Introduction

The last decade has been characterised by a proliferation of projects that use new technologies to launch various forms of “crypto assets”. This development has been inspired by the initial combination of cryptographic methods and economic incentives to construct a decentralised register of data, called “blockchain”. The first and most prominent of these crypto assets is the Bitcoin network, which launched in 2008. Bitcoin and a sub-class of blockchain-based projects closely inspired by it have received widespread public attention and are being referred to as “cryptocurrencies”.

The term “cryptocurrencies” triggers diverse associations in individuals. It may be seen as a decentralised form of digital money that is severed from the influence of centralised institutions (both public and private). This view is often accompanied by sanguine comments about a society in which the role of the government is reduced to a minimum. By contrast, some might, for the same reason, associate it particularly with illicit behaviour. Indeed, this perspective is what led Nobel Laureate Joseph Stiglitz to argue in an interview with CNBC in 2019¹ that cryptocurrencies should be shut down. Others might simply regard it as yet another speculative asset to increase their wealth. This aspect is understandable, considering that in May 2010 two pizzas were sold for 10,000 Bitcoins (BTC)² and that one BTC traded for over 34,000 USD at the beginning of January 2021. A different perspective results from a focus on the underlying technology of cryptocurrencies – the blockchain, the potential of which (and consequently that of cryptocurrencies) can be analysed from several angles. The technology can, for example, be seen from an efficiency lens (i.e. saving transaction costs) or from an institutional lens (i.e. competing with existing institutions in the facilitation of transactions). These two perspectives are likely to be intertwined, as different institutions can exhibit different magnitudes of transaction costs.

In its essence, however, the term cryptocurrencies insinuates some relation to the concept of money (in particular, digital money). Digital money has existed for quite some time now. In fact, the majority of the existing money supply consists of digital money, since (in addition

¹ www.cnbc.com/2019/05/02/joseph-stiglitz-we-should-shutdown-the-cryptocurrencies.html
² https://bitcointalk.org/index.php?topic=137.msg1195#msg1195
to physical notes and coins), the majority of means of payments in official currency consists of funds in bank deposits. But an intriguing question is what makes cryptocurrencies as potential “digital money” so interesting. Part of the answer is related to the concept of transaction costs and the notion of trust. Transaction costs were introduced into the economic doctrine by Ronald Coase in 1937 and later extended by, for example, Oliver Williamson (1985) and Douglass North (1990). To keep things simple, it suffices to note that the coordination of transactions can incur different costs. These include, for example, costs of contract negotiation (and renegotiation), contract writing, contract enforcement, opportunistic behaviour, information asymmetries, price discovery, and unverifiable information. Different institutions may incur these costs to different degrees. Whenever one institution can coordinate transactions at lower costs than another institution, it can be regarded as being more efficient – and more efficient institutions tend to supersede less efficient ones.

Transaction costs in the traditional monetary and financial systems can often be related to dependence on third parties (e.g. central banks, commercial banks, courts) to facilitate transactions: they are needed to safely store money, ensure access to stored money, process and validate transactions, provide security mechanisms in case of unforeseen events, and guarantee the value of money. These third parties have to be trusted to fulfil their legal and contractual obligations correctly and truthfully. Additionally, the legal and economic system have to be trusted to deter or sanction any violations. This seems to be particularly relevant with respect to financial systems. Zingales (2015) raised awareness about the dichotomy between the scientific community’s and general public’s opinion on the US financial system. The former group is usually characterised by a significantly more positive stance than the latter. The general public commonly associates financial activities with rent-seeking behaviour – and such behaviour increases transaction costs. Cryptocurrencies were arguably born out of a desire to escape the dependence on trusting centralised third parties. This dependence bothered Satoshi Nakamoto, founder of the Bitcoin network, who had the vision to create “a purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution” (2008: 1).

While such a decentralised system of record-keeping does indeed eliminate the need to rely on certain centralised third parties to process and validate transactions, this does not imply that this is achieved in a costless manner. In this chapter, we will discuss in what way cryptocurrencies may change transaction costs as well as the need to trust others. Additionally, we argue that associated costs might simply be transformed or borne by other parties than under traditional arrangements. Moreover, even assuming that cryptocurrencies facilitate more transactions at lower costs, the question remains whether a “the more the better” attitude is necessarily a desirable outcome. Be that as it may, since its creation, the Bitcoin network has been at the centre of many debates about the future of our monetary system. This contribution tries to bring some of these debates into perspective.

The rest of this chapter is structured as follows. The next part provides an introduction to the techno-economic characteristics of crypto assets and the blockchain technology. Afterwards, we discuss those crypto assets referred to as cryptocurrencies in the context of money and monetary systems, while the fourth part considers further types of crypto assets designed to provide alternative products and processes in the financial sector; special attention is given to the concepts of tokenisation and decentralised finance (DeFi). The following section discusses the conditions under which individuals choose to transact with each other. It questions the notion that more transactions (due to lower transaction costs) necessarily make all transacting parties better off. Finally, the last section provides concluding remarks.
The techno-economic properties of crypto assets

Before discussing the potential of crypto assets in the context of the monetary and/or financial sector, it is instructive to devote a few pages to the functioning of crypto assets. In particular, this requires an understanding of blockchains – the technology underpinning them. The first blockchain protocol was proposed in the Bitcoin white paper. Nakamoto (2008) noted that previous attempts to create peer-to-peer payment systems that did not rely on centralised institutions failed to solve the double-spending problem. This problem emerges out of inherent properties of digital objects: they can easily be copied. To prevent somebody from copying and subsequently spending the same digital coin twice, transactions have to be monitored and validated. This can be done by traditional third parties. In a decentralised administration system, things get more complicated. Firstly, decentralised consensus on the validity of transactions has to be reached. Secondly, information on processed transactions needs to be distributed in the network and publicly accessible. Finally, transactions must be irreversible. Nakamoto (2008), for the first time, proposed a distributed and decentralised system that meets these requirements and solves the double-spending problem: the Bitcoin blockchain.

Satoshi Nakamoto’s innovation utilises a combination of cryptography and economic incentive schemes. A simple decentralised consensus mechanism based on computational effort (proof of work) incentivises and ensures correct validation of transactions by special network participants (miners). Validated transactions are subsequently combined into blocks and added to the system. Every new block is uniquely linked to the previous one, thus creating an ever-growing chain of blocks – the blockchain. Information on the state of the blockchain and information contained within transactions is distributed over myriad storage devices (nodes) of network participants. Cryptography ensures that transactions cannot be reversed. Transactions recorded on the blockchain are thus distributed, decentralised, and immutable. These characteristics are the result of a clever combination of economic incentives and cryptography. The following paragraphs introduce the concepts employed and clarify some of the terminology used in this context.

