FRIEDRICH NAUMANN FOUNDATION For Freedom.

POLICY PAPER

# FOUR WAVES OF DIGITAL CURRENCIES AND THE FUTURE OF MONEY

Sven Hilgers and Konrad Greilich

ANALYSE

# Publication Credits

**Published by**
Friedrich Naumann Foundation for Freedom
Truman-Haus
Karl-Marx-Straße 2
D-14482 Potsdam-Babelsberg

/freiheit.org
/FriedrichNaumannStiftungFreiheit
/FNFreiheit

**Authors**
Sven Hilgers
Theme Manager Globalisation, Free Trade & Market Economy
Friedrich Naumann Foundation for Freedom

Konrad Greilich LL.M. (Tel Aviv)
Scholarship Holder, Friedrich Naumann Foundation for Freedom
Doctoral Candidate at the Bucerius Law School
on Blockchain & Corporate Law

**Editorial team**
Referat Globale Themen
World Order and Globalization Hub

**Contact**
Phone +49 30 220126-34
Fax +49 30 690881-02
Email service@freiheit.org

**Last update**
May 2022

# Executive Summary

The rise of digital currency has changed the financial world in record time. Established business models are facing new challenges. The development is often reduced to a single cryptocurrency: Bitcoin. But numerous other digital currencies have come into being since the appearance of this first crypto asset that enables direct transactions between private individuals. This policy paper outlines how different types of digital currencies have arisen in four waves and offers policy recommendations on how to shape their future development.

The diversity of digital currencies and their technological development can be seen in the first three waves. The authors classify developments by functionality, organizational form, governance, and source of value. With each wave, new functions are added or there is a shift in how the digital currencies can be utilized. A striking aspect of the emergence of digital currencies in the first three waves is the dominance of private actors without any major influence of public actors. Most of them are based on blockchain or distributed ledger technology, the technical details of which will be explained here as well.

The fourth wave is currently underway: In central bank digital currency (CBDC), central banks are developing an electronic form of established national or supranational currencies and are facing numerous critical decisions. This development will usher in a new currency era, in which different currencies and forms of currency come into far greater competition with one another in a single currency area.

Building on the analysis of the four waves, we offer suggestions about what sort of regulation makes sense for this new currency era and how digital central bank money can make a positive contribution. Whereas economic issues are the focus in the development of central bank digital currency in liberal democracies, there are many signs that CBDC can also be used for surveillance and social control in authoritarian, state-capitalist systems. Hence, what is at stake in the increasing systemic rivalry between liberal democracies and the latter is setting the standards for how digital currencies can be effectively used in the context of the rule of law. Overall, more openness to the diversity of digital currencies is needed, as well as to their potential for promoting the innovativeness of economies and the provision of stable money as a public good. A digital currency policy should thus be guided, above all, by the principles of *innovation, inclusiveness, stability,* and *freedom*.

# Abbreviations

| | |
|---|---|
| BGB | Civil Code |
| BIS | Bank for International Settlements |
| BTC | Bitcoin |
| CBDC | Central Bank Digital Currency |
| DeFi | Decentralized Finance |
| DAO | Decentralised Autonomous Organisation |
| DLT | Distributed-Ledger-Technologie |
| e-Krona | Electronic form of the Swedish currency Krona |
| e-Naira | Electronic form of the Nigerian currency Naira |
| e-Peso | Former electronic form of the Uruguayan currency Peso |
| ERC-20 | Standard for the creation of tokens on the Ethereum-Blockchain |
| e-RMB | Electronic form of the Chinese currency Renminbi |
| EUR | Euro |
| eWpG | Electronic Securities Act |
| EZB | European Central Bank |
| KYC | Know-Your-Customer |
| MiCa | Markets in Crypto-assets Regulation |
| NFT | Non-Fungible Token |
| NYSE | New York Stock Exchange |
| P2P | Peer-to-Peer |
| PoW | Proof-of-Work Mechanism |
| PoS | Proof-of-Stake Mechanism |
| SEC | United States Securities and Exchange Commission |
| SDR | Special Drawing Rights |
| SNB | Swiss National Bank |
| SWIFT | Society for Worldwide Interbank Financial Telecommunication |
| TARGET | Trans-European Automated Real-time Gross Settlement Express Transfer System |
| TIPS | TARGET Instant Payment Settlement |
| USD | US dollar |

# Table of contents

# 1. Introduction

Since the start of the global financial crisis more than a decade ago, the global economy has been influenced by two concurrent trends: Fewer people are using cash in favor of digital forms of payment and digital transactions. These two trends do not only affect the financial world. In fact, the way in which people pay has far-reaching consequences for a society's functioning, the innovativeness of economies and the how people and firms relate to each other (Leibrandt/De Teran 2021). Crises are often the drivers of change in this connection. Consumers' way of making payments has not only changed significantly since the COVID-19 pandemic: Digital forms of payment have been on the rise and the significance of cash as a means of payment has been falling for years – and the conventional financial world is trying to keep up.

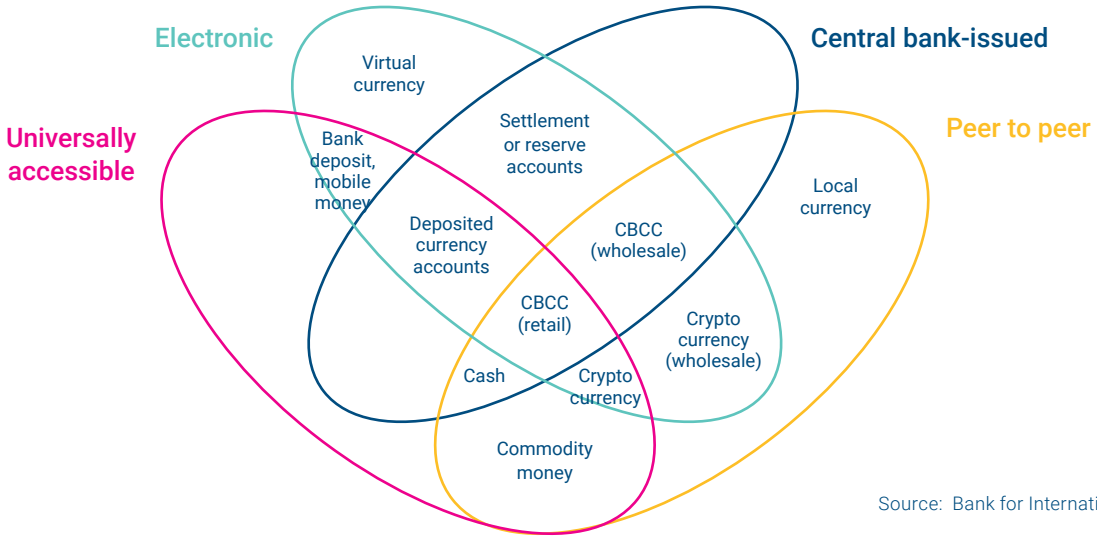
In the aftermath of the 2008 financial crisis, the former chair of the American Federal Reserve, Paul Volcker, remarked at a Wall Street Journal event in the UK that "the ATM has been the only useful innovation in banking for the past 20 years" (Haldane 2020). Around that same time, probably the most important monetary innovation since the introduction of paper money was born: the cryptocurrency Bitcoin. Bitcoin is the first private form of money that allows for direct digital transactions without relying on intermediaries like banks or central payment processors. There are a wide variety of applications for the so-called distributed ledger technology (DLT), or blockchain technology, on which many digital currencies are based, and numerous digital currencies have come into being in the years since the financial crisis. As a result, platforms developed their own currencies or payment systems, central banks are working on digital versions of their currencies, and public regulators are trying to find standards for the new currency era.

"Digital currencies" as used here is a general term comprising both new types of cryptocurrencies and conventional currencies or means of payment in digital form. Whereas some are based on the new blockchain technology or DLT, i.e. on a sort of decentrally administered accounting system, others use conventional payment systems. Just as all digital currencies are not based on a blockchain, currencies are not the only field of application of blockchain technology, with observers are speaking more generally of a new form of computing (Tapscott/Tapscott 2016).

This policy paper is about digital currencies, their diversity, and their numerous possible applications. The question, whether there is competition between private and public, i.e. government-issued, digital currencies, is no longer relevant. The relevant question is above all how a new and more highly competitive currency era will be shaped. To analyze this, we will depict in this policy paper how digital currencies have evolved to the present. Building on experiences with this new form of money thus far, we will develop different options for shaping the new currency era. The focus in this paper will be on how the regulatory framework for the wide variety of digital currencies should look like, so that the evolution of digital currencies can contribute to economic innovation and growth, as well as financial stability.

There are various models and indicators available for analyzing the many different forms of digital currencies. The "money flower" is regularly used in the publications of the Bank for International Settlements (BIS): a Venn diagram depicting the overlap between different forms of analog and digital currencies.

