The Value of Blockchains and Cryptocurrencies
Decentralized Finance #1
The Value of Blockchains and Cryptocurrencies

Decentralized Finance #1

Bitcoin is a groundbreaking invention, enabling two very critical things: the creation of digital assets and the ability to send these digital assets directly to anyone and anything. This is about as big as the invention of the printing press or the steam engine and will change how our societies work on a foundational level.

After reading part one of this three-part series, you will have learned why this is a big deal and how blockchains and how cryptocurrencies work, more specifically:

• Which new technological principles Bitcoin invented
• How Bitcoin and blockchain transactions work
• How Ethereum enhanced the economic and technological foundation Bitcoin built
• How tokens create new economic universes

If you are already familiar with these basics, feel free to skip to part two and three, where we will discuss how to make smart decisions and use decentralized finance (DeFi) to enhance your business. For a broader overview on why we think DeFi is an integral part of the future of businesses, check our insights on 2030 – a different world.

How Bitcoin works

Until the invention of Bitcoin anything digital of value had to be maintained by a trusted party. Being able to create unique virtual coins changes everything. But before we dive into details let's define these terms.

A digital asset is a unique token that cannot be copied, replicated or taken away from anyone without permission.

This is not achieved easily. In a digital environment anything is made of 0 and 1 and can thus be copied without knowing the difference. Because Bitcoin is money, something had to be invented to allow for a digital asset – in this case a virtual coin – that is unique.

This replication problem is usually solved by having a trusted party such as a bank control the ledger or database of who owns what. In Bitcoin that trusted party is obsolete, and that is what changes the game. Instead of the ledger being owned by an entity, which
creates power and dependencies, the ledger now is simply a public good like the air you breathe.

The revolutionary thing about Bitcoins is that the owner, meaning the holder of the key, can send it to any other address without restrictions. Such a transaction contains:

- **Hash**: Unique identifier of transaction
- **Input**: Coins that are sent from a specific address
- **Output**: Specific address that will receive the coins
- **Script & data**: Script with encryption that only the receiver can solve (locking script) and some extra room for data if needed

The script part of Bitcoin is rather simple and old-school with cryptographic functions that allow the owner to sign the transaction by a private key and can easily be verified by a public key. Satoshi Nakamoto (pseudonym of presumed inventor of Bitcoin) purposefully limited the functionality of the script language for security reasons.

As you can see above, the script language of Bitcoin has a set of commands that look like an old school programming language. Most common Bitcoin transactions take an input (some coins) by unlocking them with a private key and then sending them as output to a new address by wrapping the coins into a new math riddle that can only be solved with the private key of that address. This is a very simple, focused and secure script language.

### Why Bitcoin is a big deal

Digital assets and transactions are not new at all. In fact, we have been trading stocks via online brokers for decades now. So, what is special about Bitcoin?

The difference between stock trading, online banking or mobile payment apps and Bitcoin is that – while in both cases the product itself may be digital – the operation and the business is not. Behind the scenes, the centralized examples are all run manually in brick-and-mortar buildings and by people. A blockchain, however, is run by software autonomously. In Bitcoin, operations and governance are exclusively digital and governed autonomously by incentives. This enables entirely new functionalities and increases efficiency by orders of magnitudes.

### 500 years overdue: a leap in technology

In order to create something of value, we need four base technologies:

- Tools
- Communication
- Organization
- Money

Since the industrial revolution, Tools have become machines and robots that have cons-
tantly been re-innovated and improved. On the Communication side, we had language, scripture, the printing press, telephone and television followed by the (somewhat) recent invention of the internet and along with social media. In those two areas technological “leap events” lead to constant re-innovation and improvements until probably yesterday.

Money and Organization, however, are an entirely different story. The last time our organizational systems were re-invented was around the French revolution or when the US was founded. Companies existed then and do so in pretty much the same form structure with the same form of government that were re-fined at that time as well. Likewise, the fiat- and debt-based money we use today came about around the same time the Medici started to rule and transform the culture for Europe with their double book accounting and thus became more powerful than kings.

In short, two of the fundamental technologies of we use to create something of value – Money and Organizations – are older than the invention of the steam engine. Bitcoin fixes this.

When you transfer money for example through mobile payment you are using the services of a company run by humans in manual decision-making processes that govern the operations. This company has to submit to the laws of a country that are in their core made the exact same way as they were half a millennium ago. As a result, governance and organizational processes tend to be slow and inefficient.

Bitcoin invented a new form of organization that is autonomous, automated and digital. So, while digital assets and digital transactions do not seem special – after all what’s the difference of sending money via a Bitcoin or a paypal wallet – the system that runs underneath (a blockchain or a company) are of two technologies from entirely different eras. Blockchain is a new leap in the evolution and development of human technology of a magnitude that we have not seen since the industrial revolution.

Bitcoin does not depend on the social infrastructure that every other organization until its invention depends upon. It runs on its own. Instead of laws Bitcoin is governed by proto-
col rules. These rules are automatically followed because of its incentive structure: the money. The actions of participants are geared by game theory. It works in a way that makes the system secure when actors perform according to their self-interest. Follow the rules and get rewarded, else get ejected. The defense is its decentralization and security is generated as a byproduct from the incentives that participants compete for. Anyone that is attacked or removed from the system will be replaced by someone who is happy to take those incentives. This way the organization of the operations and the money work hand in hand in a decentralized way. Meaning that unlike other institutions, blockchains cannot be controlled or attacked.

One of the most successful projects that tried to build upon and repurpose Bitcoins was the stablecoin Tether (USDT). It was built on the OMNI protocol, which in turn was built on Bitcoin. Then came Vitalik Buterin and thought up the idea to create a more abstract version of that blockchain, one that anything could be built upon. Thus, Ethereum was born.