Decentralised consensus mechanisms are the backbone of the blockchain technology. Their underlying models are based on economics, and since the advent of the Bitcoin network, various concepts have been proposed. The proof-of-work (PoW) based consensus mechanism, proposed by Nakamoto (2008), remains the most prominent up to date, although different concepts are gaining momentum due to inherent shortcomings of this mechanism. But before we elaborate on this topic, we have to understand the concept of the PoW consensus protocol. In the PoW system, “miners” try to solve a mathematical problem that can only be solved by a trial-and-error process through the exertion of computational effort. They are incentivised to exert this effort because the first one to publish a correct solution in the network gets rewarded with a pre-specified amount of BTC, the native cryptocurrency of the Bitcoin network. The protocol publishes a new variant of the problem to be solved in regular time intervals. Once a solution has been found for a new problem variant, recently instructed transactions by Bitcoin owners are validated and get added to the chain. This mechanism creates a competition between miners to validate transactions (to be the first to solve the problem).

To ensure that BTC are not double spent, the network draws on the information contained in all past transactions included in the blockchain. As a result, the newest block is connected to all previous blocks. Such a system is astonishingly robust against malicious attacks. To trick the system (e.g. by altering past transactions to one’s benefit), one would have to convince the whole network of a different “truth”. The truth in the Bitcoin network (and almost any other blockchain system) is the longest chain of blocks. To change a transaction, a new chain (a fork)
would have to be computed that ultimately outpaces the growth rate of the existing chain. This can only be achieved by exerting more computing power than all other miners have together. Thus, manipulating past blocks is extremely difficult, and the task becomes harder as the chain of blocks grows.

This is probably as good a point as any for the introduction of Alice and Bob, two fictional characters that are often used to ease the understanding of concepts related to cryptography (DuPont and Cattapan, n.d.). Imagine Alice wants to send some BTC to Bob, and suppose that both characters are already participating in the Bitcoin network. That means that Alice and Bob possess both a public and a private key. The former identifies the two nodes (although no personal information is provided) and the latter is used to sign transactions. Alice creates a transaction with the amount of BTC she wants to send to Bob together with his public key. She then uses her private key to sign the transaction and her public key to publicly verify that she issued the transaction. Now that the transaction has been proposed to the network, miners start exerting computational effort to validate it. Once this has been achieved, the transaction is added to the blockchain. Now suppose that Alice wanted to trick the system and spend the same BTC again. Since her transaction to Bob has already been validated, she would have to convince the entire network of a different truth. To do this, she would have to validate the transaction containing this alternative truth herself. However, as all transactions are linked to all previous transactions, she would have to redo the PoW on every transaction contained in the currently used blockchain (i.e. the longest chain), which is quite unlikely for a single person to achieve.

However, Nakamoto already acknowledged a potential risk of centralisation in the Bitcoin white paper. He therefore stated that, for the network to function as intended, more than half of the entire network’s computing power must be controlled by honest network participants. This potential flaw was later emphasised by Vitalik Buterin, founder of the Ethereum blockchain, the second largest blockchain network. Buterin (2016) pointed out that a consortium of malicious nodes might collude to create a different truth in the blockchain. This consortium might heavily invest in equipment specially developed to perform the required computational tasks most efficiently. Due to economies of scale, such a consortium might gain an advantage over regular nodes and thus be difficult to compete against. Criticisms from a different avenue concern the huge amount of electricity consumed by consensus mechanisms based on computational proof. Ethereum Wiki (2020) therefore proposed a proof-of-stake (PoS) based consensus mechanism that is more robust against centralisation.3 The PoS relies on economic stakes rather than computational effort to validate transactions. Nodes can lock some of their native cryptocurrency (put it at stake) in exchange for a right to vote on which transactions are validated and included into the system. The power of a vote is directly related to the economic value of the stake at a 1:1 ratio. This removes a potential centralisation risk due to economies of scale. PoS is additionally strengthened by a combination of economic rewards and penalties. Nodes receive some kind of interest on their capital at stake. They also get a proportion of fees associated with transactions. Penalties can take the form of a loss of the entire capital at stake.4 Ultimately, PoS is expected to be more robust than PoW due to more robust economic incentive schemes. On top of this, PoS is much more environmentally friendly, as it does not rely on electricity-consuming computational effort.

But the blockchain technology has far more to offer than the possibility of a peer-to-peer payment system (such as Bitcoin). This has inspired the development of the Ethereum blockchain.

---

3 The proof-of-stake protocol is currently being implemented on the Ethereum blockchain.
4 These are much more severe punishments than in a PoW system, where the source of the miners’ power, i.e. computer hardware, cannot be simply taken from them.
The basic idea behind the project was to provide a blockchain system which understood a general-purpose programming language. Put differently, anybody with the required programming skills could create their own blockchain-based application, which would automatically benefit from the specific characteristics of the blockchain technology (i.e. that it is distributed, decentralised, and immutable). A particularly important aspect of the Ethereum blockchain is the extended potential of so-called smart contracts. These are, in essence, scripts that translate obligations of two or more parties with respect to information stored on a blockchain in a transaction as agreed in a contract. These scripts can be encoded in transactions and are executed autonomously. Smart contracts themselves can execute further transactions and even additional smart contracts. Usually, the autonomous execution of smart contracts is tied to the observation of pre-specified events (i.e. information). Since these scripts are implemented on top of the blockchain technology, they also exhibit all of its features: they are immutable, distributed, and decentralised (for example, Buterin 2013). Thus, they have the potential to facilitate trust (e.g. in the fulfilment of future payment obligations within contracts) between two unknown parties who want to transact with each other in a truly decentralised way.

Potential use cases for smart contracts range from automatic execution of financial contracts to the transfer of property rights (we will encounter specific examples later on). They can, for example, be programmed to hold a specified amount of crypto assets in escrow and transfer them to a specified address upon the observation of a specific event, e.g. the transfer of another cryptocurrency or the delivery of a good or service. Theoretically, legal disputes over non-fulfilment of contracts can thus be precluded a priori, as the smart contract – once it is triggered – executes its code inexorably and the transaction cannot be altered ex-post. Smart contracts thus have the potential to economise on transaction costs by making traditional intermediaries (e.g. banks) superfluous and to enable more transactions between individuals by increased trust in contract fulfilment. While smart contracts are neither perfect (complete) contracts in an economic sense (all possible contingencies are accounted for) nor contracts in a legal sense, their ability to automatically enforce contractual obligations referring to information recorded on the blockchain can be considered an alternative to relying on centralised institutions (e.g. courts) as enforcement intermediaries or informal norms. Irreversibility, for example, is beneficial in cases in which one party undertakes asset-specific investments, i.e. investments that have no value outside this relation, and the other party is characterised by rent-seeking behaviour, i.e. by insisting on renegotiating the initial contract ex-post (this point has been persuasively made by Oliver Williamson, for example, 1985). Although it is worth noting that irreversibility of agreements need not always be beneficial, e.g. when outcomes of completed transactions differ from initial expectations held by at least one of the parties involved.