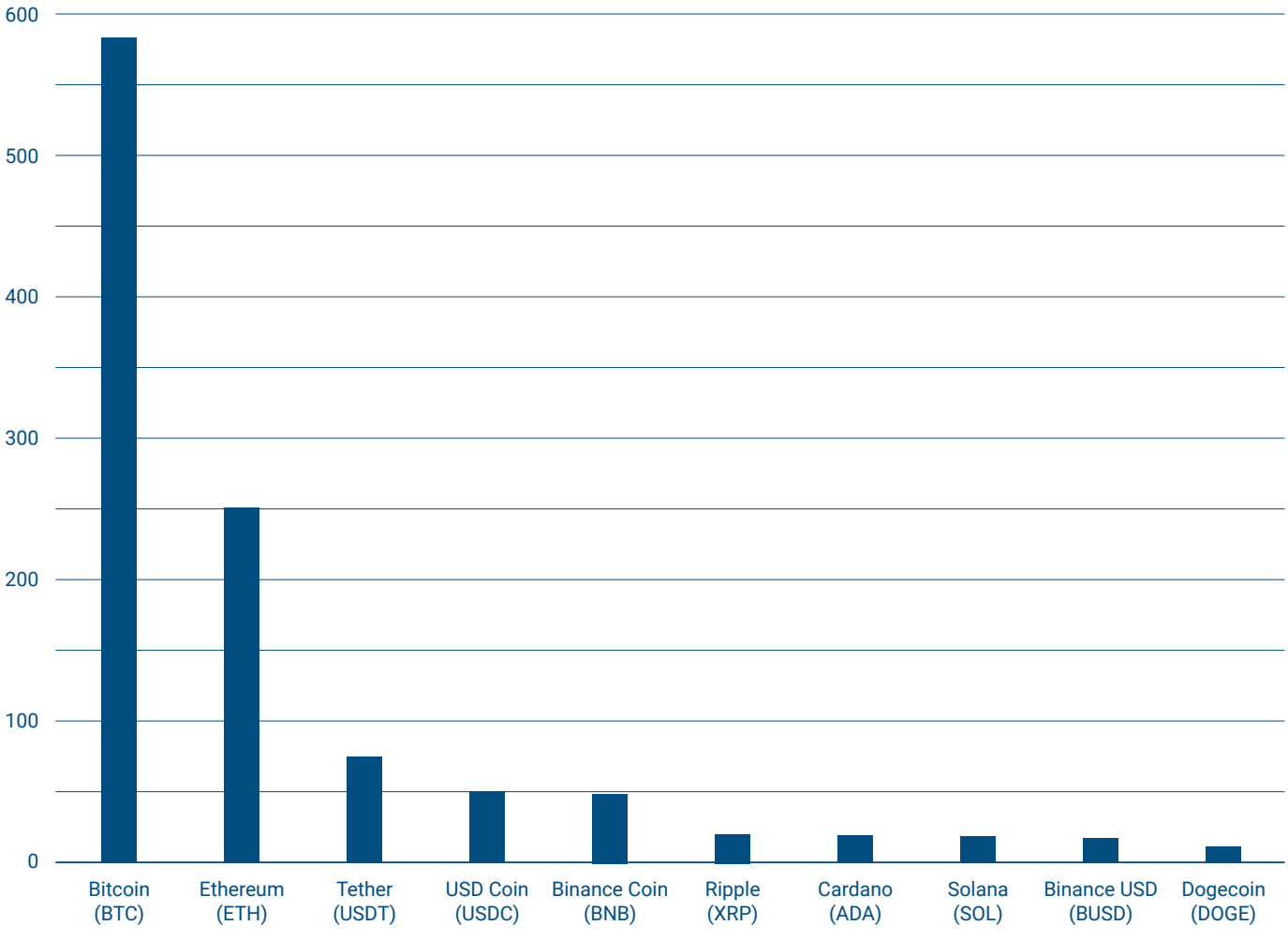
**Figure 1 | Money flower**




Source: Bank for International Settlements

However, two dimensions that are important for the emergence of a new form of currency and competition between digital currencies are missing here: the temporal dimension and the individual currency functions. The development of digital currencies has not taken place in a linear fashion; various new currencies have come into being and some of them have disappeared again over time.

**Figure 2 | Crypto currencies with highest market capitalization**
Ranking of the largest virtual currencies by market capitalisation in May 2022 (in US dollars)




Source: CoinMarketCap

Various digital currencies were created at different points in time, use different technologies, and offer different monetary functions. Not every digital currency fulfills all three typical functions typical money: that of a medium of exchange, that of a unit of account, and that of a store of value. The function as a medium of exchange is undoubtedly the most well-known function since money serves as a means of payment for most people in their daily lives. Many people who use their money as a form of investment will also be familiar with its function as store of value. The expectation that money should serve as a means for storing value also reflects the expectation that money's value and purchasing power should be stable in the long run: i.e. that both inflation and deflation should be avoided. In modern economies, the monetary policy of central banks is supposed to ensure the stability of value. Leibrandt and De Teran describe money's function as unit of account as its key utility (Leibrandt/De Teran 2021: 202). Although many things are suitable to serve as store of value or medium of exchange, only a few possess the requisite scalability and widespread availability to be used as unit of account (Leibrandt/De Teran 2021: 202). No digital currency has yet shown the ability to fulfill all three functions independently and completely. However, this may change in the near future. It is said of Bitcoin, the most widely used digital currency up to now, that is only suitable as medium of exchange to a limited extent and is not at all suitable as unit of account due to its great volatility (Hagelüken 2020: 143).

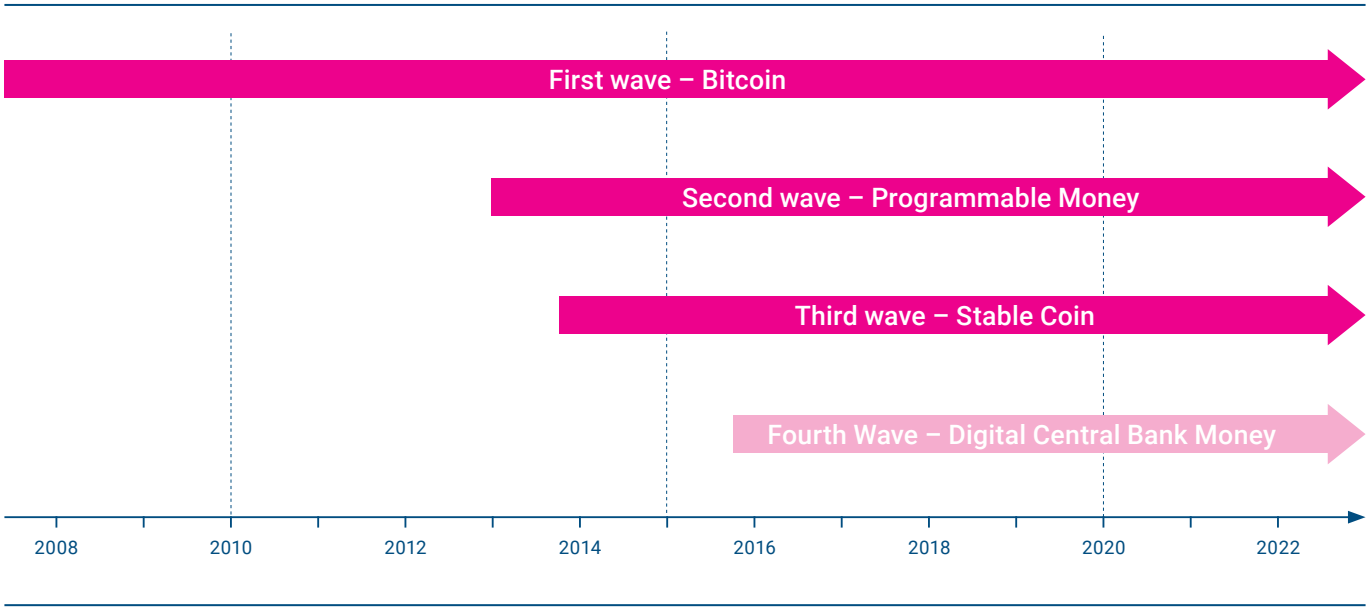
**Figure 3 | Overall cryptocurrency market capitalization in billion US dollars**


Source: CoinGecko; BitInfoCharts

However, due to its enormous rise in value, Bitcoin is regarded as digital gold and is most frequently used as a form of investment (Popper 2015). Other digital currencies are more suitable as medium of exchange or unit of account, but less as store of value. For example, a digital currency that is linked to an existing national or supra-national currency, like the euro or the dollar, can be used as a store of value; but it only gets its function as store of value from its reference to the existing currency and thus does not have any independent value storage function.

In order to describe the different developments and the variety of digital currencies since the global financial crisis, we draw on the narrative of development in waves that is widespread in the social sciences (see, for example, Huntington 1991 for democracy; Evans/Chamberlain 2015 for feminism; and Fischer 2021 for coffee). Normally, such waves are not self-contained, but rather run alongside and reinforce or hinder each other. In this paper, we identify four waves of digital currencies development that are distinguished by their specific monetary function, their form of organization and governance, and the source of their value. The functions and uses displayed by the individual currency projects can and are changing with each wave. Only the currencies of the fourth wave fulfill all traditional functions of money. The form of organization and governance of digital currencies varies between open, private, and restricted or club-like forms of organization and management. To put it simply, governance is about managing the currency, which can be done by all users in a peer-to-peer network or only by a limited circle (club). Modern fiat money – i.e. national or supranational currencies that are managed by central banks – derives its value not from the value of a commodity like, for instance, gold or silver or from reference to such values, but from regulation by and trust in the issuing states and their institutions. Digital currencies that are not issued by states derive their value from trust in the integrity of a protocol and the underlying technology with its incentive mechanisms, or the reputation of the issuing instance.

