CHAPTER 5

Blockchain and Cryptocurrencies

By now you have seen and read quite a bit about blockchain technology. However, I want to close off this book with some final concepts that you should know and understand. These will allow you to zoom into some important aspects when you look at the crypto-markets and see how they function. Several new financial instruments have been devised with the creation of cryptocurrencies and existing financial assets have found their way into the world of cryptocurrencies.

A Short History of Crypto-Markets

The history of cryptocurrencies and assets is strongly linked to the history of the blockchain technology itself, or at least it was in the beginning. Sadly, the reputation of the technology was tarnished when the markets crashed after the huge hype created in 2018-2019.¹ As we saw in Chapter 1, everything starts in October 2008, when an unknown individual called Satoshi Nakamoto released their whitepaper describing Bitcoin. The initial idea sparked both interest and skepticism and the first blockchain block ever, the Bitcoin genesis block, was released in January 2009. It was also in this month that the first transaction took place, between Satoshi Nakamoto and a developer named

¹https://docs.google.com/document/d/1cxEwTbfIWBg8n6uQYK4m3ITsKsebrqVYQ-Ps1fEcXBO/edit#heading=h.yt4uf141p1v4

© Stijn Van Hijfte 2020
S. Van Hijfte, Decoding Blockchain for Business,
https://doi.org/10.1007/978-1-4842-6137-8_5
Hal Finney. This was the beginning of the cryptocurrency world. In October 2009, there was a first valuation of Bitcoin with the New Liberty Standard, where $1 = 1,309 BTC. The first Bitcoin market, dwdollar, was established in February 2010. For the first time ever, other participants could buy and sell the cryptocurrency.

In May 2010, a notable milestone takes place in the Bitcoin world, still known to many enthusiasts and participants of the cryptocurrency world. Laslo Hanyecz spends about 10,000 BTC to buy a pizza from Papa John’s. It was the first real-world transaction where the cryptocurrency was used to buy something material. This height in perception would be crushed a couple of months later (August 2010) when first there was a hack that maliciously acted on a vulnerability in the Bitcoin network, leading to the generation of 182 billion Bitcoins. The value of the cryptocurrency is reduced to almost nothing. The perception of Bitcoin would undergo even more damage when there were more vulnerabilities discovered in September of that year, while in October there was a report suggesting that Bitcoin could be used for money laundering and financing terrorist activities. Still, in November of 2010, the market would reach a value of $1 million USD (at a valuation of $0.50/BTC).

In 2011, the first price surge of Bitcoin takes place, which leads to a valuation in June of $31/BTC (starting from parity in January). Fast forward to June 2013, when the market reaches a capitalization of $1 billion. It is also around this time that the first regulation is released by the U.S. Financial Crimes Enforcement Network. A couple of months later, another major theft took place, followed by another security breach, crushing the value of Bitcoin to $0.01. In August of the same year, U.S. federal judge Mazzant first states that Bitcoin can be used as a currency to be exchanged for goods and services. At the same time, Bloomberg starts with the integration of Bitcoin data in its portal, increasing the acceptance of the cryptocurrency.

The first major divide occurs in November-December, 2013. While the U.S. Senate starts their first hearings on Bitcoin, the Federal Reserve chairman, Ben Bernanke, gives his blessing and support for the network. In China, on the other hand, the first ban is imposed on financial institutions from handling Bitcoin transactions. In 2014, overstock.com becomes the first large retailer to accept Bitcoin payments, while Elliptic launched the first insured Bitcoin storage service. Later that year, the Silk Road is closed and its Bitcoins (29,000) were seized.  

---

2Silkroad started to accept Bitcoins as a method of payment a couple of months later. It is now clear for everyone that this was a drug trafficking network (among other things).
3Allinvain had 25,000 BTC stolen from his wallet.
4www.forbes.com/sites/kashmirhill/2013/08/07/federal-judge-rules-bitcoin-is-real-money/
5www.cityam.com/bloomberg-confirms-it-internally-testing-bitcoin-ticker/
6www.bloomberg.com/news/articles/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions
are being sold by the U.S. government.\textsuperscript{7} In New Jersey the first regulated Bitcoin investment fund (GABI) received its certification.\textsuperscript{8} By the end of the year, TeraExchange starts with the first Bitcoin-derived transactions on a regulated exchange. This meant further integration of the currency in the standard ways of working and acceptance by the main financial institutions.

In 2015, the New York Stock Exchange becomes one of the investors behind Coinbase, the UK Treasury starts a call for information on digital currency, and Barclays starts to accept Bitcoin as well. The next year, the cabinet of Japan recognizes virtual currencies as having a similar function as regular currencies and Bidorbuy in South Africa starts to accept Bitcoin as payments together with Steam. In August, a new major hack takes place with Bitfinex. Later in 2016, the Swiss railway operator SBB would accept Bitcoin in their ticket machines.

The year 2017 saw an even further surge in stores accepting Bitcoin and other cryptocurrencies, whereby Russia and Norway accept, legalize, and further integrate Bitcoin payment accounts. In both 2018 and 2019, more and more stores started accepting cryptocurrencies, but they are still in the corner when compared to regular currencies. These years have also seen further crashes and rises in the market. With the appearance of the Coronavirus, both the regular market and the cryptocurrency market have seen serious decline. Only time will tell how it will affect these markets in the long run.

**Cryptocurrency Markets**

The cryptocurrency market is a volatile market that has been characterized in the last years with steep rises and falls. Contrary to other financial markets, cryptocurrency markets are characterized by their decentralized nature. This means that they depend on peer-to-peer markets, where transactions are propagated through nodes and eventually stored in blocks. This also means that there is no central authority or government that is backing the currency.

Similar to other markets, the laws of supply and demand influence the price of cryptocurrencies. The total number of coins and the rate at which they are released or destroyed are the dominant factors dominating supply. You have cryptocurrencies such as Bitcoin, which have a limited total supply (only 21 million Bitcoins be mined, after this point it becomes impossible because of the limitations implemented in the algorithm of the network). This is completely different from Ethereum, which doesn't cap the total number of Ether that can be mined. Ripple is a third example where more of the cryptocurrency is released in several rounds.

\textsuperscript{7}www.theguardian.com/technology/2014/jun/24/us-auction-seized-silk-road-bitcoins

\textsuperscript{8}www.bbc.com/news/world-europe-jersey-28247796
Market capitalization (supply and demand) is a second factor that determines the value of the cryptocurrency. The more investors are interested in a certain cryptocurrency, the more demand will increase and hence the value of the cryptocurrency will rise. Other factors include the integration of cryptocurrencies as a usable means of payment in (online) stores and e-commerce payment systems. The greater the general acceptance of a specific cryptocurrency, the more likely the value of the currency itself will increase.