Essentially the difference is that, while the programming language of Bitcoin was kept extremely restrictive and simple (most likely for security reasons), the language that is used in the script part of the transaction of Ethereum is turing complete. This means that any computer program can be written onto its blockchain. So, in addition to sending coins from one address to another, on Ethereum you can also send a whole program to the blockchain. Ethereum has two types of accounts, contracts (or programs) and user accounts. Once a program is published to the blockchain, it can be executed from anyone by sending a transaction to it. These so called “smart contracts” can have commands, money or both. They can even call other smart contracts to string together many functionalities from various applications. Technically smart contracts can be done on Bitcoin as well but because of the limits of the scripting language this is practically unfeasible.

With Ethereum whole applications can now live on blockchains. As they leverage the same underlying technology as Bitcoin there are a few key differences compared to traditional software applications:

- They run autonomously and cannot be stopped (unless this feature is built on top)
- They operate 100% transparent (the program is visible to anyone)
- They cannot be altered, deleted or changed (unless this feature is built on top)

**Taking it to the next level**

After Bitcoin was invented, clones of it appeared all over the place. Some tried to enhance the technology or to use the blockchain network for a different type of application. Some were pure scams.

Bitcoin and blockchains are so insanely valuable because they modernize Money and Organizations, bringing both of these fundamental technologies from an era of pre-industrial revolution to the modern digital age.
• Anyone can use them without permission, including other smart contracts
• They have no operators or admins that have control or authority over them (unless specifically implemented)
• They run for free but every interaction with them costs a transaction fee (the user pays the operational cost)

Similar to how we could not envision Facebook, Twitter and Uber back in the 90s, this will enable new application functionalities that we may not be able to imagine just yet. We already see a glimpse of what will soon be possible in DeFi applications and the metaverse that is being built upon, most recently the cultural adoption with NFTs.

**Tokens and ICOs**

Simply put, a token is a cryptocurrency. However, in addition to being money, it contains a smart contract allowing for extra functionalities such as voting rights or the ownership over digital and physical assets. Tokens are important because they are always the financial foundation of digital applications. Bitcoin and any blockchain need tokens for incentives and governance.

Before Ethereum, in order to make a new token, developers needed to create a whole new blockchain. Now, however, all you need is a tiny piece of code you can send to the Ethereum blockchain and, voila, a new token is created. Thus, it is not surprising the first thing people did on Ethereum was to create tokens. Thousands of them popped up left and right. Most of these tokens were used to raise funds for companies. This funding is called ICO (Initial Coin Offering) analogous to IPO (Initial Public Offering).

Most ICOs worked liked this: A team created a company, issued a token and then sold the tokens to raise funds, promising some future outcome/product. That, however, is the classic form of a security, like a stock or bond and is regulated in every country you can think of. Moreover, one is not allowed to sell securities except via regulated markets and processes.

More often than not the ICOs in the 2016 to 2017 bull run were scammy, fraudulent or naively run illegally. The issue was the company. By using the legacy organizational structure you are inheriting the legacy legal system.
Tokens had their own little bubble in 2017 with the ICO craze. Tokens are still the foundation for all dApps but much better distribution models exist. Thus ICOs are fairly rare these days. | Source: Statistica

The utility of Ethereum grows with every innovation. New protocols get built continuously and are being used. This is best seen by the number of contract calls that are continuously rising. | Source: Glassnode
People did not understand that it is not only the token that needs to be digital: the organizational structure must to be digital as well to ensure you do not have to deal with the overhead of the legacy world.

**In order to do tokens right, they need to not be controlled by a company. Instead, they should control the decentralized application.**

Today ICOs are not very common anymore as there usually are better ways to distribute coins for both investors and users but they are a perfect example how of using a new technology (ICO) the same way as an old technology (IPO) is usually just worse. The issue with this approach is that the same laws that apply for stocks do also apply for tokens, thus the underlying system has not yet changed.

We will cover better ways to distribute tokens more in-depth in the next part. For now it is important to retain that tokens are the base of all good Decentralized Applications (dApps) and blockchains rely on. Bitcoin, Ethereum and all the other great DeFi protocols simply would not work without them.

So far, we have covered the early history of blockchains, and more importantly, why and how they fundamentally changed the way organizations may work.

Bitcoin and blockchain can seem complex at first and sound like a buzz word that is doomed to irrelevance. Yet they have invented technological foundations that allow for digital currencies and economies. Tokens provide the incentives to run the decentralized organizations that govern these new universes. This creates an ecosystem that works independently from the social structures we have relied upon so far and similarly creates a whole new digital universe. And that is why, all of a sudden, so much new value is created.

Since then financial services emerged as a first layer of applications that are being built on top of blockchains, known as Decentralized Finance, or short, DeFi.

In the next part, we will explain what makes these killer apps so groundbreaking and why traditional financial markets are increasingly superseded by their digital counterparts.
About the authors

**Philipp Knirck** studied Business Informatics and brings over 15 years of consulting experience in Europe, America, and the Middle East across industries. Now, he is mainly active in the US, exploring new markets, building successful teams and achieving measurable results. His specialties are blockchains, cryptocurrencies and NFTs. He consults organizations on how to implement blockchain technology into their core processes in a way that creates value.

**Melanie Zollinger** holds a master's degree in Business and Economics. She has over 7 years of experience in Marketing in the consulting industry and occasionally accompanies IT projects from a communications aspect. She has co-written numerous specialist articles on IT project management, digital transformation and industry trends, validation and compliance topics, and most recently on blockchains and cryptocurrencies.