**Figure 4 | Four waves of digital currencies**




**Section 2** will discuss the first three waves of digital currencies, starting with wave number one and the emergence of Bitcoin as money for the Internet, which was developed by several committed computer experts and, thanks to the technological innovation of the blockchain, ushered in not only a new currency era, but also a new computing era. The second wave is no longer "merely" about money for the Internet, but rather about programmable money that can follow certain predetermined rules and is, so to say, a currency on the Internet. The third wave takes up the technological innovations of the first two waves and tries to create stable currencies ("stablecoin") by linking to a reference value. All three waves are developed and managed solely by private individuals or private institutions; the state only gets involved in the fourth wave. But government regulators and security agencies have also had an eye on the currencies of the first three waves. At first, it was about their misuse for criminal purposes and about matters of financial oversight, but since the mid-2010s even established figures like the then head of the Federal Reserve, Ben Bernanke, have been making positive comments about the potential of digital currencies (Popper 2015: 266; Vigna/Casey 2015: 113). **The third section** then looks at the fourth wave and digital central bank currencies. For a variety of reasons, especially the concern about loss of control over monetary policy and ensuring a stable means of payment, central banks are getting involved in the development of digital currencies. On the one hand, this could give rise to a renewed dominance of government-issued national or supranational currencies in the digital domain or, on the other, could lead to the coexistence of public and private digital currencies and some kind of competition between them (Groß et al. 2020a: 712).[1] However, this competition will be significantly different from the currency competition described by the economist Friedrich August von Hayek (1976). For von Hayek and many of his followers, the issue was a competition between stores of value and not a competition between new forms of money with different functions and areas of application (Hayek 1976; Brunnermeier et al. 2019). **The fourth section** on digital currency policy deals with this digital currency competition and examines how a robust framework for technical innovation and economic dynamism can be created. Nevertheless, at the same time a monetary and financial system that ensures monetary and financial stability as well as financial inclusion, transparency and trust in payment systems needs to be secured. In conclusion, we will identify four guiding policy principles when dealing with digital currencies: inclusiveness, innovation, stability, and freedom. Neither these four principles nor the four waves and policy recommendations are definitive or exhaustive. The new currency age is developing too fast for certainty. This rapid development should not serve as an excuse for inaction or lead to the temptation to prohibit digital currencies out of fear of what is new and unknown, as some countries have already tried unsuccessfully. Used correctly and in an appropriate framework, digital currencies can contribute to real gains in freedom and prosperity all across the globe.

1 Public and private do not refer here to the organizational form, but serve rather to distinguish between governmental and private action. Public digital currencies refer to money that is issued or managed by the state, whereas private digital currencies, on the other hand, are issued by non-governmental organizations or private individuals. In terms of organizational form, a limited distinction is made between "open," i.e. in the sense of freely accessible, and private forms.

# 2. Three Waves of Digital Currencies

The development of digital currencies has accelerated greatly over the last decade. Numerous variations and forms of digital currencies have come into being in a very short time. First attempts to develop digital money were made in the 1990s in the form of eCash, and David Chaum's underlying concepts still play an important role for current developments. However, it was only in the context of the global financial crisis that technological development and the demand for new forms of payment created an environment in which digital currencies represented a real alternative to the established monetary and financial system. Development has been taking place in waves since then and is continuously changing the financial world.

## 2.1 First Wave: Bitcoin, Money for the Internet

The programmer Satoshi Nakamoto, whose real identity is still unknown to this day, set off the raging debate on digital currency on a Saturday afternoon in November 2008, when he distributed the Bitcoin White Paper (Nakamoto 2008a) on a Cypherpunk movement mailing list. In the white paper, Nakamoto described the technology as a new form of electronic cash, which functions without a central issuing authority and is operated and managed solely by its users (Nakamoto 2008b). Unlike numerous prior attempts to create a digital currency by private actors, Nakamato was able to provide an outline of a system in which double spending of the digital currency would be largely impossible even without a central issuing authority, thanks to a technical solution. The currency was thus not exposed to the issuer risk that led to the failure of numerous private digital currencies in the past: i.e. the risk that the issuing instance will not be able to meet its payment obligations (Kutler/Power 1998). The Bitcoin network, which has existed for over ten years now, simultaneously created the technological basis for the cryptocurrency craze and gave birth to blockchain technology. The key innovative element of the Bitcoin network and blockchain technology is the intelligent combination of cryptography with a system of economic incentives for the purpose of preserving and maintaining a database in a decentralized network (The Economist, 31 October 2015). At least a quick look at blockchain technology and the underlying ideology of the early adopters and developers is essential for understanding the debates about digital currencies. The first wave of digital currencies can thus also be referred to as money for the Internet and, considering the inventors, as money for nerds. The Bitcoin network does not only respond to the issue of practical implementation with technical and cryptographic solutions, but also leaves controlling monetary policy and money supply strictly to the technical protocol. In the view of the inventors, the value of the currency is solely created by the underlying algorithm (Savelyev 2017: 119).

### The Cypherpunk Ideology

Who Satoshi Nakamoto, the inventor of blockchain technology, really is remains unknown to this day (Wallace 2011), even though individual suspects turn up from time to time and some out themselves (without proof) as the supposed genius (Fox-Brewster 2016). Thanks to his work and his chosen form of communication, situating the anonymous inventor ideologically is far easier. Nakamoto did not send the white paper to just any mailing list, but rather to the list of the Cypherpunk movement. The Cypherpunks emerged at the end of the 1980s in California, and they have been advocating ever since for extensive use of cryptography and other privacy-protection technologies to preserve and enable personal anonymity even in the digital age (Popper 2015). One of the pioneers of the movement, Eric Hughes, summed up the self-image of the Cypherpunks in his 1993 manifesto and thus also gave the Bitcoin network its marching orders: "We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money" (Hughes 1993). In the white paper, Nakamoto himself makes clear that an independent currency is required for trade on the Internet. He notes that small transactions are still prohibitively expensive and dependent on major financial institutions to verify every transaction and charge high fees (Nakamoto 2008a: 1). He argues that the current system, consisting of banks, payment systems and nation states, also allows for the reversibility of transactions, meaning that the current payment system is not only too expensive for small Internet transactions, but it also always involves the risk of a transaction being undone (Nakamoto 2008a: 1). Nakamoto wanted to dissolve this dependence of cyberspace on financial institutions, and to this end, he designed the Bitcoin network - a system for a kind of electronic cash that is managed exclusively by users and makes cheap anonymous transactions possible (Nakamoto 2008a: 8).

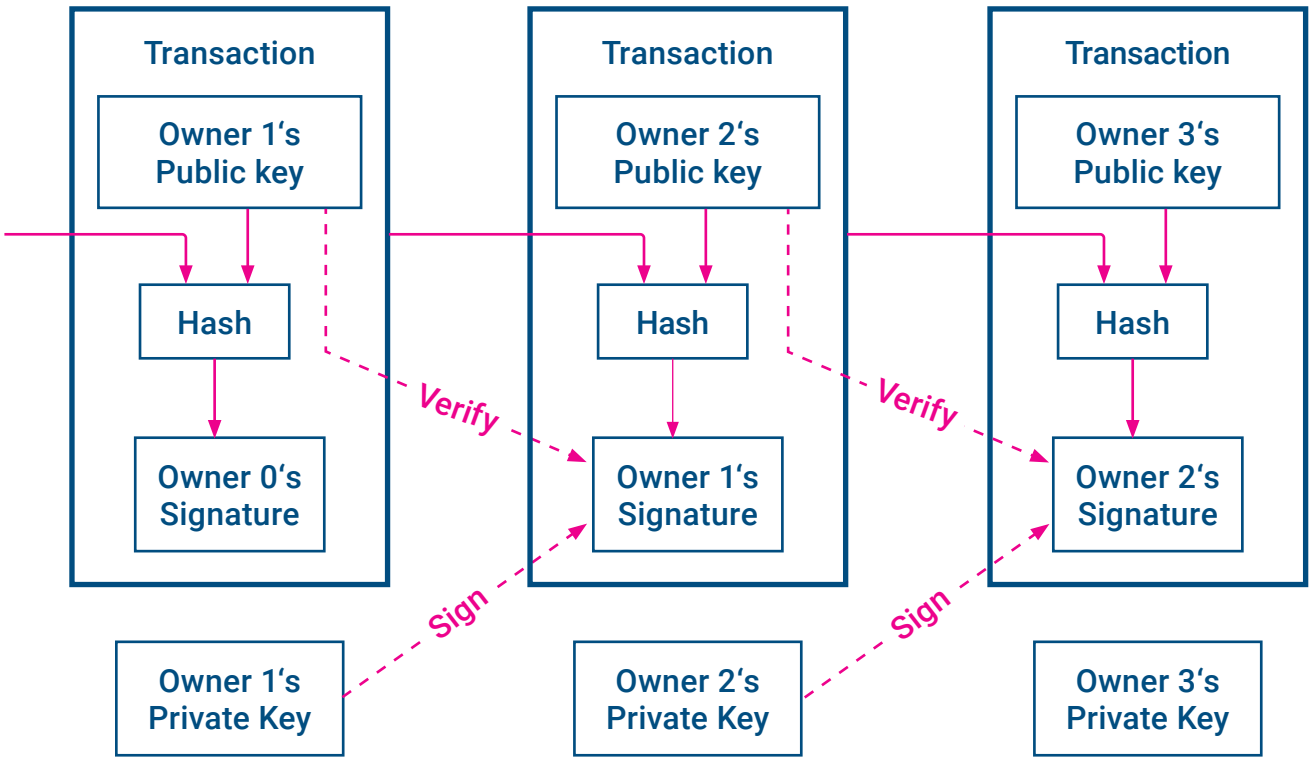
### The Blockchain Technology

The system proposed by Nakamoto operates without any central entity and succeeds, nonetheless, in almost entirely preventing the double spending of digital coins. Double spending of cash is avoided in the physical world thanks to the central issuing of unique banknotes by central banks. In addition, these banknotes or coins are endowed with numerous security elements to prevent unauthorized reproduction (Armelius et al. 2021). In the digital world, bits representing a digital currency can be very simply reproduced and disseminated without much cost (Antonopoulos 2017: 27). The original file and the copy created in a matter of seconds