Changes in regulation—such as acceptance of cryptocurrencies as a legitimate means of payment or investment, creating a framework for ICOs, and further enabling investments in blockchain infrastructure—greatly influence the value of cryptocurrencies (as we saw with the crash in 2018). Others factors are press coverage, investor acceptance, and the growth of interesting blockchain use cases. Finally, prosecution of those who lure investors into nonexistent cryptocurrencies, creating fake ICOs and stealing investor funds, further increases the value of legitimate cryptocurrencies.

A second aspect of the crypto-world is the existence of crypto-assets. Cryptocurrencies are one aspect of crypto-assets, but you also have other digital assets that can be traded. Next to cryptocurrencies, you have platform tokens, or crypto-commodities, utility tokens, and transactional tokens. Ether (from the Ethereum network) is considered a platform token, as the platform can be used to create decentralized applications. Utility tokens exist on top of other platforms such as Ethereum. These tokens have been developed with a specific use case in mind. Finally, there are transactional tokens. Examples are Ripple, IOTA, and Stellar. These tokens are used to enable cross-border payments.

Next to cryptocurrencies, derivatives trading has also been created. These financial instruments play into the value of cryptocurrencies and how they change over time. There are options and other instruments out there that are even more high risk but promise high return. If these instruments are used and traded in high amounts, they can introduce even more uncertainty in already volatile markets.

You should understand that people will keep on finding new ways to create financial instruments. Understanding these instruments and the markets they function in is crucial for any investor.

Some Core Cryptocurrency Concepts

In this section, we cover core concepts that you will almost certainly hear or read about if you decide to enter the cryptocurrency market. Understanding these core concepts will help you not only better understand these markets but also understand the possible issues with these markets.
Atomic Transactions

Atomic swaps are cryptocurrency transactions that happen peer-to-peer without needing a third party such as an exchange. The first atomic swap took place on September 20, 2017 between Decred and Litecoin. These transactions can take place in several ways—either directly between the separate blockchains even though they have different native coins, or by using off-chain channels. These transactions between different cryptocurrencies make the entire cryptocurrency system even more flexible.

With the advent of atomic swaps, we enter the possibility of a world with fee-less exchanges. These (on-chain) swaps can take place because the participants work based on a shared secret. Similar to the Lightning network (which is a network on top of the Bitcoin network to improve scalability and transaction speed), here we similarly use hashed time-locked contracts (HTLCs). In short, when we have two participants that want to exchange two different types of cryptocurrencies, they open a payment channel. The first participant creates a payment address. There is a deposit on this address by the first participant and, after this, a value is created. This value is the key, while the hash of the value is the lock. The first participant sends the hash to the second participant. The second participant generates an address but uses the hash they received to do this. They then send their coins to the second address.

Still following? Well, only the first participant can unlock the second address by using their value. This can be done by signing the transaction for the second participant’s address. Similarly, the second participant signs a transaction for the first participant’s address. One problem: the second participant doesn’t have the value to unlock their new coins. This value is revealed when the first participant signs their transaction. This way, the second participant can unlock the account.

The assumptions here are that both currencies support hashed time-locked contracts. Furthermore, they need to have the same hashing algorithm. When this is not the case, atomic swaps between the currencies simply cannot happen. Of course, one could try to achieve swaps by using several steps (direct swap between BTC and ETH isn’t possible but using DOGE is). Off-chain transactions take place via a layer 2 protocol such as the Lightning network.

In practice, the Komodo platform and blockchain.io are both focusing on atomic swaps between several parties.

---

9https://blockgeeks.com/guides/atomic-swaps/
The ICO

The ICO (initial coin offering) is the crowd sale of new cryptocurrencies to possible investors.\(^{10}\) In the past years, there was almost regulation making it an attractive way to lure investors. However, this has also allowed a number of conmen to enter the scene, certainly during the high days of the crypto-bubble. Investors were no longer thoroughly checking about what they were investing, and just wanted to profit as well from the major profits that were being made in the crypto-market. Some of the ICOs were purely based on ideas, without anything else, and were able to reap in millions without anything concrete to match. Some of these projects became a success, but most ICOs that had nothing than an idea behind them led to nothing. To give you an idea, in about 4.5 months in 2018, 6.3 billion USD were raised with ICOs! Table 5-1 shows some of the biggest ICO scams (to date).\(^{11}\)

| Scam Name         | Amount of Money Scammed (USD) |
|-------------------|------------------------------|
| Pincoin and iFan  | 660,000,000                  |
| CentraTech        | 32,000,000                   |
| Onecoin           | 30,000,000                   |
| Plexcoin          | 15,000,000                   |
| Bitcard           | 5,000,000                    |
| Opair and Ebitz   | 2,900,000                    |
| Benefit           | 2,700,000                    |
| Bitconnect        | 700,000                      |
| Confido           | 375,000                      |
| REcoin and DRC    | 300,000                      |
| Ponzicoin         | 250,000                      |
| Karbon            | 200,000                      |

Does this mean that every ICO is a scam? Of course not, but just as with regular investments, it is up to you to perform due diligence, concerning the projects and the companies behind an ICO, but also concerning the regulation and the possible pitfalls. This relates to personal liability as well (remember the DAO case!). Research the development team behind an ICO project as well. It is not an uncommon tactic to invent fake founders and biographies to give a project more legitimacy. Even if the development team is real, is their...

\(^{10}\)https://blockgeeks.com/guides/initial-coin-offering/
\(^{11}\)https://medium.com/@tozex/the-five-biggest-ico-scams-54967ec92b87
experience real? Next, read the whitepaper thoroughly. Is the documentation reasonable? Can they achieve what they want to achieve? Do you see this project going somewhere? And even if there is a convincing whitepaper (as was the case with Plexcoin), do not immediately trust them. Another red flag is if you cannot clearly follow the ICO process. For a legitimate company, it shouldn’t be too hard to show how the process works and show the progress during the sale. If they hide this or make it extremely difficult to understand, you should know something is wrong. But finally, and I cannot state this clear enough, always exercise caution when considering investing in an ICO. Getting rich quick is always a nice idea, but the likelihood of it happening is really small. If something sounds too good to be true, it probably is.

