Blockchain and Bitcoin – Answering some basic questions

by Valentijn van den Hout - @vvdhout | This is not financial advice.

1. What is a blockchain?

A blockchain is a type of database that stores data in chronologically linked blocks. It only allows the addition of data (as well as reading) and does not provide the option to delete or change data. In other words, if you want to "change" data that is stored you will have to add new data that indicates this change. Because we can see which block is the latest addition we can then decide what the most up to date data is. Coming back to the blocks, data that we want to store on the blockchain is put together in batches (or blocks) and is added to a previous chain of blocks by linking it to the preceding block via its hash. This hash is kind of like the fingerprint of the block; a completely unique code that can be used to identify it. Hence, if we add blocks to this chain in this manner, we end up with a long chain of blocks that each is link to the previous block, allowing us to see the entire history of the database in chronological order.

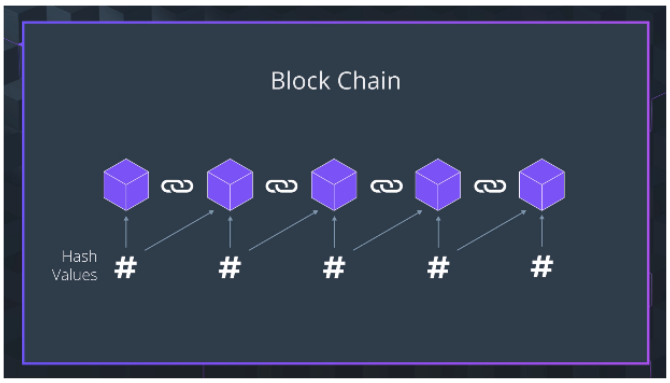

Figure 1: Blockchain data structure (credits to Udacity)

2. What is blockchain technology?

Nowadays, when we talk about blockchain technology we actually are talking about the combination of a blockchain type database and a distributed peer-to-peer network that maintains and interacts with this database (this is also called distributed ledger technology, or DLS). It is the combination of a blockchain database and this p2p network that runs on a protocol (code) that enables the new and innovative functionality that powers cryptocurrencies and blockchain-based applications.

3. What is so special about blockchain technology and why is it innovative?

It enables the trustless storage of data without the need for an intermediary. Being able to store and agree on the validity of data without the need for trust between the actors that are part of the network enables things such as digital currency, transferring ownership of digital assets, identity management, and much more. Not only does it put the control back into the hands of the users, it also means data is no longer stored at a centralized place with a single point of failure or control (e.g. censorship of who can and cannot partake). On top of that, given that trust is no longer an issue, personal data no longer needs to be collected and stored, making data leaks such we have seen more and more frequent lately impossible.

4. Can you explain in more detail how blockchain technology works; Bitcoin, for example?

Since the inception of the internet we have had to deal with an issue of trust when interacting with other actors on the network. We are quite good at dealing with each other on the internet as long as we are not actually transferring something of value to each other. The moment this happens, we need to be sure that the other party acts in a desired way. To make this a bit less abstract, if you have a digital dollar for example which would basically be a piece of code, and you transfer that to me via the internet, I need to know that you have not copied that dollar before you send me the code. If its organized in a way that all assets on the internet are organized (existing in code), you could just copy and copy and copy, and the digital dollar I receive will deplete in value (there now is a possibility of unlimited supply -> no scarcity). This is called the ***double spending*** problem; you could spend the same digital dollar twice. In other words, I need to trust you, something which is quite hard because in many cases you might be anonymous and you know nothing is stopping you from acting maliciously. This (among a few other reasons) is why banks exist. They generate the artificial trust that allows us to transfer value. Just focusing on the currency aspect of things at this moment, banks cooperate to maintain their ledger of account balances. The moment you send money to me via the internet, what really happens is that your bank makes sure your account balance goes down, and my bank makes sure that my balance increases. It is nothing more than an entry in a database. The banks themselves will have sorted out whether they trust you enough to provide you their services. This seems like nothing special, but it makes it possible to “transact” value over vast dimensions of space (i.e. the internet). However, there still is a need for trust in a third-party, namely the banks, and the banks in their turn need a way to trust the individuals (which often means collecting a lot of personal information). The power to manage this wealth is given to the banks, not the individuals who are the supposed owners, and we have to trust the banks to be a well-intentioned and competent custodian (think about the multiple credit bubbles by lending with just fractional reserves). That's not the only issue with the current monetary system that Bitcoin addresses - devaluation of fiat currency by central bank policies being a major one - but more on that later. Bitcoin is the first big and successful implementation of a blockchain p2p network and it focuses solely on the ownership and transferring of Bitcoin (a digital currency). Instead of having a bank hold a centralized ledger (or database) of who owns what, all the nodes (computers) in the distributed network (all over the world) hold the same ledger. Every time a change has to be made to the network (e.g. I want to send Bitcoin from my address to yours), the protocol verifies my identity of the address to send money from (using my private key), checks whether I am allowed to send the amount of Bitcoin (do I own enough Bitcoin), and then updates the ledger on every single node across the network to represent the new state of the network. This is an incredible new way of transferring value from one party to another, without us needing to trust the other party. The protocol uses some clever game theory mechanisms to make sure that those that