by using the CTRL+C key combination are indistinguishable for a third party. This is where Nakamoto came in with his invention now known as blockchain technology. The Bitcoin network has three essential properties that have led to it sometimes being referred to as distributed ledger technology. First of all, the network consists of a database (ledger) in which each movement of bitcoins (transaction) is recorded (Antonopoulos 2017: 42). This database is not administered by a central agency like a central bank, but rather stored and maintained in a distributed network of an indeterminate number of computers (nodes) (Antonopoulos 2017: 30). The third property – and the most innovative element – is the technological solution used by the individual nodes within the distributed network to come to agreement on a uniform content of the database: the so-called consensus mechanism (Antonopoulos 2017: 27).

The database thus resembles a bank statement (Kaulartz 2016: 475), which uses the logic of double-entry bookkeeping to record every transaction between network participants chronologically (Antonopoulos, 2017: 42). New transactions are combined into a block and added to the transaction history approximately every ten minutes (Antonopoulos 2017: 27). These transactions are the core of the blockchain: They make the transfer of bitcoins possible and the entire network is designed to ensure they are secure and cannot be forged (Antonopoulos 2017: 116). From a technical point of view, transactions are electronic messages signed using asymmetric encryption. The public key in the key pair can be compared to an account number, whereas the private key corresponds to the PIN that controls it (Antonopoulos 2017: 85). The owner of both keys can thus freely dispose of the bitcoins associated with the account number by propagating signed transactions on the Bitcoin network (Antonopoulos 2017: 49).

**Figure 5 | Schematic overview of bitcoin transactions**




Source: Nakamoto 2008a

But for this to happen, the owner’s account number must itself possess bitcoins. Nakamoto described the bitcoin as a chain of electronic signatures (Nakamoto 2008a: 2). The signature chain of every single bitcoin always begins in the block in which it was newly created. At the same time, the creation of new bitcoins also serves as an incentive for network participants to ensure the uniformity of the database within the distributed network and to prevent double spending of coins. The consensus mechanism used for this purpose in the bitcoin network is usually referred to as proof-

of-work and is extremely energy intensive. As described above, transactions are combined into a block and attached to the database every ten minutes. So-called miners collect new transactions, check whether they match the transaction history, and then combine them into a block. For miners to have the right to add a new block to the transaction history, they have, in addition to checking the transactions, also solve a mathematical puzzle (Antonopoulos 2017: 50), which they do by way of repeated computational efforts to guess a random sequence of numbers. All the nodes participating in the consensus mechanism try to solve the puzzle simultaneously and only the winner of the race has the right to add the next block onto the blockchain. Every new block contains the so-called coinbase transaction, which awards the winner with a block reward in the form of newly created bitcoins (Antonopoulos 2017: 51). This is the only way new bitcoins get created (Nakamoto 2008a: 4). The result of the puzzle can then be checked in turn by all the other network participants with very little effort (Antonopoulos 2017: 50). The ease of verification and the high costs involved in solving the puzzle keep the miners honest and secure the integrity of the transaction history (Catalini/Gans 2016: 1). Only for propagating correct blocks can miners earn the block reward and thus refinance the electricity costs incurred while solving the puzzle. Dishonest miners who include fake transactions in the block are quickly recognized by the network. The blocks propagated by them are not accepted as part of the database by the other network participants – the electricity costs were thus expended "for nothing." Thanks to this combination of signed transactions and a mathematical puzzle whose solution is incurred at a high cost, the Bitcoin network has succeeded in maintaining a common database of assets for over ten years without a central authority having to, or being able to, intervene in the process.

Even as Bitcoin has achieved a market capitalization of over 500 billion euros in less than ten years and deemed legal tender in September 2021 by El Salvador, the first county to do so (The Economist 04 September 2021), there is a great deal of worldwide criticism of this currency without a currency authority. Justified criticism of the network is widespread and can be divided into three categories: environmental impact, its use by criminals, and missing properties of a genuine currency.

## Impact on the Environment

Undoubtedly the biggest point of criticism of Bitcoin currently concerns the network's enormous carbon footprint (Ebert et al. 2021). The described proof-of-work mechanism protects the integrity of the database through the energy use that is required for solving the puzzle and that gives rise to substantial costs for participants. Before the mining ban imposed by China's autocratic government, the bitcoin network consumed around 175 terawatt hours of electricity per year (Cambridge Center for Alternative Finance 2021). This is the equivalent of around 1,720 kilowatt hours per transaction (Digiconomist 2021) and is, in comparison to the likewise global Visa network, 1.16 million times more energy intensive (De Best 2021) than the processing of a single credit card transaction.[2] Even if overall Bitcoin only uses barely 0.1 percent of the global energy supply and, according to a study by the US-Bitcoin Mining Council – a lobbying group that represents nearly 32 percent of the network's mining power – relies on renewable energy for over 55% of its energy needs (Bitcoin Mining Council 2021: 9), numerous investors are turning away from the network due to its environmental impact. In addition to overall energy consumption, the enormous wasting of energy in the network is a particular target of criticism. Since only one miner can win the race for the next block, but the whole network expends the processing power and all computers are engaged in the same activity, 99% of the energy used is more or less wasted. Besides the massive carbon emissions and the great waste of energy, the proof of work mechanism and mining are also the target of criticism for high resource use. Thus, for instance, the massive need for computer chips for mining is increasing the pressure on existing supply bottlenecks for semiconductors (Ebert et al. 2021: 1).

## Money for Criminals?

Besides energy use, Bitcoin has always been subject to criticism that it is a currency for organized crime and that anonymity within the network would help to get around money laundering regulations or regulations for preventing terrorist financing (Foley et al. 2019; Hagelüken 2020: 147). Reference is regularly made here to the possibility of using Bitcoin on the "Silk Road" platform to be able to pay for illegal goods and services (Adler 2018). A recent analysis by the blockchain analytics firm Chainalysis suggests that in 2021 less than 0.2 percent of cryptocurrency transactions have been connected to illegal activity – significantly less than the 5 percent of global GDP that, according to United Nations research, is connected to money laundering (Grauer et al. 2022: 5; Kaul et al. 2021: 18). Other studies arrive at a higher share for the bitcoin network, but point to the fact that as the use of Bitcoin is increasing, its use for criminal purposes is decreasing (Foley et al. 2019). The fact that Bitcoin is nonetheless known as money for criminals is probably to be explained, on the one hand, by the growing number of ransomware attacks in recent years in which blackmailers regularly demand ransom in Bitcoin (Ip 2021). On the other hand, however, this skepticism can also be attributed to a widespread misconception about the properties of Bitcoin transactions. Every transaction is documented in the Bitcoin network, the transaction database can be consulted by everyone, and hence it can also be used by law enforcement agencies for the purpose of investigations. The "paper trail" that is thus created led, in the end, to the identification and

2 Comparing a VISA transaction to a bitcoin transaction is not entirely appropriate and is only used here for the purpose of illustration. Whereas a VISA transaction only gives rise to a claim between financial service providers, a Bitcoin transaction is final and does not require any further infrastructure for processing. In the VISA system, the involvement of numerous financial intermediaries as well as governmental agencies is required for the complete processing of a payment and the corporate organization of VISA itself is hardly climate-neutral. Consequently, the real energy costs for processing a VISA transaction are significantly higher than the server costs of an individual transaction considered here.

conviction of the operator of the Silk Road (United States Court of Appeals, Second Circuit 2017; Rogoff 2016: 214) and made it possible for the FBI to recover a large part of the ransom involved in what is undoubtedly the best-known ransomware hack to date (Uberti 2021). Despite this, there is no doubt that Bitcoin, like any other currency, can also be used for criminal activities. Beyond the attention-grabbing drug sales or contract murders, however, the extent to which it is appears often to be overestimated by the public. According to Citigroup research, a comparatively low 2 percent of all Bitcoin transactions are used for illicit purposes, whereas no less than 2 to 5 percent of all transactions in established currencies are used for money laundering (Kaul et al. 2021: 18).