While the first ICO ever was probably the sale of Ripple in early 2013, it was the Ethereum ICO in 2014 that was able to draw the public’s attention, because it raised 18.4 million USD. What did the investors receive in return? More often than not, the answer is “tokens,” which can refer to value, stake, voting rights, or anything else for that matter. When you ask the SEC (Securities and Exchange Commission), there are only two types: security tokens and utility tokens.

Security tokens are identified using the Howey test, which consists of three questions:

- Is it an investment of money?
- Is the investment in a common enterprise?
- Is there an expectation of profit from the work of the promoters of the third party?

If not all these questions can be answered positively, you are dealing with a utility token. These tokens give holders the right to use the network or take advantage of the network by voting.

So why do projects start an ICO in the first place? Most importantly because they wouldn’t be able to start an IPO (initial public offering). The ICO allows them to have a shot at their project, without having to go through all the regulatory requirements linked to an IPO. But probably the most important advantage is the strong link that is created between a project and the community. As most of these projects also need that same community to exist and flourish, ICOs deliver the perfect platform to create a mutual, beneficial relationship. Table 5-2 shows the ICOs with the highest returns to date.

---

12[www.investopedia.com/tech/how-identify-cryptocurrency-and-ico-scams/]
However, you should also consider the disadvantages, and there are quite a few. As mentioned, there are scammers out there who are waiting to take advantage of people not looking into the details. On top of that, even if the development team behind a project is genuine, 90% of startups still fail! Another disadvantage is the appearance of “crypto-whales,” which are investors that immediately buy huge bulks of the ICO, cutting in line by paying high amounts of transaction fees, thereby destroying the idea of decentralization. An example is the BAT ICO, where 35 million USD was raised in 24 seconds by a few investors.

A fourth disadvantage is the popularity of certain ICOs that effectively clog up the network, thereby preventing investors from participating or even completely cutting out the ICO! Finally, I should also mention the security of ICOs and security platforms as a whole. In the past, several infamous hacks have taken place, leading to the theft of millions. Due to the nature of cryptocurrencies, there will always be security measures that you have to take into consideration and certainly with something that is new or untested, you can imagine that there are flaws that have been overlooked by even the best developers.

Even though ICOs still take place, you should also know that regulatory bodies are taking a deeper interest in them. The SEC forces new ICOs to declare if they are a security and China and India have banned ICOs altogether. Within the EU, the ICOs have to meet the AML/KYC regulations that are in place. It is seen as a high-risk investment that should be strongly regulated to protect the investors. However, the EU believes that it should
support innovation and has therefore not banned the practice.\textsuperscript{13} The future will show how regulation changes over time and how ICOs might evolve.

**Fractional Reserve Banking and Bitcoin**

There have been some discussions on the concept of fractional reserve banking and the use of Bitcoin (or any other cryptocurrency for that matter). Basically, you have two major views looking at the concept: the Keynesian and the Austrian view.\textsuperscript{14} From the first perspective, there is no real difference from any other currency. Banks can still present customers any token as “available for withdrawal,” while at the same time making them available for loans for different customers.

Of course, the bank is responsible for keeping a sufficient supply in deposit to make sure it can handle the withdrawals and payments from the customers. These banks would need to rely on their own reserves, as a central bank would not be able to help them in case of a default. If we take Bitcoin as an example, we can understand that, even though there is a maximum supply of 21 million Bitcoin, with the use of fractional banking, the Bitcoin money supply can be multiplied by the money multiplier. Some supporters of the idea of fractional reserve banking with Bitcoin (or any cryptocurrency for that matter) state that this limited supply could make it better for fractional reserve banking than any other currency, as those are traditionally more likely to become inflationary, where a currency with a limited supply is more likely to be deflationary.

The Austrian viewpoint takes a different approach. For fractional banking to have an effect on the money supply, the debt instruments used by the bank must be accepted if they were themselves proper money. In the past, there were some other forms of Bitcoin, such as Casascius physical Bitcoins (stopped in 2013) and Bitbills (stopped in 2012). In the past, there have been some other debt instrument issuances, but these often led to issues as they were restricted to a narrow field of uses. The transactions happening outside of the Bitcoin network are not compatible with it. In the past there have also been issues with eliminating the excess instruments (Mt. Gox hack in June 2011), bankruptcy (mybitcoin), or investor bailout. Based on the previous information, we have to consider over-issuance, the general acceptance of debt instruments, and the market price of the debt instruments at a different rate than the reserve ratio of the issuer.

So, is it possible to create a fractional reserve banking system with a cryptocurrency? Several views have been issued in the past, stating that this can only be an illusion if you look at the background of cryptocurrencies, the

\textsuperscript{13}www.cyberius.com/blog/news/european-regulations-on-icos/

\textsuperscript{14}https://en.bitcoin.it/wiki/Fractional_Reserve_Banking_and_Bitcoin
regulatory issues, combined with issues related to scalability and transparency. Others do believe in the system, such as the reports that MasterCard has been trying to patent cryptocurrency fractional reserve banking.\textsuperscript{15} One of the key ingredients for such a system to emerge and to become successful is that a cryptocurrency (or more than one) should emerge as a widely accepted means of payment. The same cryptocurrency would have to be used for high-value transactions between large institutions, which are two though requirements for a cryptocurrency today.

Other impacts of fractional reserve banking on cryptocurrencies is the influence on price. By using fractional reserve banking, you are likely to reduce the value of the cryptocurrency for investors that are holding on to a certain deposit. This means that it might be against their interests to support these practices. There are several ways to offset these developments. One is that the maximum amount of cryptocurrency deposits through fractional reserve banking must be a finite multiple of the amount of outstanding cryptocurrency. Another is that investors might decide to hold more of the fractional reserve banking cryptocurrency deposits than they would of the underlying cryptocurrency.

As you can see, there are several ways to discuss the theoretical possibility of fractional reserve banking with a cryptocurrency, but these remain theoretical for the time being. The underlying factors that need to be fulfilled before one might even consider fractional reserve banking are quite onerous. Even as a best case, it would be risky. Combine this with regulatory issues, the problem of clear oversight by any type of government, and the absence of clear insurance for investors, and it becomes pretty clear that this doesn’t seem realistic in the near future. Central banks and governments are better suited to deal with the risks introduced by “classic” currencies and banks, while cryptocurrencies bring a whole set of risks of their own.

### Stablecoins

Stablecoins are another important aspect of the blockchain world and cryptocurrencies that we should take into account. These are specifically designed to reduce the volatility of cryptocurrencies and are commonly pegged to a stable asset or basket of assets.\textsuperscript{16} These currencies can be backed by commodities, fiat, or other cryptocurrencies.

