy from the 1990s through 2003.

Tokens
A token is a programmable digital asset with its own codebase that resides on an already existing block chain. Tokens are used to help facilitate the creation of decentralized applications.

Vitalik Buterin
Is the creator of Ethereum, the blockchain platform that acts as a world computer for decentralized applications. Its cryptocurrency, Ether, has seen its value skyrocket in 2017 (Ethereum's market cap is nearly $30 billion). He cofounded Bitcoin Magazine and now leads Ethereum, working on upgrades to its protocol.

Curated by: Voltnoi Brege & Quetempo