### Not Real Money

Of the three functions of money, Bitcoin, at least up until now, does not fulfill any of them to a sufficient extent. Given its high volatility, limited dissemination, and lack of scalability, it is thus far less suitable as medium of exchange or as unit of account. Due to high demand, however, and an absolute limitation of supply, Bitcoin is often referred to as digital gold and is used more and more as a form of investment. Only the future will show whether this will be enough in the long run for it to function as a means for storing value. In the first wave, in any case, the focus was more on the innovative technology and the independence from intermediaries and from the existing financial system and less on functionality in terms of a conventional understanding of money.

## 2.2 Second Wave: Internet Money, The Emergence of Programmable Currencies

### From Bitcoin to the World Computer

Not even two years after the publication of the white paper, Nakamoto and numerous fellow developers who had joined the project early were discussing further areas of application for the technology (Werbach 2018: 55). If digital money without a central controlling authority was possible, why should it not also be possible to program it or to use the technology for transferring other assets and information (Pilkington 2016: 13)? In 2011 a domain name registration system called "Namecoin" was developed and initially built on the Bitcoin network with a technique called "colored coins" that adopted all the properties of the network, such as its resistance to censorship (Bradbury 2013). In the case of "colored coins," the bitcoins contain additional information, which, like the bitcoin itself, can be exchanged between participants and makes it possible for other assets, like shares or property rights, to be moved around on the decentralized network (Rosenfeld 2012: 7).

In 2013, the Bitcoin developer Vitalik Buterin took the idea of "colored coins" a step further. Buterin thought of using the technology not only to transact other forms of assets, but to run full-fledged software programs on decentralized system, thus allowing for uncensorable smart contracts. After the publication of the conceptual white paper by Buterin, Gavin Wood followed up in 2014 with the yellow paper containing the technical specifications for the new system called Ethereum. The first block of the new blockchain, also known as the world computer, was published in late July 2015. The Ethereum blockchain essentially works like the Bitcoin blockchain with its own form of money: the cryptocurrency Ether. As of now, it still relies on a similar proof-of-work process, although the development of a far more resource-efficient proof-of-stake mechanism has long been underway, and it appears that the transition may take place this year.[3] Unlike Bitcoin, Ethereum has a Turing-complete programming language in the form of Solidity. Not only is it possible to attach additional information to the Ethereum blockchain, but it is universally programmable making it a general purpose technology, which can influence and change numerous economic sectors (Werbach 2018: 72). With the help of smart contracts and thanks to the ERC-20 token standard with the Ethereum Improvement Proposal 20 "colored coins" can be easily created on the Ethereum platform since 2015 (Yilmaz 2021). For the purpose of distinguishing between the different forms it has become common practice to refer to the currency of the protocol as a coin and to "colored coins" issued on the protocol as tokens (Nowak 2021). An ERC-20 token exists independently on the Ethereum blockchain and, like the protocol currency Ether, is managed by users via public and private keys. The trades with the token are secured by the underling protocol's consensus mechanism and it can be used in smart contracts running on the blockchain.

In the meantime, an enormous ecosystem has been built up around Ethereum, in which loans are handed out among strangers, online advertising is being organized without a central authority like Google, and in peer-to-peer markets bets are made on real world events to predict future outcomes.

Whereas the Bitcoin network continues to exist, without any formal governance institution and is still managed through an informal process that involves developers, miners and users and relies entirely on volunteers, the Ethereum network has some degree of institutionalization. Shortly after the white paper was published, a foundation was established under Swiss law which raised over 31,000 bitcoins in a crowdsale for the protocol development (ethdocs.org 2016). Although the Ethereum Foundation has no formal authority over the blockchain protocol and, as in the Bitcoin network, decisions always have to be endorsed by the community of miners and users, its existence creates a certain concentration of influence. Just the financing of developers, who work has considerable influence the protocol evolves, already

3 Proof-of-stake relies on a type of security deposit to ensure the integrity of the database instead of high energy use. Miners have to deposit large sums of cryptocurrency, which are destroyed in the event of dishonest behavior or attempts at manipulation. Like in the case of proof-of-work, this ensures that dishonest behavior does not pay and gives rise to high costs in terms of lost assets.

converts the foundation into a key instance within the network. Its influence in the informal decision-making process is surely at least comparable to that of major shareholders in a corporation.

### Smart Contracts

The idea of programmable money or even completely digital contracts is far older than the blockchain technology itself. In the 1990s, the American legal scholar and computer scientist Nick Szabo already published his initial ideas for so-called smart contracts (Szabo 1996). The blockchain technology as an irreversible and incorruptible publicly shared repository of information now makes it possible to apply the concept reliably for the first time (Wright/De Filippi 2015: 2). According to Szabo, a smart contract represents a series of promises that are formalized in digital form and include an autonomous enforcement mechanism (Szabo 1996). Among German legal scholars, a definition of Kaulartz and Heckmann is increasingly well received. They describe smart contracts as software that guides legally relevant actions contingent on digitally verifiable events and that is also used to conclude contracts (Kaulartz 2016: 618). The example of a vending machine that ejects a product when someone inserts a coin and presses a button is often used to illustrate smart contracts. Smart contracts are supposed to be the vending machines of the Internet, so to say. They allow the implementation of autonomous contracts involving digital goods where the risk remains largely limited to malfunctioning of the technical instrument employed, and a breach of the contract or manipulative behavior after the contract has been concluded is almost entirely ruled out.

A digital currency is essential for carrying out the exchange of services with smart contracts. Currently, all the well-known smart contract platforms like Ethereum, Cardano and Solana have their own cryptocurrencies to make the use of smart contracts possible. Nonetheless, completely intermediation-free trading is not (yet) possible, since users still depend on intermediaries for the conversion of central bank money into the cryptocurrency in question (Werbach 2018: 75).

### Potential, Function and Challenges

Smart contracts and programmable money within decentralized networks gave light to the promise to roll back the centralization of the Internet, which initially started as a peer-to-peer network, and was supposed to enable peer-to-peer collaboration in the digital world independent of large intermediaries (Wright/De Filippi 2015: 1). Nowadays, even though it started as a decentralized freedom project, the internet is shaped by central intermediaries such as Google, Facebook and Airbnb, which allow users to propose commercial applications on the Net. These intermediaries reduce the transaction costs for users, create trust between strangers, and process the transfer of value. The blockchain technology is often also described as a trust technology, because it creates a new form of trust between strangers using cryptography and smart incentive mechanisms: trust that until recently could only be created by intermediaries (Werbach 2018: 20).

Besides the re-decentralization of the Internet, proponents of the technology expect that there will be numerous other areas of application going well beyond the digital world. Starting with the democratization of corporate organizations in the form of decentralized autonomous organizations (DAO) (Wright/De Filippi 2015: 15), some even consider the realization of global government to be possible (Shapiro 2018) or want radically to revolutionize the financing of public goods with the help of market forces (Buterin/Hitzig/Weyl 2018).

## 2.3 Third Wave: The Appearance of Stablecoins and Platform Currencies

Cryptocurrencies are known to the general public not only for their use in criminal activities, but often also due to their extreme price fluctuations. In the first half of 2021 alone, the value of a bitcoin fluctuated between 54,000 and 24,000 euros. An ether was worth 600 euros at the beginning of the year and rose to as high as 3,500 euros for a time, before falling again to 1,500 in June 2021.[4] Daily price fluctuations between 5 and 10 percent are not unusual for cryptocurrencies with a high market capitalization – and for the hundreds with low market capitalization, even greater fluctuations are more the rule than the exception. As a result of such enormous fluctuations, dependable trading with cryptocurrencies and using them as unit of account, like a central bank currency, is nearly impossible. Due to the need for on-ramping and off-ramping,[5] users of cryptocurrencies must repeatedly rely on central intermediaries and are thus forced to leave the cryptosphere, which is exclusively controlled by program code, in order to store value in stable units of account.

### Stablecoins

Over the years, a real need has led private actors to try to use different approaches to create stable cryptocurrencies. Most of these are linked to the American dollar and are known as stablecoins. Thus far, two approaches have prevailed, which are distinguished, above all, by their degree of centralization. All versions of currently existing stablecoins are issued as tokens on already existing blockchains. All the stablecoins mentioned in what follows exist at least as ERC-20 tokens on the Ethereum blockchain.

On the one hand, there are numerous stablecoins that are issued by a central authority. In this case, the intermediary

4 Data from https://coinmarketcap.com
5 On- and off-ramping is often used to refer to the process of switching between central bank money and cryptocurrencies. Users are dependent upon large intermediaries as financial service providers, who, for example, convert euros into cryptocurrencies for often high fees.

issues cryptocurrencies and holds reserves in the issued reference currency in return. These stablecoins, which are often referred to as "fiat-pegged", are essentially distinguished by the sort of reserve. The reserve of the USD-coin, which is issued by circle in partnership with the crypto exchange Coinbase, is filled with US dollars at a 1:1 ratio and undergoes monthly independent audits (Grant Thornton LLP 2021). By contrast, in the case of the oldest stablecoin Tether, which is closely connected to the crypto exchange Bitfinex, the coins in circulation are only partly backed by reserves, with the reserve largely consisting of short-term cash equivalents such as debt securities and at least 10 percent of it consisting of pure loan guarantees (De/Hochstein 2021). In addition to being criticized for the composition of its reserve, Tether has also long been criticized for the lack of transparency of its reserves and has yet to present an independent audit report (Yue 2021).