A first example is the Digix Gold Token, which is backed by gold. Introducing a gold standard to the cryptocurrency world, these tokens are clearly linked and backed by a precious metal, which provides more security than stablecoins backed by either fiat or other cryptocurrencies.\textsuperscript{17}

\textsuperscript{15}www.frbatlanta.org/cenfis/publications/notesfromthevault/04-fractional-reserve-cryptocurrency-banks-2019-04-25
\textsuperscript{16}https://en.wikipedia.org/wiki/Stablecoin
\textsuperscript{17}https://digix.global/
Fiat-backed stablecoins base their value on a pegged fiat currency, where a third-party (regulated financial entity) holds the value of the backing fiat. These tokens can be traded and redeemed for the backing currency at the issuer. One should not underestimate the cost of such a peg, as you should take into consideration the cost of maintaining the backing reserve, legal compliance, maintaining licenses, audits, and more. TrustToken is a company that specializes in stablecoins, such as TrueUSD, TrueGBP, TrueAUD, and more.\(^{18}\) It uses multiple third-party financial institutions to maintain its peg to these currencies and claims to have passed several security audits in the past.\(^{19}\)

A second and much more controversial fiat-backed stablecoin is called Tether. The whitepaper was published in January 2012 by J.R. Willett, and it describes a new cryptocurrency on top of the Bitcoin network. By using Mastercoin and the Mastercoin foundation (now the Omni foundation), he created (together with Brock Pierce) the Tether cryptocurrency. It used to claim that it was backed by USD, but changed its statement on March 14, 2019.\(^{20}\) Since that date, it also includes loans to affiliate companies, therefore immediately jeopardizing its status as a stablecoin.

Even worse, the New York attorney general alleges that Bitfinex used Tether reserves up to 850 million USD to cover up their own missing funds, which occurred in mid-2018 and hadn’t been disclosed publicly.\(^{21}\) Tether Limited now even claims that Tether owners have no contractual rights or legal claims that the Tethers will be exchanged for USD. On April 30, 2019, Tether Limited’s lawyer claimed that each Tether was backed by $0.74 in cash and cash equivalents.\(^{22}\)

The company has also been accused of not providing the promised audit results of their adequate results backing Tether, manipulation of the Bitcoin price, the unclear relationship with the Bitfinex exchange (the Paradise papers leak suggests a link, as Philip Potter and Giancarlo Devasini were responsible for setting up Tether Holdings Limited in the British Virgin Islands in 2014; next to these leads, there is also the fact that the spokesperson for Bitfinex and Tether has stated that the CEO of both is Jan Ludovicus van der Velde\(^{23}\), and the lack of a long-term banking relationship (there were transactions

---

18. [www.trusttoken.com/currencies](http://www.trusttoken.com/currencies)
19. [www.coindesk.com/trusttoken-says-it-passed-3-security-audits-with-no-bugs-found](http://www.coindesk.com/trusttoken-says-it-passed-3-security-audits-with-no-bugs-found)
20. [www.forbes.com/sites/francescoppola/2019/03/14/tethers-u-s-dollar-peg-is-no-longer-credible/#3b108717451b](http://www.forbes.com/sites/francescoppola/2019/03/14/tethers-u-s-dollar-peg-is-no-longer-credible/#3b108717451b)
21. [www.wsj.com/articles/bitfinex-used-tether-reserves-to-mask-missing-850-million-probe-finds-11556227031](http://www.wsj.com/articles/bitfinex-used-tether-reserves-to-mask-missing-850-million-probe-finds-11556227031)
22. [www.bloomberg.com/news/articles/2019-04-30/tether-says-stablecoin-is-only-backed-74-by-cash-securities](http://www.bloomberg.com/news/articles/2019-04-30/tether-says-stablecoin-is-only-backed-74-by-cash-securities)
23. [www.bloomberg.com/news/articles/2018-01-30/crypto-exchange-bitfinex-tether-said-to-get-subpoenaed-by-cftc](http://www.bloomberg.com/news/articles/2018-01-30/crypto-exchange-bitfinex-tether-said-to-get-subpoenaed-by-cftc)
through a Taiwanese bank, back through Wells Fargo). In 2017, other Tether coins were issued—Euro Tether on Bitcoin’s omni layer, and USD and Euro Tether as ERC-20 tokens on the Ethereum network.

The case of Tether has clearly shown that stablecoins cannot be trusted blindly. However, you should understand the popularity of Tether, as it is the most traded cryptocurrency when we talk about daily trading volumes. It is very popular in Asia and is even feared to clog up the Ethereum network because of the number of transactions that are taking place every day.

Another player that wants to fill the gap and create a major stablecoin is Facebook, with its “Libra” project. The launch of Libra (formerly known as GlobalCoin or Facebook coin) is projected in 2020 at the earliest, so it doesn’t exist yet, but there has been already some controversy surrounding the project. The project started in 2017 with Morgan Beller working on Facebook’s blockchain initiative (later on David Marcus and Kevin Well joined the project). By February 2019, there were already about 50 engineers working on the project in a completely separate division.

The project was met with a lot of criticism, also relating to the questionable reputation Facebook has when it comes to privacy of its users. There were some scandals in the past showing that the company takes privacy regulation quite lightly (Cambridge Analytica comes to mind), so a cryptocurrency linked to this Internet giant seems to be the next step in controlling our personal data. Other concerns are linked to the sheer size of the company and the number of users, making it rival many fiat currencies, but without the checks and balances that are in place for centralized currencies. Libra also wouldn’t be a decentralized currency but would use a centralized system, with the “Libra association” in Geneva, Switzerland at its core. The bucket behind Libra would consist 50% USD, 18% Euro, 14% Japanese yen, 11% Pound sterling, and 7% Singapore dollar.

The launch of the currency has been stopped due to the criticism received from the public and many regulatory institutions. On September 4, Mark Zuckerberg announced that the launch would be postponed until all (United States) regulatory concerns have been dealt with. Originally, the plans were supported by a number of big and important payment parties. PayPal left the project on October 4, 2019, while eBay, MasterCard, Stripe,

---

24 www.wsj.com/articles/the-mystery-behind-tether-the-crypto-worlds-digital-dollar-1534089601
25 www.cnbc.com/2019/07/20/facebook-libra-partly-created-by-female-engineer-morgan-beller.html
26 www.washingtonpost.com/technology/2019/09/19/facebooks-mark-zuckerberg-dined-with-lawmakers-last-night-privacy-cryptocurrency-were-menu/
Visa, and Mercado Pago left on October 11, with Bookings Holdings following on the 14th. A number of companies still support the association, such as Uber, Spotify, Lyft, PayU, Coinbase, and many others.