maintain the ledger do so in a desirable manner; if they pursue self-interest it is actually good for the network. More details on the inner workings of Bitcoin can be found here:

Satoshi Nakamoto's Bitcoin Whitepaper: A Walk-Through

This is just a brief example of how blockchain technology enables a digital currency such as Bitcoin. However, it also enables the distributed storage and maintenance of data that represents something other than only digital currency transactions. Ethereum, for example, allows developers to store code on the Ethereum blockchain that enables different type of functionality.

5. What is Ethereum, and what is the difference compared to Bitcoin?

Where Bitcoin uses set smart contracts in its protocol that only allows the storage of transactional data (namely transactions of BTC from one address to another), Ethereum (and other similar "Turing-complete" blockchain protocols) enables us to write our own smart contracts. These are pieces of code that can create all sort of variables, store these variables on the blockchain, change these variables, and write functions to be executed by the protocol (Ethereum Virtual Machine). This means we can start to store much more data than just transactional data of a specific currency on the blockchain, something which Ethereum also enables just like Bitcoin (the transfer and tracking of Ether, its native digital currency). However, the Ethereum blockchain operates vastly different than the Bitcoin blockchain, and with that brings big difference between the underlying mechanisms of it's currency. Continuing on the different use cases of these smart contract blockchain protocols, one very popular use case of Ethereum is the tokenization of (digital) assets. We can create a unique token to represent an asset (also called a non-fungible token, or NFT), and transfer this token between addresses to represent ownership. Now we can not only transact value and track ownership in the form of a digital currency, we can also do this for any asset we want to represent with a token, and we can code the logic that a user interacts with to instigate these changes to the blockchain data. Whether an NFT is or is not valuable, is another discussion altogether that warrants its own elaboration: A framework for understanding NFTs and their value

And this is just a very specific example of how smart contracts can be used. In essence, we can create a great deal of blockchain-based applications that regards the storage of data (often ownership tracking is an ideal segment) in a distributed manner.

6. What is Web 3.0?

In the early days of the internet, users only requested data from servers and consumed that data. A domain provided a webpage with information and we were not able to do anything more with that than navigate through it. This is Web 1.0. Then, applications started showing up that enabled interaction and the creation of content by the user, making the user and her data the source of value. Sites like Facebook, YouTube, Wikipedia, and Airbnb among others, became more and more prominent, and all the content and data generated by the users allowed them to extract value from it. They could decide to use it themselves or, and this happens all too often, sell it off to other parties. Web 3.0 is the response to this trend of our own data getting away from us. It is an internet that has been envisioned for a while but has only become possible now that blockchain technology has arrived. Instead of having centralized parties that run applications and collect all its data, we can decentralize and run these applications in a distributed manner. Where blockchain-based computation systems such as the Ethereum Virtual Machine allow for decentralized computation of code, distributed file storage systems such as IPFS (Inter

Planetary File System) allow us to decentralize file storage. Our own personal data can now be linked to our wallet address and be stored encrypted on the blockchain, allowing us to dictate if, when, and which data is made available to an application. We get to choose how our data is used. Combine this with digital currencies that allow the direct transaction of value over the internet between peers and we have an internet that is owned by its users.

7. Could you recap all of this information in a nutshell?

In short, blockchain technology allows us to store data in a distributed manner as such that it is not controlled by any centralized party and does not provide a single point of failure, that allows for identity verification using private and public keys, and "changes" to the data stored without the need to trust other peers on the network. Combining identity verification and data storage makes it a great candidate for tracking and transferring ownership of assets, be it a digital currency, tokens representing physical assets or digital assets (NFTs), personal information, and even interacting with code that is computed by the distributed network (e.g. on the Ethereum EVM).