Much of the discussion surrounding the potential of the blockchain and crypto assets is based on a common narrative: trust. The blockchain technology quite generally tries to reduce the need to trust third parties (e.g. banks, courts, etc.) to fulfil their obligations and not to act opportunistically. Additionally, transactions might be executed more efficiently without

---

5 Even though Ethereum is one of the most prominent platforms for smart contracts, its founder, Vitalik Buterin (2018), seemingly regrets the use of the term “smart contract”. His reasoning is that the term relates the concept of self-executing code too much to legal aspects of contracts. He goes on to state that a more technical term, such as “persistent code”, might have better defined its purpose.

6 Any real-world event has to be verified by so-called oracles, which can provide off-chain information in a decentralised way. See, for example, Ellis et al. (2017), who discuss the oracle Chainlink.

7 Paul Milgrom and John Roberts (1992: 127) describe a complete contract as one that “would specify precisely what each party is to do in every possible contingency (including those where the contract’s terms are violated) so that each party individually finds it optimal to abide by the contract’s terms”.

---

Tobias Eibinger, Ernst Brudna, Beat Weber
additional intermediary steps. This is why many observers see crypto assets as promising and many of their innovations as having the potential to shape our society in the long run. The following sections will discuss two such areas in some detail: the monetary system and finance.

Cryptocurrencies in the context of money and monetary systems

The term “cryptocurrencies” suggests to some degree that the technology might be interpreted as money. After all, Bitcoin contains the term “coin” in its name and was devised as a peer-to-peer electronic cash system, with an elaborate architecture designed to facilitate payments. Its predefined supply limit evokes the limited supply of natural resources like gold, which has a long history of being used as a material to mint coins and backing asset in monetary systems. But whether BTC were intended to challenge traditional money directly is unclear. Moreover, the simple question whether cryptocurrencies in general, and BTC in particular, may be defined as money is not straightforward.

In a capitalist market economy with an elaborate division of labour, most people depend on permanent economic activity in order to earn and spend income. Economic activity under these circumstances requires money to perform three functions (see Krugman et al. 2012, in the place of many). Firstly, it has to function as a unit of account – a stable yardstick to measure and compare prices of goods, services, and contractual payment obligations (wages, debt, taxes). Secondly, it has to be widely accepted as a medium of exchange. Thirdly, money has to be stable enough over time to serve as a basic means to store value in liquid form. Money with these three functions serves as a basic infrastructure for markets to operate. Currently, money takes the form of various national currencies, most of which monopolise monetary functions in their own geographic area, some of them also across borders.

Crypto markets and user behaviour

Now, can cryptocurrencies be described as money according to the three functionalities mentioned? As a first step towards answering this question, we can observe actual user behaviour with regard to cryptocurrencies. Do crypto owners actually treat cryptocurrencies like money, as characterised by the three functions referred to earlier? A key observation about crypto assets like Bitcoin is that their market value is subject to huge fluctuations. The value of one BTC, for example, might change considerably over a single day, making it neither a stable yardstick nor a predictable store of value. Whatever their technical potential as a means of payment, most current crypto users treat cryptocurrencies like other goods and assets priced and traded on markets for stores of value and collector items within existing official currency networks, not as rival currencies: the market value of cryptocurrencies on trading platforms is measured in official currency.

Some merchants may accept them as optional means of payment, but to avoid exchange rate risk, they only rarely set prices of their goods and services in crypto units of account. And except in cases where payment in official currency is no option (e.g. in illicit transactions), spending cryptocurrencies is usually unattractive for their voluntary owners, because it would involve the opportunity cost of missing out on a potential future appreciation of their market value. Additional hurdles may include transaction fees and capacity limits of blockchain payments as well as reduced price transparency, as crypto owners are faced with price in official

\[\text{For a time, series of Bitcoin prices, see: www.coindesk.com/price/bitcoin.}\]
currencies. Ultimately, we can conclude that so far, crypto assets like Bitcoin satisfy the functions of money at best partially and theoretically.

**External determinants of cryptocurrencies’ competitiveness: network effects on currency markets**

To explain the failure of Bitcoin-like cryptocurrencies to rival existing currencies so far, reasons both external and internal to cryptocurrencies can be considered. Central external reasons encompass network effects. Networks characterised by such effects convey various benefits on their users, and these benefits rise with the quantity of membership and the quality of services provided (one may think of languages, telephone networks, social media). That is why the individual choice of joining a network is different to the individual choice concerning competing ordinary consumption goods, which can be chosen and consumed by individuals without regard to what other people are doing. To see, how such effects make big and stable currencies robust to competition in currency markets, note that individual choice among competing currencies is about the decision to join a network with associated qualitative as well as quantitative benefits. The prime quality feature of a currency network is access to the three functions of money outlined earlier.

With respect to quantity of membership, there are benefits for every member of a large network: a large membership in a currency network reduces participants’ transaction costs for negotiating and comparing prices, agreeing on a means of payment among transaction partners, exchange rate risks among different means of payment, collecting information to form expectations about the future value of the currency, search costs for transaction partners accepting means of payment in a particular currency, etc. These transaction costs favour a monopoly position of a currency in its own jurisdiction and pose disincentives for members to leave an existing currency network and join a different one. Such networks can be challenged by bigger foreign currency networks of superior quality. But they are particularly robust against completely new potential networks, such as the one offered by several crypto assets.

**Money and cryptocurrencies: internal design differences**

In addition to the self-supporting features of a currency subject to network effects, the public sector behind official currencies can internally strengthen its own network against competition. Such measures encompass an exclusive acceptance of official currency for tax and administrative payments and legal tender laws normalising official currency as the standard for payments. On top of that, a number of elaborate institutional safeguards have been developed to stabilise the value of an official currency in terms of a predictable evolution of domestic purchasing power of money (as measured by the evolution of prices of goods and services) over time. This necessitates avoiding both excessive inflation and deflation.9

In such a system, centralised but controlled intermediaries play a key role. Cryptocurrencies usually try to avoid a dependence on (trusting) such parties. So, it is important to understand what kind of trust contemporary money requires. It is trust in the solidity of a set of interrelated

---

9 Deflation might be undesirable due to several reasons. In an economy-wide deflation, all or most prices are subject to downward pressure. This can lead to an economy-wide self-feeding downward spiral between falling prices of goods and falling incomes (wages and profits from goods production), hurting economic activity and future planning. At the same time, claims of creditors on debtors remain unchanged, with falling debtor income resulting in an increasing debt burden (see, for example, Krugman 2010).
obligations and responsibilities designed to make any violations of these obligations difficult and costly. In today’s major currency areas, a number of legal obligations and economic incentives are in place to promote monetary stability and general acceptance of domestic currencies (Weber 2018).