On the other hand, there are also relevant stablecoins that are not issued by an intermediary, are not backed by central bank money, and are entirely administered in the crypto ecosystem. On example is the DAI stablecoin that is supposed to be stabilized by depositing other cryptocurrencies in a smart contract on the Ethereum blockchain, in order for it to always represent the value of one dollar. Its stability is made possible by a complicated system of incentives, which, by giving users the opportunity to make profits through arbitrage when there are deviations from the reference value, compels them to restore the correlation with the reference value thanks to their purchases and sales (Shekhar 2018). The DAI token is not managed by a central intermediary, but rather is issued and administered exclusively by way of smart contracts. The smart contracts are administered in turn by MakerDAO. When there are problems with the decentralized arbitrage system, MakerDAO can use its own reserves of cryptocurrencies to intervene in the price mechanism via purchases and sales. MakerDAO itself is not a typical intermediary as it consists exclusively of a combination of smart contracts and an incentive system for encouraging collaboration and can hence be described as a decentralized autonomous organization.

## Platform Currency

Apart from stablecoins, which are essentially meant to enable trading within the crypto ecosystem, there have also in recent years been repeated efforts made by individual platforms to issue their own means of payment for trading on the platform (Brunnermeier et al. 2019; Hagelüken 2020; Leibbrandt/De Teran 2021). Facebook's announcement that it will launch its own currency in partnership with numerous global companies was particularly big news (The Economist 2019a). The announcement created an enormous uproar among legislators, regulators and central banks around the world at the time and has been met with stiff resistance since then (Partington 2019; The Economist 2019b; Hagelüken 2020: 150). The project has not only changed its name, but the originally planned 2020 start was postponed until some unknown future date (Morse 2021). At the same time, the idea of a global and independent currency is being transformed more and more into a dollar stablecoin with Facebook as the issuing intermediary (Morse 2021). The fierce resistance from regulators in the United States and European Union and the lack of a viable use-case led to Facebook abandoning the idea in 2022 (Heath 2022). Facebook (since 2021: Meta) wants to focus on combing its services to create a Metaverse, a special kind of virtual reality, in which it will most probably let users pay in various digital currencies and charge fees on transactions (Van Boom 2022).

When even companies as powerful as Facebook, despite grand announcements, have difficulties getting such a project to the starting line, it would appear extremely doubtful that platform currencies would have any relevance at all in the long run. The resistance of nation states fearing for their own monetary sovereignty appears to be an enormous hurdle. As a reaction to Facebook, the European Commission introduced the Markets in Crypto-Assets-Regulation (MiCA) which mainly focused the regulatory efforts ensure financial stabilities for projects like DIEM/Libra with compliance and transparency requirements equal to big banks and European supervision for issuances with cross-border relevance. Even though Facebook most likely would have been able to comply with the regulation, interest groups representing small and more crypto-native projects like MarkerDAO voiced skepticism about the scope of the regulation as it might harm innovation, lead to prohibitively high cost for smaller projects.

At the same time, the concrete purpose for projects for single-platform currencies seems questionable. Thus, for example, the announcement by the American bank JPMorgan Chase & Co that it would be launching a digital currency of its own called JPM Coin attracted a great deal of attention, but here too observers have doubts about its actual utility (Leibbrandt/De Teran 2021: 207). Gaming platforms that give users the possibility of paying for extras with cryptocurrencies, trading their winnings beyond the borders of a platform or even of creating the infrastructure with which video players can be paid for their erstwhile strictly private enjoyment are a somewhat different matter (Rixecker 2021). They may become more relevant if the Metaverse will be built openly and with a focus on composability instead of being run by central intermediaries such as Meta. Some first projects of this sort have been brought to market and investors have shown great interest (Haigh/Ahmed 2021). Even if the use of blockchain technology raises further questions here, the topic as such is not new from a monetary perspective and also has been discussed by legal scholars and courts for several decades already (Lober/Weber 2005).

## 2.4. The Current State of Digital Currencies

The first three waves demonstrate the diversity of digital currencies and their technical maturity. They depict the constant evolution of this new form of currency and serve to classify the different currency waves along the lines of function, organizational form, governance and value source. New functions are added with each wave or there is a shift in their usage. In the first three waves, private actors are responsible for the emergence of digital currencies without there being any major governmental influence. Most of them are based on blockchain or distributed ledger technology and can be described as cryptocurrencies in light of their technical structure.

Fundamentally, currencies derive their value from trust. In the case of the currencies of the first and second waves, this trust is trust put in the technology: i.e. the cryptographic protocol and the consensus mechanisms. The third wave adds the need for trust in an issuing instance, which issues the currency on the infrastructure of the first and second waves. In the third wave stablecoins, the trust in the issuing instance is based on actual backing by national currencies or a basket of currencies or more computer protocols. None of the three waves are completed yet; particularly the currencies of the second and third waves will continue to undergo significant evolution. In a commentary, The Economist thus described the open-source system Ethereum with its Ether currency as a "self-improvement machine" due to its capacity for adaptation (The Economist 18 September 2021). In any case, the waves can be expected to continue to run concurrently for quite a while still.

**Table 1 | Overview development of digital currencies**

| | Function | Organizational form | Governance | Value |
|---|---|---|---|---|
| **1. Wave: Bitcoin** | Not clear | Open | Open | Trust in protocol (PoW) |
| **2. Wave**: **Programmable money** | Medium of exchange + NEW: Smart Contract | Open | Open | Trust in protocol (PoW; PoS) |
| **3. Wave**: **Stablecoins** | Store of value + unit of account | Private or decentralized | Club or open | Trust in issuing instance or incentive structure and technical protocol |
| **4. Wave**: **Digital central bank money** | Store of value + unit of account + medium of exchange | Open | Club | Trust and embedding in state institutions |

So far, however, none of the digital currencies of the first three waves has been in a position completely to fulfill the three classical functions of money: the function of medium of exchange, that of unit of account and that of store of value.

Only government-issued central bank money has been able to do this to date. In the upcoming fourth wave, it is precisely this actor, the state, that begins to develop a digital form of fiat money: viz. digital central bank money.

# 3. Back to the Future: Central Bank Digital Currency

The rise of private digital currencies has not left the established national or supranational currencies untouched. Originally dismissed as a niche product, in the second wave at the latest, central banks and regulators recognized the implications that the digital transformation can also have for traditional currencies. Initially, regulators and authorities were interested in the possible misuse of digital currencies for illicit transactions like drug trafficking and terrorist financing. However, central banks have also long since identified potential uses and risks for monetary policy. Specialists regard it as a sure thing that there will also be digital central bank money – or, as it is usually referred to, Central Bank Digital Currency (CBDC) – in the near future (Rogoff 2016; Carney 2021: 117). Most central banks are already exploring digital versions of their currencies – some are already in the development and trial stage and others have rolled out first iteration already. Among major economies, the People's Republic of China is currently furthest along in developing digital central bank money (Work 2020; 2021). The world's oldest central bank, the Swedish Riksbank, has also already entered the pilot phase for its e-Krona. In July 2021, The European Central Bank announced that it was starting a two-year trial period for a digital euro. The Bank of Japan is already testing a digital yen, whereas the Bank of England is still in the research phase. The American Federal Reserve has thus far been the most hesitant of the four largest central banks, but is also now evaluating a digital version of the dollar. Some states have already launched their digital currencies. The Central Bank of the Bahama has fully launched the Sand Dollar in 2020 and the Central Bank of Nigeria followed in October 2021 with the launch of the e-Naira. Altogether, more than 80 central banks representing over 90 percent of global GDP are involved in developing CBDC (Atlantic Council 2021). This development ushers in a new currency era, in which different currencies and forms of currency could again come into far heavier competition with one another in a single currency area. There will be a number of digital currency projects in this new wave, which has only just begun: some of them will form part of the first three waves, some will disappear from the market after a time, and others will tend to fit into the existing financial system. The fourth wave thus involves a return to the decisive role of central banks in the monetary policy of this new form of currency, but also an entirely new competition between private and public, i.e. government-issued, forms of digital currency, on the other.

## 3.1 The Central Banks Get Involved

For decades, central banks were the key players in monetary and currency policy. Since the global trend toward independent central banks and the global financial crisis, they have been regarded as "the only game in town" (El-Erian 2016). At the same time, however, private actors were largely responsible for the innovation around money and especially of forms of payment (Leibrandt/De Teran 2021). From the emergence of banknotes to checks, credit and debit cards to modern payment service providers like PayPal, Alipay and Klarna, private actors have often had a decisive influence on how people use central bank money. As long as cash was the most important means of payment, central banks could observe these developments without being disturbed: the guardians of the currency were still in a position to supply people in the currency area with central bank money in the form of coins and notes. This is changing, however, as cash is increasingly losing its significance in payment transactions and in everyday life.

