The Blockchain

At the center of the Bitcoin network is a decentralized ledger that contains the balance of every Bitcoin user. Bitcoin identifies users by large strings of letters and numbers such as "38eUHrPStpgJK2Ej2dKJnqjq3dtiWHsf7B". The address is the **public part** of a public–private cryptographic key. The **private part of the key** is under the control of the user.

The blockchain is arguably the most important innovation introduced by Bitcoin. It is the missing link that makes distributed peer-to-peer digital currencies possible.

The blockchain is in essence a distributed database holding all the Bitcoin transactions since the beginning (January 3, 2009) and a method to secure this database. The blockchain keeps a secure list of all the transactions. However, there are relevant questions, such as whether a transaction output is spendable, that the blockchain does not answer directly. Software that uses the blockchain, like mining nodes or wallets, must parse the blockchain to extract the relevant information. This information extracted from the blockchain is usually fed to a database.

The blockchain uses proof-of-work to secure the distributed database.

This means the blockchain is secured against tamper attempts by the computational power that has been applied to create it. An attacker wishing to change the blockchain would have to apply a computational power equivalent to all the computational power spent from that point in time to the present. Furthermore, the attacker would have to outrun the legitimate Bitcoin network, which keeps adding entries to the distributed database. In other words, it would have to catch up, computationally speaking, with the legitimate network to change the information in the database. Attacks to the blockchain will be covered.

The blockchain is an ever-growing chain of blocks. Each block contains a group of new transactions and a link to the previous block in the chain. New transactions in the network are collected into a block which is appended to the blockchain. Note that old transactions are still in the blockchain: old blocks are never removed from the blockchain, thus the blockchain can only increase in length.

The miner who solves the hashing problem uses the coinbase to pay the block reward to herself. Therefore, solving the partial hash inversion problem is called mining. All miners in the network compete to mine blocks. The hash rate of a miner is her computational power, measured in hashes/second. The network hash rate is the total hash rate of all the miners in the network, and it stands at around 30,000 TH/s at the time of writing. Mining a block can be compared to a lottery, where the chances of a single miner are proportional to her share of the network hash rate.

Exchanges

Exchanges allow users to convert bitcoins (and other cryptocurrencies) to fiat money. Some exchanges allow the conversion of different cryptocurrencies, such as between bitcoin and other alt-coins.

Exchanges admit different types of orders such as limit orders or market orders. The orders are gathered in an order book that is run through an order matching algorithm. Exchanges collect fees from both parties in the trade. Most exchanges operate continuously, on a 24/7 schedule.

Trade shares

You now know that bitcoins behave like usual shares or currencies. It means you can apply all the powerful methods of technical analysis — that's the collection of tools that was developed for professional traders and have made many of them astonishingly rich. Of course, you need to be smart (and, if you are reading this book, you are!) to outsmart the market and the brave. And, we must add the usual disclaimer: only invest money that you can afford to miss. Never invest borrowed money as you might end in deep trouble otherwise.

What is the idea of technical analysis in a nutshell? —It is very simple. You can gain much more for your investment if you do not just sit and wait, but rather use the cyclic character of price evolution and sell your stock (here bitcoins) when the price is high and buy them again when the price is low. To do it properly, you need to determine the trend and find the right moments when the trend is reversed.

Alternative coins

Alternative coins or alt-coins are cryptocurrencies that copy many of the features of Bitcoin. Most of the alt-coins are based on Bitcoin's source code with some changes. As Bitcoin's code is released under an open source license it is acceptable to take a copy of the code, modify it, and release a new cryptocurrency. Many developers have done exactly that, creating many alt-coins.

Development in Bitcoin has been conservative and value-preserving, focusing on avoiding the introduction of errors. On the other hand, altcoins often do not have the restrictions of a production system like Bitcoin, or the requirement of backward compatibility, allowing them to test new tweaks and features. However, Bitcoin can opt-in some of these features if the developers consider them worthy.

Some alt-coins that have proposed interesting changes, either technical or to the economics of Bitcoin. The focus of the chapter is to highlight these changes with respect to Bitcoin.

ETHEREUM

Ethereum is an open source second-generation distributed ledger with an associated Turing-complete platform, which can be used to build and distribute decentralized applications. Ethereum will create its own blockchain. As of the time of writing, the project is still being built, although the test network is up and running.

LITECOIN

Litecoin (LTC) is arguably the most successful alt-coin. It was released in 2011 and as of the time of writing had a market capitalization of roughly 5% of that of Bitcoin. It is sometimes referred to as "silver to Bitcoin's gold."

PEERCOIN

Peercoin (PPC) was introduced in 2012. Its main innovation is that it uses a hybrid proof-of-stake/proof-of-work system. In a proof-of-stake system new blocks are minted—analogous to mining—by holders of coins in proportion to how many coins they control. Proof-of-stake does not involve solving a partial hash inversion problem and thus requires minimal electricity consumption.

NAMECOIN

Namecoin (NMC) is both a crypto-currency and a decentralized key/value store. This decentralized key/value store is used to implement an alternative Domain Name System (DNS). The DNS is the piece of the internet infrastructure that enable human-readable addresses to be resolved to IP addresses. Users running a Namecoin node have a full copy of the key/value store and can access it at any time. Or some users might prefer to connect to a Name-coin node and query the node for specific information.

DOGECOIN

Dogecoin (DOGE) was introduced in 2013. Dogecoin is a straightforward fork of Litecoin. Its main innovation lies in its marketing strategy. It associates with the famous internet doge meme, transmitting a message of light-headedness and fun that will hopefully cater to a wider demographic than other cryptocurrencies.

Buy and Sell Bitcoin & other cryptocurrencies

First thing to consider when looking for the best bitcoin exchange is how safe it is. This boils down to asking: is it a trustworthy exchange providing transparent data of coins in cold storage (more on this later) and are customers happy? It's also good to lookout for which currency pairs are available: are you looking to trade bitcoin for USD, Euros, or other fiat currencies. The location usually gives an idea of what's on offer. However, the largest bitcoin sites usually have many options for buying bitcoin with government issued currency and altcoins.

The sheer complexity of researching where to trade bitcoin led me to make this blog. Although you should always do your own research before investing, I hope this helps. Below is the table of the best exchanges to buy bitcoin online. If you are new to cryptocurrency exchanges, then lookout for the 'beginner-friendly' column.

There are now many bitcoin exchanges you can choose from, and more flexibility in terms of payment options. Here are the best exchanges you can use to buy and sell bitcoins and other cryptocurrencies.

QuadrigaCX

The most convenient way to trade

Bitcoins with the same day funding & withdrawal. When it comes to Volume, QuadrigaCX is the fastest growing Bitcoin Exchange in Canada, and one of the fastest growing exchanges in the world. Our rapidly

increasing volume makes it easy to buy or sell Bitcoins at the best rate.

CoinBase

Visit CoinBase

One of the most reputable bitcoin exchanges available, Coinbase is popular among fans of the 'dollar cost averaging' method, where users can automate bitcoin purchase every week or month. It is a no-fuss platform for just bitcoin buying and selling.