The response in the United States was quite harsh, with President Trump claiming that Facebook would have to adhere to Banking regulation and questioning if they would want to proceed with the project. The response in Europe, and most notably in France, was even more harsh, with the French finance minister Bruno Le Maire claiming that Libra could be a threat to monetary sovereignty of nations and should therefore not be allowed to be developed. He also went on to state that it might incorporate abuse of marketing dominance and could introduce systemic financial risks. German MEP Markus Feber also warned that Facebook could become a shadow bank with the power it would have over Libra.

The government of Japan has also started an investigation in how Libra might affect the monetary policy and financial regulation. Finally, there were the alarming sounds from Switzerland, where the Federal Data Protection and Information Commissioner stated that it had never heard from Facebook at all (this while David Markus claimed before the U.S. Senate that they would oversee the project).

Finally, there are also cryptocurrency-backed stablecoins. While these are very similar to fiat-backed cryptocurrencies, the main difference lies in the fact that crypto-backed stablecoins use smart contracts in a decentralized fashion to back their coins. These also often allow users to take out loans against a smart contract, locking in a certain amount of collateral. These smart contracts may liquidate the user’s loan if the collateral decreases too close to the value of their withdrawal. You can immediately sense that these coins require more implementation effort via coding, introducing the risk of bugs and possible exploits. You used to have the DAI Maker stablecoin (which has currently been transformed into a fiat-backed stablecoin, pegged to USD), but the Synthetix company still offers, next to fiat-backed stablecoins, cryptocurrency-backed stablecoins.

One final example we should look into are the seigniorage-style stablecoins, which are not backed by any asset. Here, there are algorithms in place that regulate the money supply so that they can ensure that the currency maintains a certain price. One project that wanted to achieve this is called “Basis,” but it was eventually shut down because of the U.S. securities regulations that would have applied to the project.

27 https://libra.org/en-US/
28 https://masterthecrypto.com/guide-to-stablecoin-types-of-stablecoins/
29 www.basis.io/
Digital Twins and Blockchain

Something that has also gotten some extra attention in recent years is the creation of digital twins to protect brands against counterfeiting. Digital twins are of course not only limited to blockchain technology, as we all know with our digital identities. However, blockchain platforms offer a new way of storing a digital twin in a secure manner and without a centralized point of control or single point of failure.

Blockchain offers the possibility to add data and follow the process of an asset, without the possibility to simply modify or corrupt the data that has been stored. Combine this idea with that of digital certificates or blockchain-linked identities and you are able to design a process to follow up on assets, services, and products all over the world. The concept of non-fungible tokens takes a prominent role here, as these represent the asset in the digital world.

Now, where can these digital twins prove their worth? A very interesting example is that of pharmaceuticals and counterfeited products. By creating digital twins on the blockchain, one can easily follow a product from producer to consumer, and any product not matching the data in the system can be tagged as at least suspicious. This could add an extra layer to the current battle against drug abuse and medicine counterfeiting. A second example is that of notary services for the real estate market, where one could buy or sell a house based on the digital twin that is available on the blockchain.

Based on the previous examples, it should be fairly simple for you to think about some other examples where digital twins could prove to be useful or interesting and could enhance the current way of working. As with any decentralized technology, a lot will depend on the cooperation of different parties within the process, to make these digital trends a success.

Luxtag is an example of a company focusing on product and asset security. They offer a base API to follow your product as a digital twin, but also tamper-proof credentials.

Blockchain and Digital Identity

A common issue in our world today is that of personal identity. Even though it has been identified as a basic human right in the UN’s convention on the rights of the child, we often find problems in many countries. These relate to places that have been faced with war, poverty, or lack of governance. Without some basic personal information, you are limited in almost every

---

30 https://medium.com/luxtag-live-tokenized-assets-on-blockchain/how-creating-digital-twins-on-blockchain-will-protect-brands-3ada31b5fb2f
31 www.luxtag.io/
way, as you cannot own property, vote, receive government services, have a bank account, find employment, ask for protection, or pursue anything else for that matter.32

As it currently works, centralized institutions need to give you an identity, and if they do so, they can still mishandle your data. A final consideration is the possibility of identity theft, which is always looming in the modern world. If you look at the case of refugees, it is often difficult to verify their identity, their back story, and their credentials, certainly when they come from a nation at war with the destruction of information and the impossibility of verification. According to the World Bank Group’s 2018 #ID4D Global Dataset, almost 1 billion people around the globe struggle proving who they are.33 On top of that, about 1.7 billion people don’t have a bank account.34 Blockchain solutions might not only provide a means of payment to people who have been left out of the centralized solutions of the modern world, but they might also help them to finally prove their identities.

How could it facilitate the current challenges of digital identity? Well, when we think about identity theft, it comes down to how we make it very difficult to use the same identity twice for two different people. Trying to use the same digital unit twice is also known as the “double spending” issue. Similarly to preventing double spending, the blockchain technology could prevent the double use of a single identity by rogue elements in the system. By using hashes, one could also make sure that digital files haven’t been tampered with, otherwise one will immediately see that something has been changed in the data, thereby proving that they are no longer dealing with the original document. Finally, there is the malicious intent one could have in the system when trying to perform certain processes. By using decentralized consensus, these processes can be stopped in the system, protecting participants from these attackers.

Most importantly, if we could agree on one decentralized system spanning the world, identity would no longer pose a problem. We would have irreversible proof of each person, without having to question whether the data is correct or whether the data belongs to a different person. Of course, this is something that will not be happening tomorrow, but several implementations are working on digital identity with blockchain technology, such as the Sovrin foundation (also behind Hyperledger Indy), Civic, and uPort.

32 https://blockgeeks.com/guides/blockchain-and-digital-identity-ultimate-guide/
33 https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity
34 https://globalfindex.worldbank.org/
Where Do Cryptocurrencies Get Their Value?

An important question asked by people new to the cryptocurrency space is where cryptocurrencies derive their value. This very much depends on the type and kind of token you are dealing with. As we mentioned, there are the stablecoins, which try to peg to a certain asset, fiat currency, or cryptocurrency (or a bucket of those). These derive their value from the peg they are trying to maintain, but we have seen that this is not always successful, which immediately leads to the devaluation of the token.

