14.4. Cryptocurrency

Improving the world through anonymity?

> Ethereum is a community-driven technology that drives the cryptocurrency Ether (ETH) and thousands of other applications.
>
> Ethereum advertising promise

The fear of government abuse of power, that makes people cling to cash money, cannot really be prevented by cash. Since salary payments are made month after month using book money, book money must always be converted into cash. Cash can be used to pay anonymously, but an account blocking can block access to cash. Individuals (but also boycotted states) remain powerless against such measures. In order to at least protect the freedom of individuals, Bitcoin was developed in 2008 as the first cryptocurrency.

Cryptocurrencies are means of payment that are created by computer algorithms outside of government control. All transfers are stored in a decentralized computer network. Since there is no central bank, every transfer is made directly from the account of the person paying to the account of the person receiving it. State or other power structures have no way of blocking accounts or preventing payments. Cryptocurrencies are therefore an attempt to secure individual freedom.

The success story of Bitcoin began when WikiLeaks was blocked from all payment channels in 2010 by arbitrary government action. This arbitrary action was a reaction to the publication of documents that revealed war crimes committed by the US Army. Bitcoin offered the opportunity to make payments to WikiLeaks beyond government blockades and thus support the platform. The incriminating documents had been sent to WikiLeaks anonymously and in encrypted form by whistleblower Chelsea Elizabeth Manning.

Even before the development of cryptocurrencies, cryptographic methods had been developed to enable data transfers without anyone being able to read them without authorization. This development was intended, among other things, to help civil rights groups to avoid government surveillance in their work. Encrypted data transfer later developed into an internet in which everyone can be anonymous, the so-called darknet. It is known that the darknet is not only used by whistleblowers and civil rights groups today, but is also a criminal hotbed. The anonymity of the darknet has also created a cyberspace for drug and weapons trafficking as well as sexual crime. To ensure the anonymity of transactions, payments on the darknet are of course made with cryptocurrency.

This shows the dilemma of the fight for freedom on the internet. It is perfectly understandable that everyone who wants to uncover state abuse of power and illegal machinations today uses anonymous and encrypted data transfers. But the abuse of these very structures by private criminal individuals and organizations reveals that the fight for individual freedom cannot be won in this way. It is essential to create state structures that are truly democratic, so that grievances can be pointed out openly at any time. The path to this kind of freedom is undoubtedly much more difficult to fight for and defend. But real freedom can only be achieved on this rocky road.

Cryptocurrencies themselves are also caught in the dilemma. They enable payments that are not processed by state-controlled financial institutions. All transactions are thus beyond state arbitrariness and also beyond state control. As a result of the supposedly objective generation of crypto money by computer algorithms, all crypto currencies also lack any reference to real value creation through the production of goods. It is therefore no coincidence that crypto currencies have now developed into objects of speculation. Crypto money is only accepted as a means of payment in very specific political and criminal markets. The fact that it

fulfills this function of payment is a result of its acceptance as a means of speculation.[1] It can only function as a means of payment because crypto money can be exchanged for common national currencies at any time on Internet exchanges.

Crypto money enables peer-to-peer payments, i.e. direct payments, without the mediation of a real bank. But it hardly enables shopping in real shops. Crypto currencies are not suitable as everyday means of payment because their exchange rate (i.e. purchasing power) is sometimes subject to extreme fluctuations. However, a good means of payment is expected to be stable in value. However, today's crypto currencies cannot achieve this as long as the creation of money is not linked to real value creation.

I see one reason for this in the fact that cryptocurrencies were and are being developed by people who spend a lot of time in the virtual world and have comparatively little connection to the real world of goods production. The high financial prestige and the great structural importance that IT knowledge has within today's organization of production and society lead to the belief that all problems can be solved technically. The idea that computer algorithms and artificial intelligence can solve all of humanity's problems seems to be widespread, especially among IT experts. This belief will probably only be shaken when food production drops drastically as a result of the ecological destruction of soil, insects and water sources. Only then will it become clear that pure data management without reference to the real world has no foundation and cannot offer viable solutions to the problems at hand.

The high energy consumption of blockchain technology[2] is already casting doubt on the future viability of cryptocurrencies. The reason for the high energy consumption is that every computer that participates in the blockchain system must constantly solve cryptographic tasks, which requires continuous computing power and therefore energy. The energy consumption for Bitcoin is estimated to be roughly equivalent to the annual consumption of a country such as Denmark or Sweden. The continuous occupation of all computers in the blockchain system with complicated mathematical puzzles is intended to prevent the decentralized blockchain network from being hijacked. This would happen if a single person controlled more than 50% of all computers in the blockchain system and thereby gained the power to decide which transactions are valid and which are not. Such control could, for example, be abused to transfer money from the system to one's own account, then exchange it for local currency and thus withdraw it from the system. This control and security mechanism is called *proof of work*.

There is now a new energy-saving security system for cryptocurrencies. This system, called *proof of stake*, replaces the solving of mathematical puzzles with a kind of lottery. It is said to save up to 99% energy. But this system favors those who provide many computers for the crypto system.iii It therefore promotes the accumulation of resources and thus the concentration of power in a few hands. The algorithm-based democracy of the blockchain can therefore, like capitalist offline democracy, be manipulated and ultimately destroyed by the concentration of economic resources. A permanently viable democracy therefore requires the prevention of economic overaccumulation in any case. We therefore urgently need better solutions to create democratic monetary systems.

It is not enough for individuals to evade state control in order to gain freedom. It is necessary to subordinate state control bodies to democratic control. This is the only way to truly achieve freedom.

---

1 Cryptocurrencies experienced a brief but huge hype between 2016 and 2018 thanks to the Ethereum platform, through which - as in any chain letter system - a few people became very rich because many lost a lot of money. In total, around 400 billion is said to have flowed into newly launched cryptocurrencies (in so-called initial coin offerings, or ICOs for short) worldwide.
This hype is very reminiscent of the founders' frenzy and founders' crash in Germany at the end of the 19th century. When the credit money system was introduced in Germany in 1870 (relatively late) with the new joint-stock banking law, banks and joint-stock companies sprang up like mushrooms. The new credit institutions financed some dubious companies that were not interested in serious business but in quick profits. In 1873, many of these companies went bankrupt in a financial crisis so named “Gründerkrach” (founder crisis). As a result, numerous banks collapsed. All those who had invested their money in these banks were cheated.

2 To put it simply, a blockchain is a large, decentralized database to which new data blocks are constantly being added.