**Legal obligations.** While issuing of banknotes and coins in official currency is monopolised by the central bank, issuing deposits in official currency is not. Whatever its form, money is an obligation for its issuer. A central bank is liable for accepting banknotes or deposits issued at nominal value when they are repaid after circulation (to discharge third-party debt obligations acquired in the act of money creation). The public sector is liable for accepting money in domestic currency to discharge tax payment obligations of users. Commercial banks are liable to redeem customer deposits in notes and coins issued by the central bank on demand.

The central bank’s objectives as well as their room of manoeuvre is determined by legal mandates. Current mandates in major currency areas focus on stability of prices and macroeconomic performance, granting central banks operational independence to use instruments in a way to achieve their tasks. While central banks accept government debt from their customers in the banking sector in exchange for new money, there are legal prohibitions against direct access of governments to central bank finance in major currency areas. More generally, democratic control procedures are in place (legal constitution and independent courts, parliaments, elections, etc.) to keep government misbehaviour in check. Finally, note that in most jurisdictions, legal tender laws do not outlaw the use of other currencies in private transactions but establish official currency as a standard.

**Economic incentives.** Before new money can circulate among users in the economy, its creation is conditional on the issuer (central bank) receiving an obligation for future repayment from a debtor at the prevailing interest rate. This generally incentivises responsible economic use of new money. With money creation being demand-determined, there is no way for the central bank to increase the money supply without counterparties willing and able to fulfil the central bank’s conditions. Although money is not a legal claim on valuable goods supplied by private producers, its status as being a claim on sizeable and reliable issuers makes it attractive for general acceptance in the economy for private transactions in markets.

The negative fiscal and legitimacy implications of macroeconomic instability associated with high inflation or deflation provide a counterweight to incentives for governments to either promote high inflation as a way to erode the value of government debt and increase tax receipts or to promote deflation by excessive hoarding of tax revenue. Market competition is envisaged to impose discipline on prices, wages, and credit. This also applies to currencies in the global economy: liberalised cross-border movement of capital increases the threat of substitution of domestic currency if the superiority of foreign currencies in terms of membership size and stability becomes large enough for domestic users to incur the transaction costs involved in collective currency switching.

**Crypto design compared to official currency**

Issuing entities of official currency can adjust the terms and conditions for money creation and backing assets to let supply adjust to changes in demand with the objective to stabilise the value of money. Blockchain-based systems rest on a different set of value propositions, inspired by a desire to avoid the use of centralised intermediaries that can exert an influence on money and its users. To achieve this objective, blockchain protocols largely rely on algorithms, and these may

---

vary substantially. The wave of crypto projects inspired by the appearance of Bitcoin has been characterised by the emergence of new types of crypto assets that are intended to serve a specialised subset of potential use cases and operate with different supply rules. Among these are stable coins and crypto assets intended to serve various non-currency purposes (such as Ethereum).

Bitcoin-like cryptocurrencies depend on reward-based decentralised operations to produce a supply of “coins” that consist of data on blockchain with no external reference (e.g. a backing asset) and no centralised system owner or issuer. In other words, Bitcoin-like cryptocurrencies are no one’s liability. The supply of these “coins” is directed by pre-set parameters, which differ in their degree of flexibility across cryptocurrencies. Prices are thus solely left to the interplay between the fraction of the supply of “coins” that is currently offered for sale and the current demand on crypto markets.

In the case of the Bitcoin protocol, the supply is limited to a total of 21 million BTC that can be mined. At the end of 2020, around 18.5 million BTC have been created, and it is estimated that the last subunits of BTC will be created around the year 2140. Once this last unit is created, the supply of Bitcoin cannot be expanded according to the protocol, unless miners agree on changing it. For the blockchain to continue to work after this point, it is expected that Bitcoin users must be prepared to pay considerable fees for transactions to enable continued cost recovery by miners (Hayes 2020). Although future demand for Bitcoin is highly uncertain, supporters hope that continued new demand for Bitcoin on crypto markets after the supply has reached its upper limit will contribute to continued appreciation of its market value in official currency.

A predetermined supply schedule of a good, asset, or currency with no claim or backing asset behind it and no information about (or anchor for) the future evolution of demand almost inevitably results in fluctuating market value in an economic system where market value is determined by the interaction of supply and demand. This is a typical feature of markets for collector items and other assets in limited supply and may incite users to include crypto assets in their portfolio. But it will in all likelihood undermine the asset’s competitiveness against stable major currencies.

Stable coins explore mechanisms to improve on the value stability of crypto assets. Some such mechanisms provide services close to an official currency within the crypto sector; some of them aim at entering the global market for mainstream payment services. Some stable coins have decided to recede on the decentralisation principle on which Bitcoin is based in order to profit from improvements requiring centralised responsibility. Most variants of these are vehicles for tying the value of crypto currencies to official currencies, trying to import or free ride on their stability mechanisms instead of offering an alternative currency. Furthermore, some corporate actors and even central banks have started to explore the possible integration of some features of blockchain and crypto assets into potential future payment instruments issued by centralised intermediaries.

The supply management of stable coins is based on more stability-oriented supply rules compared to volatile cryptocurrencies (such as Bitcoin). The mechanisms governing the supply of such stable coins can broadly be categorised as asset-backed and algorithmic. Asset-backed systems either aim at maintaining a peg to official currencies (e.g. USD) or to crypto-assets (e.g. ETH), while algorithmic stable coins rely on smart contract protocols to minimise price volatility (Hileman 2019). One prominent asset-backed stable coin is Tether, which aims to maintain a 1:1 peg to the USD. According to the company issuing the crypto coin, each native USDT is backed by an official USD in reserves. Such a system relies on centralised third parties to maintain the peg and can therefore be described as a centralised stable coin.

11 According to Tether’s homepage, reserves “include traditional currency and cash equivalents and, from time to time, may include other assets and receivables from loans made by Tether to third parties, which may include affiliated entities” (Tether 2020).
An example of a decentralised stable coin is the DAI, created and managed by MakerDAO. The stable coin envisages a fixed ratio of 1 DAI to 1 USD.\(^\text{12}\) Stability is attempted through a combination of economic incentives and “monetary policy” tools. As soon as the DAI market price deviates from the parity, users are incentivised to buy/sell DAI due to arbitrage possibilities. Additionally, the protocol can be updated to adjust the “DAI Savings Rate”, a sort of interest payment on locked DAI. These fluctuations in supply and demand should steer the DAI towards parity with the USD (MakerDAO n.d.).\(^\text{13}\)

Although stable coins that are referenced to official currency do not pose a competitive challenge to their reference currency, they may increase foreign currency access in other currency jurisdictions. Thus, potentially increasing the threat of currency substitution among official currencies, and in some sectors of economic activity where access to official currency is hampered or costly (e.g. unregulated trading of crypto assets against official currency, cross-currency payments).