A lot of people will say that it simply comes down to supply and demand. And to a certain extent, this is certainly true. As we have seen in the past (and still today), fluctuations in price can be clearly linked to the demand for certain tokens, just as the vanishing demand for a specific cryptocurrency might destroy its price. However, there are some other aspects that we should take into consideration when we look at possible drivers of the value of a specific token.

When we move away from stablecoins to more general cryptocurrencies, there are a couple of factors that we have to consider. First of all, these tokens can be seen both as a medium of exchange and as a store of value. When we extrapolate from the Bitcoin case, the store of value valuation of a certain cryptocurrency is linked to its power as a medium of exchange. If a token does not achieve success as a medium of exchange, it will not be able to act as a store of value. A second consideration is the legitimacy of cryptocurrencies that might increase/decrease over time, leading to more or less adoption of these tokens, which in turn has an impact on their volatility. Thirdly, we have to look into the appearance of speculative valuation bubbles. These reduce the attractiveness of these currencies for participants interested in stable environments. Other possible considerations are whether some of these coins might be used for fractional reserve banking (or not), and if there is a limited or limitless supply of these tokens. You could also take into consideration the energy spent to mine a token and the value created in other processes (i.e., contributions to science or specific industries). Finally, some tokens represent a certain service or product, such as Internet access, media distribution, voting rights, and more.

Only when you take all these drivers into account, together with a healthy (and hopefully growing) interest from a supporting community, can you try to understand how the value of certain cryptocurrencies is derived, and how their value might change in the future.

35 www.investopedia.com/ask/answers/100314/why-do-bitcoins-have-value.asp
Crypto Dust

Crypto dust is something specific to the cryptocurrency world, but something you should certainly be aware of. As you might have guessed, dust refers to tiny pieces of value of a certain token. These tiny outputs are generated after a number of transactions and eventually require more fees to be transacted than their actual value. This is because these tiny transactions take up just as much space on the blockchain as large transactions, leading to the discrepancy between the fee that needs to be paid and the actual value of the transaction.36

As you can imagine, for many cryptocurrencies, the transaction fee is linked to the popularity and congestion of the network. This means that a certain value today might not pose a problem, while tomorrow it might become crypto dust. The only way to fix the issue with dust is by collecting enough of these dust values and consolidating them into one transaction by lumping them together. This technique depends on the wallet you are using and the cryptocurrency that you want to consolidate. The only possible issue with this is the price you pay: your privacy. As you are sending a lot of dust from different change addresses to your main wallet account, it can become apparent to other participants that these are linked to you as well. Certainly if you have been through a KYC (Know Your Customer) process that verifies your identity (necessary for financial institutions to fight financial crime), the link can easily be made.

Linked to this issue are so-called “dusting attacks,” which are used to determine participants’ identities.37 This attack consists of dust transactions that are sent to the victims’ wallets. They keep these transactions in a log and after a while the attackers can link several wallets together and determine the identity of the person behind a certain wallet. Certain wallets, such as the Samourai wallet, now flag dust transactions as suspicious by default to protect their users.

Exchanges and Attacks

When we talk about cryptocurrency exchanges, we talk about online platforms that allow participants to exchange a digital asset for another based on the market value of these assets.38 You should not confuse these exchanges with wallets or wallet brokerages, which allow you to buy or sell a small range of cryptocurrencies, which in turn can be exchanged for other tokens. Most exchanges will allow you to trade one token for another, while some others will still allow you to trade for a limited number of fiat currencies (an example is Kraken).

36www.coindesk.com/bitcoin-dust-tell-get-rid
37www.binance.vision/nl/security/what-is-a-dusting-attack
38www.ethos.io/what-are-cryptocurrency-exchanges/
When you want to start using these exchanges as well, or start trading cryptocurrencies, you should start by setting up your own online account. One example where you can do this is Coinbase. Of course you can use any other online service but you should always consider the safety of these online services, so do your research before you open an account. You want to make sure that your invested funds don’t just suddenly disappear. There are also lists available online, such as in Belgium where the FSMA has published a non-exhaustive list of websites linked to fraud.

Nevertheless, once you have set up your account, you will most probably only be able to buy specific cryptocurrencies (i.e. Bitcoin and Ether). If you want to buy something else, you will have to open an account on an exchange. There, you can trade the Ether or Bitcoin you bought for other tokens. With most of these other tokens, it is not possible to simply convert them back to fiat if you want to cash out (or at least not for now). This means you have to convert them back to Ether or Bitcoin first, which then can be exchanged for fiat currency. On top of that, you will have to take into account local regulations when it comes to profit from trading and cryptocurrencies in general.

All of this seems fairly easy to understand. So why are these exchanges so often victims of cyberattacks? Well, first of all, these exchanges have to hold large amounts of cryptocurrencies to ensure their liquidity (immediately proving that criminals are lured by the money they might make if they are successful). There are also a lot of transactions happening. The investments in cybersecurity are often limited, as these companies need their cash to grow and innovate, and cashing out stolen cryptocurrencies is often a whole lot easier than doing so with fiat currency. This makes it even more attractive to prospective criminals.

A lot of people seem to have the idea that to attack such an exchange, very specific attack vectors need to be used to be successful. In reality we are dealing with a web service that is susceptible to a lot of the same attacks as any other web service, meaning that there is a range of server-side and client-side attacks that can be executed. When we look at the report provided by hackernoon, we can see that there are four sections of attacks that are relevant for exchanges (when they look at those exchanges that have a daily trade value of at least $100,000): user security, domain and registrar security, web security, and DoS protection.

I will not go into detail about all the possible attack vectors for each of these sections, but it’s important to understand that none of them got an A+ score, meaning that none of them are ideal. Only 21 got an A score while most got

---

39 https://medium.com/block-to-basics/crypto-exchanges-why-are-they-being-hacked-so-often-b4346f281deb
40 https://hackernoon.com/security-problems-of-crypto-exchanges-d5e2f595fb79
a B score, meaning that they have some issues. Table 5-3 shows the 21 exchanges that received an A score from the Hackernoon report.