8. When is blockchain interesting to use over traditional database systems?

Anytime you want data stored to not be controlled by a single party (because of data manipulation, censorship, single point of failure, hackability, etc.) and want a great deal of transparency in "changes" to the data (additions, really), blockchain tech is a great solution. This is why we already see many blockchain-based solutions for anything related to ownership. One of the most simple but powerful applications of the technology is Bitcoin, where the data stored simply represents value and transactions of value between entities. It has created a new money system that is sound, cannot be manipulated, controlled, or censored, puts ownership in the hands of individuals, and is completely digital.

9. Could you explain in more detail why Bitcoin is considered valuable?

There are a lot of great resources that can help you understand the backdrop of the monetary system of the society we currently live in, and if you truly want to grasp the severity of the features I am going to mention next, I recommend you study these topics in more detail (Layered Money by Nik Bhatia is a great start). I hope the previously mentioned benefits of blockchain technology already put some of this into perspective. Bitcoin is valuable because it is a monetary network that is censorship resistant and controlled by no particular entity, allowing its users to have complete ownership over their own wealth and transact value directly to somebody else via the internet, no matter where the person is located or who the person is, without the need for trust between them. The currency is fully divisible and orders of magnitude easier to transport and transfer, and perhaps most important, it has a set monetary policy that guarantees a certain available supply and scarcity. If we compare this to all the other alternatives – for example fiat money and precious metal – it blows all of them out of the water as a better money system. These features have become more obvious and important every single year but especially in the backdrop to the massive amount of money "printing" and currency devaluation by central banks since the start of the COVID-19 pandemic. And lastly, everybody has access. Everybody with an internet connection can become a part of this new technology and use Bitcoin, and there is no way to stop it. Right now we are in the middle of a mass adoption phase of a new money system, and it's absolutely wild to be able to experience it in real-time.

10. That's cool and all, but how do I make money?

Even though a lot of people have a lot of knowledge and experience in the space, most are not actual financial advisors. It's important you don't expect them to be. Nothing in this document is financial advice. The goal is that you have a level of understanding of the space, and in particular the systems or assets you are putting your money into, as such that you feel comfortable seeing the price fluctuate, because it will fluctuate. My own personal opinion is that if you are not willing or able to put in a lot of time researching individual teams, protocols, coins, tokens, what have you, you should probably not invest in them. There are 1000s of different coins out there that all claim a unique value proposition, and even though many will ride the crypto market waves for a while, in the end, a lot are going to fail because they just don't add actual value. Don't try to find the next 1000x coin; if you haven't done the deep research, you are either going to be lucky or wrong. Neither is sustainable. What I do hope is that this document has given you certain insights and intuitions on how the aforementioned most popular protocols work, in particular Bitcoin. As mentioned, Bitcoin is still in an adoption phase with as of this writing around ~2% of the world owning some. If it is going to be what it suggests it can be, Bitcoin penetration will become as widespread as the internet. The price of Bitcoin, leaving aside its fluctuations around the average trend, represents an adoption curve of a completely new technology. This is different than fluctuations in a mature market with a mature asset; there is so much adoption it needs to go through still. Here are some tips for people that have don't have the background in the space but are looking to be a part of it:

1. Expect it to go to 0. **It's not going to happen**, but just make this your assumption. Especially for anybody who has not deeply researched or does not fully understand the protocol, you are going to have doubts and fear pop-up as the price dips and jumps, just because there a certain aspects that are uncertain to you. Expect it to go to 0 and invest only the amount of money that if it were to be gone, you are okay. Consider everything higher than 0 upside. This is just so you can keep your hands off when there is a sell-off. The more you learn about the underlying system and the price dynamics, the more lenient you can be here because your faith will be less fragile to price movements.
2. **Break the assumption that your fiat holding is safe and everything else is a risk**. Your fiat money (USD, EUR, JPY, etc.) – just like everything else – is an asset (using the term loosely here) that you choose to store value in. All assets perform relative to each other. Having money in fiat should be just as much as a choice as putting it in a house, investing in a company, or buying Bitcoin. If the products you buy become more expensive in USD due to inflation (say, for example, the central bank decides to print double the amount of money into existence out of thin air…), your fiat currency is getting devaluated comparatively. Just understand it as a concept. Break the idea that fiat is per definition safe.
3. **Don't try to time the market**. Look long-term. If you believe in the system, it does not matter if you buy at $50,000 or at $45,000. Chances are you don't have years of experience in trading combined with years of experience in blockchain technology and specifically Bitcoin. Again, you are either going to be lucky or wrong, and the worst is if you wait to buy on a dip that never comes (this happens to many, many people).

11. When do I sell my Bitcoin?

See #2 in the previous section.