**Crypto assets with additional non-currency functionalities:** Ethereum was the starting point for a whole genre of crypto assets. It introduced a blockchain-based platform for projects built on top of it, allowing the launch of crypto assets covering various use cases. Contrary to the Bitcoin network, the Ethereum protocol ties the supply of Ether to the amount of mining activity without determining a predefined total amount of coins. The supply is, for example, determined by block rewards or the difficulty of mining new blocks, where increased difficulty increases the time it takes to validate transactions and thus decreases the amount of newly minted coins (EthHub n.d.a). Such decisions on the Ethereum blockchain more closely resemble traditional policy decision processes. Stakeholders of the network (e.g. developers, miners, users) can propose changes to the protocol, which can then be evaluated and voted upon off-chain. Once all stakeholders agree on an update to the protocol, the changes will be implemented (EthHub n.d.b).

The supply implications depend on the protocol and on the policy decisions the network participants make, offering some degree of potential to adjust supply to demand on crypto markets. Of course, such a system is to some degree susceptible to the influence of stakeholders with a strong influence on other users (e.g. experienced developers or simply well-known individuals). In the case of Ethereum, its more flexible supply governance compared to Bitcoin did not have the effect of stabilising its market value. But it has been used as a platform to both initiate new crypto projects and inspire others. Meanwhile, a subsector of crypto assets has emerged that seeks to retain and refine the decentralisation principle and apply it to areas of the financial sector beyond currencies (we will explore this aspect in the following sections).

### Doing away with the trust and costs of intermediation?

Many observers associate blockchain-based crypto assets with the ability to replace the need for trust in transactions. The *Economist*, for example, devoted one of its cover issues in 2015 to the blockchain technology; it was titled “The Trust Machine”. It was argued that the blockchain enables two parties to transact without having to trust each other and/or a centralised third party. Scientific papers often refer to the technology as being “trustless” (for example, Davidson et al. 2018). They argue that the blockchain substitutes for trust – trusting another party in a transaction involving only information that can be verified on the

---

12 It actually maintains a ratio of 1 DAI to the ETH-equivalent of 1 USD.
13 For a time, series of the DAI against the USD, see https://coinmarketcap.com/currencies/multi-collateral-dai/.
blockchain – are no longer a necessity to facilitate efficient transactions. Both views of the blockchain technology – creating trust and substituting for trust – are misleading.

Cryptocurrencies may come without centralised intermediaries, but not without intermediation functions. Some of these functions are decentralised (the register of transactions and holdings is administered by competing miners instead of banks); some of them are not offered within the system (it is technically possible to join the network without asking a responsible bank-like entity for permission or disclosing your identity; no entity is responsible for guaranteeing the value of coins or backing them with assets).

For those intermediary functions that are decentralised in blockchain-based crypto assets, the need to trust in a centralised intermediary is replaced by the need to either trust in the intended functioning of rules, algorithms, and incentives contained in the software, or to trust in one’s personal ability and incur the cost of verifying the state of the blockchain with a personal computer. Fees for user transactions apply, depending on the amount of network traffic, and current miner compensation from newly produced crypto units.

Those intermediary functions that are eliminated in the blockchain-based set-up require additional arrangements to be performed outside the cryptocurrency’s blockchain. Individual users are faced with the choice of either placing trust in their own ability and personally incurring the cost for the following services, or trusting fee-based intermediaries in the crypto sector to service them: acquiring the knowledge and resources how to access crypto currencies and information about them; finding someone else to exchange and measure cryptocurrencies against something valuable (an official currency, or a good or service); storing and protecting the personal access key to individual crypto ownership against theft or loss, etc.

Additionally, cryptocurrencies’ decentralised mechanisms fail to replace the role of intermediaries in contributing to monetary stability – a feature of money that is associated with saving transaction costs for individual money users. In the absence of monetary stability, transaction costs in a currency network rise, making them unattractive: unpredictability of money’s value implies the lack of a yardstick for individual and collective planning of the economic future, an undermining of price transparency and comparability as the basis of functioning markets, additional efforts required for acquiring information relevant for economic activity, and the lack of a basic means to store value with minimal risk.

Decentralised cryptocurrencies come without centralised intermediaries, but they eliminate neither the need for intermediation nor the costs and trust required for economic transactions and storing economic value (Campbell-Verduyn 2019). A key point in this context is that the internal consistency of the data produced and stored on the blockchain may be credible but would be meaningless and irrelevant unless referring to, and evaluated by, the outside world according to rules and mechanisms prevailing in this context (e.g. markets where people are prepared to spend official currencies to purchase Bitcoin according to their personal value judgements, contributing to the emergence of a market value for Bitcoin). So, the technology’s ability to transform trust requirements is always limited (Frolov 2021).

Crypto use cases beyond currency status

While current cryptocurrencies offer no incentives to use them wherever the use of stable official currency is possible and attractive (for measuring, transferring, and storing liquid predictable value), they have other features which may attract users in special use cases. A major use case for cryptocurrencies has become their use as a speculative asset based on expecting the future appreciation of their market value. Crypto assets can meet user demand on markets for
Crypto assets

risky assets, complementing a market that includes collector items (antiques, used stamps and records, art, etc.), and other financial and non-financial assets (gold, silver, land, etc.) in limited supply that bear the chance of financial returns or changes in market value.

A further potential use case is the use of cryptocurrencies as means of payment in transactions related to illicit activity (digital markets for drugs and other illegal goods, illegal online gambling, tax evasion, etc.) and for transactions where users have a particularly strong preference for privacy for various reasons (Tzanetakis 2018). Unlike bank accounts, it is technically possible to access and transfer cryptocurrencies without disclosing user identity to intermediaries. In these cases, such users might be willing to incur the additional transaction costs involved in using cryptocurrencies as means of payment.

If such uses became widespread, they could ultimately indeed undermine taxation and regulation of economic transactions as important pillars of the governance of official currencies and economies. To limit the possible contribution of cryptocurrencies to the expansion of dark markets, tax evasion, and money laundering, regulators have agreed in international fora to submit intermediaries serving as access points to crypto assets (e.g. crypto exchange platforms) to Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) rules, thus creating a level playing field with regulated banks in this respect. Tax authorities have submitted a number of crypto uses to taxation and have started to use the services of private firms specialised in identifying users behind crypto accounts to enforce it (Houben and Snyers 2018; OECD 2020a).

While crypto assets seem to be ill suited to compete against traditional currency systems, they might impact other sectors more strongly. In fact, we have already encountered crypto assets that are not targeted towards being used as currency, but rather to facilitate non-currency uses: on top of the Ethereum blockchain, a subsector of crypto assets has emerged that seeks to retain and refine the decentralisation principle and apply it to areas of the financial sector beyond currencies.