Table 5-3. Exchanges with an A Score. Source: Hackernoon.com

| Kraken   | Cobinhood | Poloniex | BitMEX | Bitfinex | Bitliss | BitMart |
|----------|-----------|----------|--------|----------|---------|---------|
| BtcTurk  | Coinbase Pro | GOPAX  | Livecoin | UEX  | HitBTC | BTC-Alpha |
| LiteBit  | Exrates  | Luno     | Kucoin | Paribu | Bitso  | Coinbe  |

To deal with these risks, several wallet solutions have been developed. A final example is the ZERO, developed by NGRAVE. While private keys stored by exchange platforms can be stolen during an attack, this wallet is locked away from any type of networking, has its own approach to key generation, and takes into account the use of QR codes. It is so far the only wallet that was able to obtain the EAL7 Common Criteria Certification.41

Cryptocurrency Market Capitalization

When you look into cryptocurrencies or start researching specific currencies, you will almost immediately come across charts discussing the market capitalization of a token.42 What do they mean? Consider the example shown in Figure 5-1 to get a better understanding of this concept.

Figure 5-1. Cryptocurrency graph. Data Source: coinmarketcap.com

---

41https://medium.com/ngrave/ngraves-zero-hardware-wallet-is-the-coldest-wallet-of-them-all-483aa3d32a14
42https://coincentral.com/cryptocurrency-market-capitalization/
To get a better understanding of the price of a certain cryptocurrency, you should look at these charts. These charts can give you an idea of the market value, the volume, and the evolution over time of a currency, and you can also follow the impact of certain events. Analysts commonly use these charts to make informed investment decisions, as these charts show them the total current coins * current price.

These charts generally serve as an indicator of the amount of risk involved for investors. However, one should always take into account the fact that we are dealing with cryptocurrency markets, which inherently pose an increased risk for investors compared to other “classic” forms of investment. This might change in the future, and I am well aware that there will be people who do not agree with this view, but you should always take this into consideration when you plan to invest in the crypto-market.

Back to our story, you can, similarly to the stock market, divide coins in small cap, mid cap, and large cap based on the changes in the market capitalization. It should be clear that large cap are the more stable coins but the small caps can yield enormous rewards (often linked to enormous risk). While Bitcoin currently has the largest market capitalization, you can also look into smaller altcoins and consider what their future growth potential might be. Of course, you should also know that these charts don’t guarantee what the future value of a cryptocurrency will be. You should look into the coins you want to invest in, analyze the supply and the underlying assumptions/technology before you make a final decision. The market cap also doesn’t provide information considering the velocity of the cryptocurrency. Trends have to be analyzed over time. It’s important to take into account the numerous allegations of crypto-market price manipulation.\(^3\) Research shows systemic trends in Bitcoin price and the number of “large” participants in many altcoin markets, which means you need to scrutinize these investments even more closely.

Common appearances are wash trading (buying and selling with one’s own funds to create the perception of market activity), pumps and dumps (artificial buying of an altcoin, after which you sell your stake to victims), dark pool trading (large trades outside of standard exchanges), shilling (generating false hype around a coin for personal gain), and whale trades (large investors pushing the price in their favor).\(^4\) A final consideration when you look into overall market capitalization of the crypto-market is the existence of dead coins, which should be subtracted from the overall number (even though an exact number is unknown). Alternative approaches to performing deeper market analyses can be found in the corner of fundamental analysis.

\(^3\)www.forbes.com/sites/billybambrough/2019/09/25/striking-bitcoin-research-points-to-price-manipulation/#4f9186665c2b
\(^4\)https://hackernoon.com/the-mysterious-manipulation-of-crypto-markets-and-how-to-manage-5234e19e6e77
Crypto Futures Trading

For those of you who are interested: futures trading has also entered the world of cryptocurrencies. In December 2017, the Chicago Mercantile Exchange launched the first Bitcoin futures contract. These futures were cash settled, meaning that at the end of the contract, one has to compare the current market value to the agreed upon price, after which there is a transfer of the value. These types of contracts are often used to smooth out the risk that an investor (or miner) has by holding a certain amount of a tokens (in this case Bitcoin). However, these can also be used by speculators who want to bet on the price movement of cryptocurrencies.

In a market where accusations of market manipulation already exist, you should take into account the extra risk you face by holding such contracts. Other criticism also refers to the fact that cash-delivered futures don’t force investors to actually hold the altcoin in hand, which leads to the fear that this could lead to the dilution of the market supply. There are also physically delivered futures, such as those provided by Bakkt. Upon settlement, there is a “physical” exchange of Bitcoin between the participants. Kraken has futures on Ethereum, Litecoin, Bitcoin Cash, Ripple, and Bitcoin.

As this book does not focus on options trading, I will not go into the details of going short, long, and margin calls. All I can do is issue a warning for those who want to enter this type of market. It is a market that can provide liquidity and offer hedging instruments to existing positions, but it can also introduce a whole lot of risk if you speculate on future prices. As with any market, it is always the same rule: know the market you are entering and understand the risks of the instruments that you are buying or selling. And even in that case, always do your due diligence.

Crypto Dividends

Throughout this book, I have shown that cryptocurrencies have been used and are being used in a similar way as “classic” investment instruments. They have been used in ICOs to raise money for startups, create digital twins and crypto-assets, and people have made money over mining and trading altcoins.

---

45 [https://medium.com/scalar-capital/futures-crypto-8ac1a993ce85](https://medium.com/scalar-capital/futures-crypto-8ac1a993ce85)
46 [www.bakkt.com/index](http://www.bakkt.com/index)
47 [www.kraken.com/features/futures](http://www.kraken.com/features/futures)
48 [www.howtotoken.com/for-traders/trade-bitcoin-futures-ultimate-guide-part1/](http://www.howtotoken.com/for-traders/trade-bitcoin-futures-ultimate-guide-part1/)
49 [https://coinsutra.com/cryptocurrency-dividends/](https://coinsutra.com/cryptocurrency-dividends/)
However, some of these altcoins have implemented a new strategy for investors to make money: dividends. There are two ways you can start making dividends with cryptocurrencies:

- Staking: Holding a proof of stake coin in a special wallet
- Holding: Buying and holding an altcoin in a wallet

A first example of an altcoin paying dividends is Komodo (KMD), which can be staked in a staking wallet after you buy it. It promises a return of 5% on an annual basis. NEO is a smart contract token, similar to Ethereum, where you can stake your NEO in order to receive a payout in GAS. VeChain uses the same mechanism as NEO, but instead of paying out GAS, it pays out VTHOR.

Another example is BTMX, which is the token of the BitMax exchange. You can lock up the coin to earn USDT (the reward is calculated and distributed daily). Kucoin (KCS) is an altcoin linked to the KuCoin exchange and distributes 50% of transaction fees to the token holders. The Coss token of the Coss Exchange has a similar mechanism in place.