Central bank digital currency would significantly differ from money in an online bank account or payment with a debit card. First, it is important to understand here that money in a checking account is different form of money than cash. A coin or banknote represents a claim on the central bank and hence is regarded as "the ultimate risk-free asset," whereas bank deposits only represent a claim on the bank that is administering the account (Carney 2021: 118). In several jurisdictions this claim on the bank is legally guaranteed. The US and the EU guarantee up to 250,000 dollar or 100,000 euro per person and financial institution. Hitherto, people's interaction with the central bank has been mostly indirect and has been shaped by the financial system as an intermediary. Although central banks issue coins and bills to commercial banks, administer the central bank reserves of these commercial banks, and try to use their monetary policy to keep the value of the money stable, private actors are in fact largely responsible for the creation of money by, for instance, procuring new money for non-financial actors (for example, businesses and consumers) through loans. This is not a problem as long as people can pay with the cash provided to the private bank by the central bank. However, the more payment transactions move into the digital domain, the more the possibility for central banks to provide a reliable means of payment in the event of a crisis diminishes. This is where the development of central bank digital currency comes into play: As the digital equivalent of traditional central bank money in the form of coins and bills, it would represent a direct claim against the central bank and guarantee the finality of a digital payment (Auer/Böhme 2021: 5; BIS 2021: 70). It would give people access to a universally accepted means of payment even in the event of a crisis. This distinguishes central bank digital currency not only from established "electronic money," but also from the digital currencies of the other waves.

Regardless of the chosen technology, central bank digital currency derives its value from trust in the issuing state or organization of states, as well as the issuing institution, and not from being backed by a basket of currencies, a particular database technology or cryptographic computer protocols. In contrast to privately issued digital currencies, central bank digital currency has a central entity in the form of the central bank, however uses similar technologies as privately issued digital currencies. To what extent intermediaries such as commercial banks are still needed for payments largely depends on the technical design. Only a digital currency whose value is guaranteed by the central bank is considered real digital central bank money (Auer/Böhme 2020: 92). Moreover, a central bank digital currency is in principle meant to fulfill all three functions of a currency as medium of exchange, unit of account and store of value. The extent to which it is able to fulfill these functions depends on choices regarding its technical and organizational design.

The issuing of central bank digital currency would represent a transformative change for the existing monetary system. Depending on its design, central banks would thus enter into competition with means of payment and other financial products within their currency area. This could destabilize the existing two-part monetary system composed of central banks and financial institutions as intermediaries on the one side and non-financial actors on the other. Central banks have many different motivations for their involvement in the world of digital currencies (Bofinger/Haas 2020; Kiff et al. 2020). First, central banks point to the loss in significance of cash that was already described above. In Sweden, the cash usage massively declined to below 20 percent in the recent years and was one of the main drivers behind the development of the e-Krona. This common decline of cash limits central banks' possibilities for action during economic crises and makes citizens even more dependent on private intermediaries. The creation of CBDC is meant to prepare for such an eventuality in time. On this reading, the introduction of CBDC would contribute to a stable and resilient payment and financial system and ensure that central bank money is always available for use (Gross et al. 2020b: 547). A related motivation, which is especially relevant for developing countries, is the promotion of financial inclusion by giving people without bank accounts access to the possibilities of digital payment and value storage, as well as numerous other financial services (Allen et al. 2020; Leibbrandt/De Teran 2021: 212). Other motives include creating a straightforward channel for the transmission of monetary policy stimuli, fostering the digitalization of their respective economic area, combating counterfeiting and illicit transactions, as well as warding off the danger that digital means of payment of private providers or foreign central banks could secure a dominant position in their respective currency area or strengthening the international role of their own currency (Bofinger/Haas 2020; Allen et al. 2020; ECB 2020). The extent to which these goals can be achieved, in whole or in part, fundamentally depends on how the central bank digital currency is designed.

## 3.2 Design Options for Central Bank Digital Currency

The previous three waves make clear the diversity of digital currencies – there are, accordingly, different ways of shaping digital central bank money. The options for digital central bank money discussed thus far are largely distinguished by their access to CBDC, the technical design, the technical infrastructure and the architecture on which the digital central bank money is based (Allen et al. 2020; Auer/Böhme 2020; 2021). These differences correspond to the different requests made on the new digital central bank money and have implications for its attractiveness as a complementary or alternative means of payment.

### *Access to Central Bank Digital Currency Wholesale or Retail*

The most decisive issue for banks and consumers undoubtedly concerns access to new central bank digital currencies. Up until now, the latter have only had access to cash or money via intermediaries (Auer/Böhme 2021). For the new digital central bank currency that is being developed, central banks are faced with the question of whether to enable people to have direct access to the new currency or still only indirect access via intermediaries like commercial banks. The distinction is made here between a retail CBDC (direct access) and a wholesale CBDC (indirect access) via intermediaries (Allen et al. 2020; Groß et al. 2020b: 545; Prasad 2021: 12). A retail CBDC would amount to a sort of digitization of cash, with people either having direct access by way of an account at the central bank or being able to hold and use the units of the digital central bank money on their own without intermediaries (Groß et al. 2020b: 546). A wholesale CBDC, on the other hand, would not change much for all actors: Users would still have to rely on special intermediaries like commercial banks or other financial institutions to access wholesale CBDC, and the CBDC would be used then, above all, on the interbank market and not as a general means of payment. Financial institutions with access to wholesale CBDCs could offer accounts that are 100 percent backed by central bank digital currency and thus be as similarly low-risk as traditional central bank money, allowing them to serve as a "safe asset" (Bofinger/Haas 2020: 3). The introduction of wholesale CDBC would though have little impact on the existing system of payment. The two-part monetary system, in which financial institutions act as intermediaries between central bank money and non-financial actors, would remain untouched. The introduction of a retail CBDC offers greater potential for far-reaching changes, since in this case non-financial actors would in theory no longer have to rely on banks as intermediaries to hold and

use central bank money. The impact of a retail CBDC on the two-part financial system would depend then on its technical design, and hybrid models are also conceivable.

## *Technical Design: Account- or Token-Based*

Apart from the two forms of access, central banks are faced with a decision on what forms of use the technical design should make possible. There are two options here for retail CBDCs. On the one hand, retail CBDCs can be designed as direct means of payment or exchange between users like cash: i.e. for peer-to-peer (P2P) payments. On the other hand, exchange could take place via accounts administered by the central bank (Bofinger/Haas 2020: 11; Auer/Böhme 2020). Digital central bank money that is designed for P2P use is referred to as value-based or token-based CBDC (Bofinger/Haas 2020: 11; Auer/Böhme 2020). This token-based CBDC is the closest thing to cash, since individual CBDC units (tokens) are used for payment or as means of exchange. Like coins or banknotes, the tokens have a definitive value, which is transferred from one wallet to another along with the token. Token-based CBDCs can also be used offline in principle, they do not require identification, and they can only be spent once thanks to the use of cryptography. The alternative would be an account-based CBDC, where the central bank itself maintains accounts and intermediaries (wholesale CBDC) or individuals (retail CBDC) can move around funds, like in the case of bank transfers, or use the account to store value (Bofinger/Haas 2020: 11). Depending on the model of access (wholesale or retail), account holders can transfer money either directly or indirectly, although, in contrast to normal bank transfers, what is transferred here is central bank money instead of giro money. Moreover, an account-based CBDC can be used as a "safe asset," with central bank digital currency serving as a digital store of value analogously to the proverbial "money kept under the mattress" (Bofinger/Haas 2020: 11). Like with money kept under the mattress, there is, particularly in the retail variant, the problem that this money cannot be used for value creation when it is in the central bank's account. Hence, in the case of a variant combining retail and account-based CBDC, the central bank should decide to what extent digital central bank money earns interest and whether there is an upper limit to the amount of CBDC that users can hold in the central bank account. If central bank digital currency yields a level of interest similar to that of a bank account, a "crowding-out" effect might arise, whereby the public CBDC account could displace private forms of investment, resulting in the withdrawal of important investment capital from the market if lucrative new forms of investment do not appear quickly enough (Agur et al. 2019: 3; Bofinger/Haas 2020: 12). Moreover, there would also be the possibility of enhanced capital flight into central bank digital currency and hence a greater probability of a bank run in the event of a financial crisis (Bindseil 2019: 318).

There are different proposals for counteracting this. For instance, in a working paper, Ulrich Bindseil, the ECB's Director General of Market Infrastructure and Payments, suggests a two-tier model, in which in first tier CBDC deposits up to a value of 3,000 euros get the same interest as conventional central bank money, and deposits above this amount receive a 2 percent lower interest (Bindseil 2020; Bofinger/Haas 2020: 23). The Zero Lower Bound, i.e. 0 percent, is regarded as the lower limit for interest in this proposal (Bindseil 2020: 25). In a low interest rate environment, however, there would also in theory be the possibility of negative interest above a certain level of deposits, so that a fee would be charged when central bank digital currency is used as the equivalent of money kept under the mattress. Furthermore, the choice for either token- or account-based CBDC also has implications for the anonymity of transactions: payments that are mostly anonymous, like payments in cash, would only be possible with a token-based CBDC. Identification would always be required to authorize transactions with account-based digital central bank money. The transaction can only executed, if the account holder is identified and the sum to be transferred is covered by an equivalent amount of CBDC-deposits. In the case of value-based (token-based) CBDC, the transaction is verified in principle by way of the individual token, which only to a limited extent allows conclusions to be drawn about the persons involved. Depending on the technical design, the token can usually only be traced back to the sender or third parties with great difficulty. The anonymity of payment is then comparable to cash. Hybrid models are also possible here, however.