Crypto assets as financial instruments

One way to conceptualise crypto assets designed for non-currency functionalities is to consider them as belonging to a more general class of phenomena referred to as “tokens”. The private cryptographic keys to identify and transfer a particular sum of a crypto asset on the blockchain might be considered as tokens. These are physical items, tools, or data packages that are built to authorise access to a certain function of the system they belong to: for instance, a casino chip gives access to services within the casino and can be redeemed for a certain sum of cash at the cashier. A banknote represents the value guarantee of the central bank and gives access to goods and services in all those transactions where it is accepted as a means of payment. A supermarket voucher gives access to goods available at the supermarket of a certain quantity or of a certain monetary value.

Both tokens and the phenomena they represent can be recorded in registers, sometimes referred to as ledgers. The blockchain is a ledger or register of tokens where owners of keys can induce changes that find the agreement of all other users based on their trust in the solidity of the operating rules of the blockchain, resulting in transfers among key holders without a single entity able to interfere. Whereas the initial idea of Bitcoin was to offer what was called a “peer-to-peer cash system” with a vague analogy to gold being the only reference to phenomena outside the blockchain, a number of subsequent crypto projects started to explore the idea of whether tokens could be constructed as precise representations of various non-currency uses.
Various kinds of tokens on blockchains can be distinguished. The most common tokens are native tokens, such as BTC or ETH. Private keys held by owners give them access to the native cryptocurrency, which is stored on the blockchain (i.e. ledger). Buterin (2013), however, already noted in the beginning of the Ethereum white paper that the blockchain technology offers the potential to record more than just the ownership of native cryptocurrencies. Theoretically, information on any physical and non-physical asset can be stored on the blockchain ledger. Consequently, any asset can be tokenised on the blockchain. The concept of tokenisation has already been proposed by Nick Szabo in 1998, who was bothered by the fact that traditional ledgers can be compromised by third parties (e.g. by malicious actors or simply through errors).14

The general-purpose blockchain technology provided by Ethereum enables the implementation of any conceivable tokenisation. Ethereum also provides popular standards that include common features for the implementation of new tokens.15 The ERC-20 standard regulates fungible tokens, i.e. tokens of the same value (Vogelsteller and Buterin 2015). Fungible tokens indicate ownership of an underlying homogenous good with a universal value attached to it, such as gold. They are thus interchangeable. The ERC-721 standard regulates non-fungible tokens, which are characterised by non-interchangeability (Entriken et al. 2018). An early example of such tokens are “CryptoKitties”. The idea was that a smart contract autonomously creates unique digital cats every 15 minutes which represent tokens and are stored on the Ethereum ledger.16

Other (arguably more useful) scenarios include the tokenisation of artwork, real estate, and securities. For illustration, we draw on two examples given in Voshmgir (2020). To invest in a fraction of a piece of art, a specific token could be issued (e.g. on the ERC-721 standard), where one token is associated with the ownership of a fraction of a specific piece of art. This would enable investment in a painting with considerably lower funds than would otherwise be required to buy an entire piece of art. Similarly, real estate could be tokenised and, for example, finance a credit to buy a house. Tokens (e.g. on the ERC-721 standard) that resemble ownership of a fraction of a house could be created and sold to investors. These investors would then be compensated by fractional rent payments from the owner of the house. This would foster penny-stock-like investments in specific real estate objects with low amounts of capital.

The two examples are built on an interconnection between the blockchain world and the real world. The tokenisation of assets with a real-world representation (such as art and real estate) is usually referred to as asset-tokenisation, to distinguish it from tokens purely related to the blockchain space. The OECD (2020b) issued regulatory concerns about asset-backed tokenisation because it requires trusted centralised authorities that guarantee that the blockchain token has its claimed value in the real world. Whenever this connection is contested (e.g. motivated by opportunism), contracts have to be enforced by legal institutions. In any case, it seems that asset tokens contradict the design-philosophy of a purely decentralised system that wants to minimise dependence on centralised parties.

As a general observation, a properly functioning blockchain system creates, contains, and updates token data according to its internal rules in a credible way. But that does not include

---

14 Szabo’s (1998) concept was, however, never implemented due to technological limitations at the time.
15 The indication of ownership can be either attached to existing native tokens, implemented on a new layer on top of an existing blockchain, or based on smart contracts. The latter method is most common (for example, Schär 2020).
16 www.cryptokitties.co
the creation of consensus around the interpretation of this data, its application and consequences for the world outside the blockchain. As a result, any potential transaction cost savings resulting from blockchain-operated token systems must be considered in the context of transaction costs involved in mechanisms referencing blockchain data to the outside world in terms of valuation and enforcement (Narayanan et al. 2016).

There may be demand for tokenisation of indivisible assets for facilitating their shared use over time among multiple owners (car sharing, sharing a country house etc.). If tokens are tradeable on markets, this contributes to the commodification (expansion of markets) and financialisation (creating claims on marketable assets that are tradeable on secondary markets) of non-financial asset classes. This might lead to the creation of possible positive as well as negative externalities with regard to their accessibility, price, and quality for consumption purposes of these assets among non-owners.

Tokens directly or indirectly related to traditional securities (e.g. debt, equity) are particularly interesting from a financial as well as legal perspective. Two terms commonly used in this context are security tokens and tokenised securities. The latter simply refers to tokens that represent traditional securities on a new technology. Associated benefits could include increased transparency, lower transaction costs, and lowered access barriers. Security tokens focus more directly on the blockchain technology and encompass, for example, any native tokens that pay out dividends. Several use cases will be discussed further later. Put differently, tokenised securities wrap an existing product into a new package, while security tokens represent a new product themselves (Acheson 2019).17 Tokenised securities are less problematic from a legal point of view because traditional securities are a well understood concept. Security tokens may be more complicated in this regard. Legal institutions have to define which tokens mimic the behaviour of securities and should thus be regulated.

**Decentralised finance (DeFi)**

Recently, decentralised finance (DeFi) has become the new hype in the blockchain community. The term builds around the concept of providing traditional financial services, empowered by tokenisation (as discussed previously), in a decentralised version. Examples include borrowing, lending, investment, trading, and payment services in a decentralised, peer-to-peer version. All these services are provided by decentralised Apps (dApps) on a blockchain system, each of which may feature distinct tokens. DeFi promises more security, higher efficiency, and more inclusiveness (Sandner 2019). This stands in stark contrast to related traditional systems. The financial sector mainly produces promises to pay (shares, bonds, credits, etc.), and financial services are built around these promises (e.g. creation, pricing, trading, assessment, enforcement). DeFi starts from the basic crypto idea that trust in promises is best avoided (crypto coins are no one’s liabilities) and tries to create financial instruments and services from a different angle. Although DeFi thus seems to be a particularly intriguing development in the crypto world, a complete discussion of all DeFi applications is clearly outside the scope of this contribution. The following paragraphs will therefore feature a short discussion of selected concepts that seem most promising to us.