Other interesting tokens are Pundi X, PIVX, and BiBox. The future will certainly show more altcoins with different payouts. If you are interested in such an investment, always make sure that you perform due diligence so that you understand both the dividend scheme as the risks involved.

**Bonded Escrow Contract**

Bonded escrow contracts are an area where blockchain smart contracts could effectively help optimize existing companies and the regulation in place. These smart contracts could help eliminate the middleman for a lot of existing services, effectively making these processes more consumer friendly, cheaper, and in some cases safer. When we talk about escrow services, smart contracts could introduce the “safe remote purchase.” For those who do not know what escrow services are, they simply relate to a trusted third-party when you are dealing with an untrusted relationship between buyers and sellers. An example is one of the many online platforms that handle second hand merchandising. If you sell a product on such a platform, you generally don’t know the buyer, so how can you make sure that you get your money when you send the product? And vice versa, how does the buyer know that they will receive the product when they pay the seller?

---

50 [www.bestcryptodividends.com/](http://www.bestcryptodividends.com/)
51 [https://hackernoon.com/how-a-smart-contract-replaced-an-escrow-company-in-a-60k-deal-551ff7839044](https://hackernoon.com/how-a-smart-contract-replaced-an-escrow-company-in-a-60k-deal-551ff7839044)
52 [https://medium.com/coinmonks/escrow-service-as-a-smart-contract-the-business-logic-5b678ebe1955](https://medium.com/coinmonks/escrow-service-as-a-smart-contract-the-business-logic-5b678ebe1955)
The escrow service locks in the payment of the buyer and only releases the payment to the seller when the buyer confirms that they received the product. This happens for a fee of course.

Instead of an escrow service, consider a smart contract. The code can vary depending on the use case, but it will generally force both the seller and the buyer to put up a stake so that they both have incentive to follow the stipulations of the agreement. When one of them doesn’t follow the rules of the agreement, the code of the smart contract will penalize that participant and they will lose their stake. This not only reduces the cost for the participants (as you generally don’t have to pay for a smart contract, and if you have to it will be significantly less than what you currently pay for an escrow service), but it also ensures that the participants follow the rules.

Double-Betting Strategy

The double-betting strategy is a mining strategy that has been pre-programmed in the Satoshi reference miner.\(^{53}\) This means that if a miner discovers a block and at the same time another miner discovers a competing block, the miner will not simply switch to the other block. Instead they will keep on mining on their own chain. This because neither of the miners knows which of the two blocks will be the one that the majority of the miners continuing mining.

You can understand that this is not the most optimal way of working, as hashing power and energy are lost when mining several blocks at the same time and when other miners are building on top of conflicting chains. To solve this issue, several algorithms have been proposed, such as DECOR and GHOST+DECOR.

Token Curated Registry

Token Curated Registries are a building block of decentralized applications based on fungible tokens and digital scarcity.\(^{54}\) Two examples of such registries are the adChain registry, which keeps a cryptographically secure record of publisher domain names, and Messari.\(^{55,56}\)

adChain and other registries are listings generated by token holders and these can be anything from hash records to actual detailed records stored in IPFS. The TCR is used to serve as an identity mechanism, which allows advertisers to know something about listed participants without having

\(^{53}\)https://bitslog.com/2014/05/02/decor/
\(^{54}\)https://hackernoon.com/token-curated-registry-tcr-design-patterns-4de6d18efa15
\(^{55}\)https://messari.io/
\(^{56}\)https://publisher.adchain.com/
previous relations with them and exclude fraudulent participants that would like to take advantage.\textsuperscript{57} How do participants become part of the whitelist? They can submit a deposit to become part of the whitelist, after which a challenge period starts. During this challenge period, existing participants can challenge the newcomer and post an equivalent amount against the deposit of the newcomer. In this case, a voting period starts where all the other members of the whitelist can vote on the issue. If the challenger succeeds, they receive special dispensations on top of their own deposit and all the other voters that voted in their favor receive a piece of the newcomers deposit as well (who will not become a member in this case). If the newcomer wins, they receive their deposit back and can eventually become a member. Of course, members can be challenged any point in time if evidence of fraudulent behavior arises. Changes in the deposit requirements of a TCR can lead to the removal of participants if they don’t comply.

You can see that this system helps create some kind of quality label in a decentralized world. Does this mean that TCRs are a flawless system? Of course not, as these implementations have run into some criticism as well.\textsuperscript{58} Aleksandr Bulkin cites the example of blockchain oracles, which do work in his opinion opposite to TCRs. The reason is that oracles require people to bet on (easily) publicly observable information in which honest players are rewarded and dishonest players lose their stakes. Getting the majority of the participants to vote for the wrong answer is incredibly hard, nearly impossible. The key components of the oracle is that there is objective information that can publicly be observed at a low cost. From the moment that this information is no longer publicly available or that there is a considerable cost to verify this information, the participants can be manipulated to no longer support the correct answers. When we extrapolate this logic to TCRs, which are in place to collect and verify information that is difficult to ascertain, we know that there are possible issues with the economic incentives. So, depending on the environment the TCR operates in, it will either be very successful or will fail to bring the certainty that participants in the decentralized network are looking for.

Some Final Remarks

I hope you found this book to be an interesting resource in the world of blockchain technology and development. I tried to provide a first guide, which means that I wasn’t able to explain all concepts, frameworks, and networks in detail. Each of these topics deserves (and often has) complete books of its own.

\textsuperscript{57}\url{https://medium.com/@simondlr/city-walls-bo-taoshi-exploring-the-power-of-token-curated-registries-588f208c17d5}

\textsuperscript{58}\url{https://blog.coinfund.io/curate-this-token-curated-registries-that-dont-work-d76370b77150}
My goal was to introduce these concepts so that, based on your interest, you can explore them further. The Internet is filled with free resources that allow you to learn more, but there are also numerous courses and books that give you more insight into these topics. Websites such as Hackernoon.com, medium.com, and blockgeeks.com offer tons of information that can help you even better understand the world of blockchain and cryptocurrencies.

A second remark that I want to make concerns the fact that this is almost a “historic” artifact. This means that the second I finished this book, there were already certain points that were outdated. An example is the Ethereum network future development plan that is open to change and has already changed. This means that historic information is exactly that. In the same vein, I apologize for the errata in this book. I wrote this with a lot of enthusiasm, but I am sure that there are certain mistakes that I missed and were left behind.

Finally, I would like to add that I am honored you chose to read my book. Thank you for being my reader. If you would like to be in contact, don’t hesitate to connect on LinkedIn or visit my website at www.stijnvanhijfte.com.