Centralised cryptocurrency exchanges. Cryptocurrencies can either be traded against each other or against official currency. The latter version creates a direct interface between the off-chain and on-chain world and is therefore of particular importance. It is, however, also very controversial.

17 The terms are, however, still used inconsistently in the literature.
Tobias Eibinger, Ernst Brudna, Beat Weber

Any direct connection to the off-chain world makes the central idea of blockchain – being decentralised and independent from centralised institutions – less feasible. Imagine Bob wants to enter the blockchain world and take advantage of DeFi services. First, he has to convert some official currency into cryptocurrencies. Centralised exchanges (CEX) facilitate exchanges between official and cryptocurrencies as well as between cryptocurrencies. However, CEX are akin to traditional intermediaries and thus have to be trusted not to mismanage funds and to provide security. Private keys are often managed by centralised institutions, thus giving up full control over one’s tokens. In any case, native blockchain-like security is, due to the centralised nature of such services, generally not achievable (see for example, Voshmgir 2020). Furthermore, CEX are subject to legal regulation, such as KYC and AML requirements.18

**Decentralised cryptocurrency exchanges.** Decentralised exchanges (DEX) alleviate some of the issues plaguing CEX, at least in the case of exchanges between cryptocurrencies (see, for example, Voshmgir 2020). Such systems avoid the intermediary characteristic of centralised exchanges. This is achieved, for example, through the use of Atomic Swaps. Imagine Bob successfully exchanged official currency for BTC. Now, he wants to exchange BTC for ETH. Conveniently, Bob knows Alice, who wants to trade the equivalent amount of ETH for BTC. A special smart contract can ensure that both parties receive their respective cryptocurrencies after the transaction is completed. DEX would utilise this concept and enhance it with matching algorithms to minimise the coincidence-of-wants problem associated with Atomic Swaps. However, such DEX cannot bridge the off-chain/on-chain gap in a decentralised way. The exchange of official currency for cryptocurrency requires coordination with banks or other third parties who handle cash exchanges. One option for this gap to be bridged in a decentralised version might be the tokenisation of official currencies. That is the business model behind a number of stable coin projects discussed earlier.

**Decentralised payment systems.** Bitcoin was initially developed with the aim of providing a decentralised, peer-to-peer alternative to traditional payment systems (Nakamoto 2008). However, compared to traditional payment systems, the Bitcoin network seems rather inconvenient. A block is completed about every ten minutes on average, and the system manages 3–4 transactions per second.19 Transaction fees on the Bitcoin network fluctuate widely.20 However, dApps, such as the Lightning Network, promise fast transactions with low to zero transaction costs. The application is built on top of the Bitcoin network, on which two users can exchange BTC without the need to validate each transaction. Only when two users have stopped their transactions, is the final amount of BTC each holds added to a block and validated on the original network layer. While this may compromise security to some degree, the added speed and low fees make this dApp an interesting solution for day-to-day transactions of small size (Cointelegraph n.d.).

**Decentralised credit systems.** Theoretically, blockchain-based decentralised lending and borrowing services offer lower operational costs, more control, and more security compared to traditional systems that rely on banks as intermediaries (Voshmgir 2020). In decentralised credit systems, users can provide (lend) cryptocurrencies to a pool and earn interest on their assets. This pool serves as the basis for borrowers to withdraw cryptocurrencies from. However, to borrow, users have to provide collateral to the pool, as traditional KYC processes are not part of decentralised credit systems. Still, borrowers can potentially profit from lower interest rates compared to traditional systems. Thus, both lenders and borrowers might benefit from arbitrage.

---

18 In the US, the regulation of such exchanges has recently been reinforced by the director of the Financial Crimes Enforcement Network (FinCEN), Kenneth Blanco (Chavez-Dreyfuss 2019).
Crypto assets

possibilities (Sandner 2019). Furthermore, tokenisation coupled with decentralised credit systems allows for any form of tokenised asset to serve as collateral. This would further bridge the gap between the traditional and decentralised world.

**Token sales.** The initial sale of tokens has become a popular alternative to equity-crowdfunding and for young companies to accrue capital beyond the usual FFF group (family, friends, and fools). Token sales are usually issued via cryptocurrency exchanges and promise various benefits, some of which inherently stem from the blockchain technology as such (e.g. increased security, no need to trust third parties). Other benefits include efficiency gains over traditional secondary markets that facilitate crowdfunded equity shares trading (e.g. lower costs, lower counterparty-risk) (Schär 2020). Token sales can be divided into several categories. Initial Coin Offerings (ICOs) started in 2013 and many of these were issued as utility tokens, which face lax regulations, as they are not counted as securities. This inevitably invited malicious and opportunistic behaviour, which became most evident in 2017, when 80% of ICOs were identified as scams (Satis Group 2018). This fraudulent behaviour invited harsh criticism and strengthened the public perception of cryptocurrencies as a purely speculative and shady technology. More recently, Security Token Offerings (STOs) gained traction. These tokens are explicitly designed with securities in mind and are, thus, subjected to financial regulation, which helps to strengthen trust in non-opportunistic behaviour from issuers. STOs may nevertheless be prone to the use of cheap signals, e.g. exaggeration or faked information and promises (Ante and Fiedler 2019).

**A note on background conditions**

Before we conclude our contribution, we want to elaborate on an often overlooked but instrumental concept in the evaluation of how cryptocurrencies might shape society: background conditions, or, put differently, the rules of the game (North 1990). It is sometimes argued that crypto assets (and the blockchain technology in general) reduce certain transaction costs – even though different transaction costs might arise. For now, assume that crypto assets do in fact reduce overall transaction costs. Whenever these costs can be reduced, the amount of mutually beneficial transactions in an economy increases. However, is this always socially beneficial?

According to the economic principle of free contract, this question could be answered in the affirmative. It states that a contract between two adults adequately represents each party’s evaluation of the outcome and should thus not be interfered with. There are at least two main reasons for why such a conclusion would be premature. Firstly, even though a transaction might be mutually beneficial for the contracting parties, it might negatively affect other individuals. Secondly, the principle of free contract neglects the potentially unequal distribution of the underlying background conditions.

In essence, background conditions constitute the rules of the game under which contracts (transactions) are signed. For the purpose of our contribution, it suffices to say that these conditions may encompass the prevailing regulatory framework, norms, and standards in an economy as well as the distribution of economic property rights. In particular, background conditions shape feasible alternatives to a contract (i.e. outside options) for participants in an exchange. For an excellent and more sophisticated discussion of background conditions, we refer the interested reader to Sturn (2009).²¹

²¹ Although Sturn (2009) focused on the labour market, many analogies can be drawn in the context of this contribution. Indeed, Sturn (2020) put background conditions in the context of blockchain technology and network effects in a German text.
Whenever background conditions are unequally distributed, one contracting party is usually in the position to extract a major share of the gains from a transaction. Due to a lack of attractive alternatives, the true preferences of the other (exploited) party may not be revealed. The rules of the game should then ultimately not only be designed to maximise the amount of mutually beneficial transactions, but also to minimise the number of transactions that result out of unequally distributed background conditions. Traditionally, these conditions have been shaped by the public sector to a large degree and provided a fruitful environment for the private sector to unfold its productive potential (see Sturm 2009, 2020).

So far, the most popular crypto projects reveal a preference for the ideal of a pure market economy. They create new asset classes whose creation, accession, and transfer are governed by market mechanisms and principles. Additionally, these rely on both asset and market designs intended to avoid the involvement of entities belonging to or being regulated by the public sector. In this libertarian vision, public sector activity and democratic forms of decision making on economic affairs are perceived as both illegitimate and economically distortive, whatever the initial distribution of background conditions and whatever the results produced by markets (Berg et al. 2019; Golumbia 2016; Scott 2014).

Concluding remarks

Following the structure of this chapter, we will start our concluding remarks with the monetary system. Crypto assets are often regarded and treated as a speculative asset, due to the wide fluctuation of their value vis-à-vis traditional currencies. Therefore, they are not particularly suited as a predictable store of value, which is a crucial concept defining money. Stable coins are a different matter in this regard (as they aim to uphold a stable peg to some commodity, often official currencies) and have to be distinguished from Bitcoin-like crypto assets. In any case, both types of crypto assets as of today cannot be regarded as a medium of exchange nor a unit of account due to the absence of their wider adoption.

This raises the question of what stifles this wider adoption. Transaction costs in the form of costs associated with switching currencies may provide an answer. Established currencies offer huge network effects and currency users are characterised by some degree of inertia resulting from switching costs. These might be quite large. Cryptocurrencies are built on the philosophy to abstract from centralised third parties to facilitate transactions. The blockchain technology that underpins crypto coins provides the techno-economic tool kit to achieve this. Blockchain-based decentralisation of governance poses limits to an asset producing the kind of stability of economic value that would be competitive compared to official currencies. Technically increasing the predictability of a marketable asset’s supply does not automatically result in a stable market value. Therefore, some successful stable coins try to join existing official currency networks by attempting to tie the value of their assets to official currency with various techniques.

A key raison d’être for crypto assets is their decentralised architecture. Indeed, the motivation behind the first decentralised peer-to-peer payment system (Bitcoin) came from the mistrust vis-à-vis traditional centralised third parties (e.g. banks). Crypto assets, underpinned by the blockchain technology, should eliminate the need to trust such centralised institutions. The blockchain indeed provides the techno-economic functionalities to facilitate transactions in a decentralised way. Nonetheless, the technology is not entirely “trustless”. Trust is simply

22 Nevertheless, there are also efforts to explore the potential of the blockchain technology for projects inspired by a broader range of governance visions (Berryhill et al. 2018; Scott 2016).
Crypto assets

shifted to other dimensions; now trust has to be put in the consensus mechanisms as well as the robustness of the specific blockchain architecture employed. But even the decentralised nature of transactions might, in reality, fail to emerge as an indirect consequence of transaction costs.

Cryptocurrency users have to incur search costs for finding someone accepting cryptos as payments, costs of monitoring adequate price conversion (from crypto to official currencies), the cost of protecting and the risk of losing the private key, learning costs, the risk of making an irreversible transaction, etc. For all these risks, centralised intermediary services have developed in the crypto sector that offer to absorb some of these risks if you trust them – for a fee. In any case, the question whether a more decentralised monetary system would even be beneficial to our society remains. Clearly, a decentralised monetary system would bestow certain privileges on certain stakeholders. They might use their privileges opportunistically and try to extract extra profits for themselves.

Having these transaction costs in mind, crypto assets still do offer the potential to impact the financial sector. One aspect to mention in this regard is the concept of the tokenisation of finance or entirely new financial instruments that are native to the blockchain technology. Another buzzword in this context is decentralised finance (DeFi). The concept promises, for example, increased inclusiveness, stronger security, and higher profitability. The first two examples are more closely related to the decentralised nature of the blockchain technology. It is not dependent upon centralised intermediaries, such as banks. Thus, anybody with the required experience can theoretically participate in DeFi. Moreover, there is no need to trust these intermediaries, which strengthens security (in addition to increased cryptographic security). Higher profitability seems to be a more ambivalent topic. DeFi enables the creation of entirely new forms of finance in a sandbox environment. But it is also a fertiliser for speculative and fraudulent behaviour motivated by a lack of accountability. Therefore, regulatory issues seem to continue being a prominent topic surrounding decentralised finance.

Finally, we want to highlight that the assessment of crypto assets also encompasses spheres that tend to be addressed only rarely. Political as well as moral aspects highlight a tension between a decentralised world and equally distributed background conditions, which are usually publicly provided. Private provision (by crypto projects) of these conditions can elicit opportunistic behaviour and ultimately lead to increased inequality. Historically, it has been shown that increased inequality tends to strengthen undemocratic or illiberal responses. Under consideration of these aspects, the role of the government in the public provision of background conditions should not be undermined too strongly. Ultimately, a movement that implicitly threatens the legitimacy of centralised authorities (blockchain, crypto assets) may even necessitate a stronger public sector to defend democratic values.

References


Buterin, V. [@VitalikButerin] (2018): To Be Clear, at this Point I Quite Regret Adopting the Term “Smart Contracts”. I Should Have Called Them Something More Boring and Technical, Perhaps Something Like “Persistent Scripts”. [Tweet; thumbnail link to article], *Twitter*. Available at: https://twitter.com/VitalikButerin/status/1051160932699770882?ref_src=twsrc%5Etfw%7Ctwcamp%5Eetweeterembed%7Ctwterm%5E1051160932699770882%7Ctwgr%5Eeshare_3%26amp%3Bref_url=https%3A%2F%2Fbitcoin.com%2FVitalik-buterin-ethereum-regret-smart-contracts%2F [05.10.2020]


EtherWiki (2020): Proof of Stake FAQs. Available at: https://eth.wiki/concepts/proof-of-stake-faqs [05.10.2020]

EthHub (n.d.a): What is Ethereum? Available at: https://ethhub.eth.link/ethereum-basics/monetary-policy [05.10.2020]

EthHub (n.d.b): Governance. Available at: https://ethhub.eth.link/ethereum-basics/governance [05.10.2020]


MakerDAO (n.d.): The Maker Protocol: MakerDAO’s Multi-Collateral Dai (MCD) System. Available at: https://makerdao.com/de/whitepaper/ [05.10.2020]


Crypto assets


Satis Group (2018): Cryptoasset Market Coverage Initiation: Network Creation. Available at: https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ [05.10.2020]


Tether (2020): Digital Money for a Digital Age: Global, Fast, and Secure. Available at: https://tether.to [05.10.2020]