## *Technical Infrastructure: Distributed Ledger or Conventional*

The section on the first three waves of digital currencies already introduced the blockchain as a form of distributed ledger technology (DLT), on which decentralized currencies are based. In simplified terms, DLT is a form of decentralized distributed accounting, in which the ledger is comparable to the register in which a bank, records all transfers of their account holders. In a decentralized distributed accounting system, different nodes in dispossession of the whole ledger arrange and verify transactions without necessarily knowing the people with whom they are jointly administering the register. Even if central bank digital currency is by definition not a decentralized project like most cryptocurrencies, a CBDC can also be based or placed on decentralized distributed ledger technology. A critical choice has to be made about the technical infrastructure for central bank digital currency is the choice between a conventional and a DLT-based infrastructure (Auer/Böhme 2020: 91). In the first place, every form of digital money requires decentralized accounting, since the information about transactions and deposits must be available on different devices and small transactions at least have to be also possible without an Internet connection. The biggest

difference is related to who is responsible for the accounting and has the right to create new entries: i.e., who propagates, validates, and updates transactions in the databases to avoid the problem of double spending (Auer/Böhme 2021).

In the conventional or centralized model, there are decentralized databases in which transactions and balances are recorded, but only one node is authorized to write to the databases, i.e. to update them to add transactions. This requires a central authority that can validate a transaction based on the identification of the account holder (account-based CBDC) or the validity of the individual token (token-based CBDC). In the account-based variant, balances and transactions are recorded in accounts administered by the central bank in the same way as bank balances or classical bank transfers. The difference from the existing system would, above all, be that private individuals could also open accounts for central bank digital currency at the central bank (Dyson/Hodgson 2016: 4). For token-based CBDC, the central bank maintains a technical infrastructure that, when tokens are disposed of, allows it to check their current value against a central database. This variant would be based on already existing conventional payment systems like, for example, the ECB's TARGET Instant Payment System (TIPS). This system is part of the ECB's market infrastructure and is intended to process large volumes of payments directly. The ECB is evaluating the TIPS as a possible alternative infrastructure to DLT for a digital euro.

In the case of a decentralized infrastructure based on distributed ledger technology, the basic rules for currency use, transactions and data would be centrally determined, but the transaction database itself would be updated with a decentralized network. Unlike in the central variant, there would not be any top central node in this network, but rather many network nodes that validate transactions using an algorithm – or, more precisely, a consensus mechanism (Auer/Böhme 2020: 92). In this regard, value-based central bank digital currency (token-based CBDC) with DLT technology is built on cryptographic methods like the cryptocurrencies of the first waves. The CBDC token transfer would be authorized using asymmetric encryption. As with the digital currencies of the previous waves, there are different ways of arriving at consensus among the different network nodes. In the case of CBDCs, these network nodes could be previously designated authorities such as individual central bank branches or, in a hybrid form, private financial institutions. The central bank could also build or use a DLT-based network and distributed validation instances to validate transactions in an account-based CBDC-system. In a DLT-based CDBC, the network on which the CBDC tokens reside can also be an already existing blockchain like, for instance, Ethereum. In this case, verification of transactions takes place on and within the existing blockchain network, the central bank would only centrally manage the money supply and the rules for using the CBDC.

**Table 2 | Different forms of digital central bank money**

| | Central Validating Authority | Distributed Ledger Network |
|---|---|---|
| **Token-based CBDC** | Central CBDC tokens | DLT-based CBDC tokens |
| **Account-based CBDC** | Central CBDC accounts | DLT-based CBDC accounts |

Source: Own presentation based on Bofinger/Haas 2020; Lee 2021; Auer/Böhme 2020; 2021

In all four cases, the central bank must guarantee the value of the currency for it actually to be central bank digital currency. The accounts are centralized central bank accounts in the case of a CBDC whose transactions require identification (centralized account-based CBDC) or DLT-based accounts in that of decentralized validation (Auer/Böhme 2020: 92). No identification is required, on the other hand, for payments in the case of token-based CBDC with a decentralized network or centralized database; here (any sort of) technical validation is sufficient, and this technical validation does not have to be linked to a particular identity. Using a decentralized network and token-based CBDC appears to be the most promising way of achieving a form of central bank digital currency that is as much like cash as possible. Hybrid forms can also connect DLT-based token-based CBDC to centrally or decentrally administered CBDC accounts. Of the CBDCs that are thus far in the pilot phase, the e-Krona in Sweden and the digital version of the South Korean Won are being planned as DLT-based CBDC. The European Central Bank is using the trial phase to figure out which infrastructure works best for a digital euro. Much the same applies for other central banks like the Federal Reserve, the Bank of Japan and the Bank of England. The choice of the technical infrastructure used depends here on the desired function, but also on the architecture in which the digital central bank money is supposed to be embedded in.

## *Architecture*

The introduction of central bank digital currency confronts central banks with entirely new challenges, since in connection with the aforementioned choices they have either

to prepare a completely new infrastructure or to build on an existing one: for instance, an existing blockchain from the second wave. The hitherto existing two-part monetary system – consisting of central banks and commercial banks – is largely based on the financial infrastructure of commercial banks and other financial institutions (Groß et al. 2020b: 545). The latter are supposed to transmit monetary policy stimuli and serve as intermediaries between central banks and the "real economy." They are, so to say, the infrastructure used by the central bank and the mode of access to the system for non-financial actors (Hilgers 2021: 187). The significance of intermediaries would remain undiminished in the case of a choice for wholesale CBDC and it could even increase if synthetic CBDC were to be offered: i.e. a digital currency backed by wholesale CBDC. There still would not be direct access to central bank digital currency for individuals and businesses, because the form of digital currency available to them does not represent any direct claim on the central bank. Things look different, however, in the case of retail CBDC. In an analysis for the BIS, Auer and Böhme (2021) distinguish between single-tier and two-tier retail CBDC. In the single-tier or direct retail CBDC, the entire payment system is maintained by the central bank and payments are processed on a specially prepared or designated DLT-based or conventional infrastructure. Intermediaries like commercial banks would not necessarily be required in the direct variant, but they could be used by individuals or businesses, for example, to facilitate access to and administration of their wallets in the form of a classical account. In the case of the two-tier or indirect CBDC, the central bank would, as before, only provide the infrastructure for intermediaries and process payments. The intermediaries, on the other hand, would be responsible for providing "accounts" and payment processing; they would continue to be the point of access to the financial system for individuals and businesses. Like cash, however, the money they receive or hold would constitute a direct claim on the central bank.

Other aspects of the architecture are related to verification of identity and legitimate ownership in the financial system, which is called "know your customer" or the KYC principle for short (Allen et al. 2020: 25). Financial intermediaries are usually required to verify the identity of their customers to prevent illicit transactions, money laundering and terrorist financing. Digital currencies in particular are often suspected of being misused for illicit transactions, and central bank digital currency also requires mechanisms that secure this principle to some extent. At the same time digital central bank money is expected to approximate the anonymity of cash. In the context of the technical infrastructure, both single- and two-tier CBDCs can employ intermediaries to secure the KYC principle. The technical design also allows for models in which up to a certain sum can be used anonymously per day or certain transactions can only be executed by way of a verified account.

On all issues, choices about technical infrastructure, architecture, technical design and forms of access reflect concrete functional demands and legal and political requirements. Only a few central banks that are involved in developing central bank digital currency have made clear choices so far. The European Central Bank is leaving open the question of which technology will be employed for the digital euro and is evaluating issues of access, architecture and design in the trial phase. The Swedish Riksbank is also refraining from making a definite decision on the technology for the e-Krona, but it is relying on a retail CBDC with hybrid architecture and DLT for the pilot phase. The South Korean central bank has already decided and is using a hybrid-architecture retail CBDC based on the Ethereum blockchain for its pilot project. Of the central banks that have already launched or are about to launch a CBDC, the Bahamas has opted for a hybrid-architecture retail CBDC for the Sand Dollar (Prasad 2021: 4). Overall, central banks planning a wholesale CBDC are clearly the minority. Thus, as around 44 central banks have opted for a retail CBDC and twenty are pursuing a hybrid variant, there are only five with a preference for a wholesale CBDC (Atlantic Council 2021). The Swiss National Bank, for example, has explored issuing a wholesale CBDC based on a DLT platform in a study and views CBDC, above all, as an instrument for financial intermediaries (SNB et al. 2020). Just as in the first three waves, much can still be expected to change with regard to CBDC, and developments in the different waves will have an influence on each other. The question of the technology is still undecided in most of the digital central bank money projects. The South Korean central bank is not likely to remain the only central bank to have recourse to systems from the other waves.

## 3.3 Criticism and the Future Development of Digital Central Bank Money

The emergence of central bank digital currency is also viewed critically by some, and the extent to which it will be accepted by the general public largely depends on the concrete form it is given (Bofinger/Haas 2020; Cecchetti/Schoenholtz 2021). Whereas economic issues, such as the crowding out of the private financial sector and resulting allocation problems, are the focus in liberal democracies, there are many signs that digital central bank money will also be used for surveillance and social control in authoritarian, state-capitalist systems. In the case of one of the pioneers in the domain of CBDC, the People's Republic of China with its digital renminbi (e-RMB), there are well-founded indications that the e-RMB represents a further building block in the digital surveillance state and is intended to expand the financial influence of the communist one-party state in its competition with liberal democracies (Work 2021). This might be one of the reasons why the e-RMB cannot show significant adoption thus far (The Economist 2022). The invasive rights of the state and its monitoring of private transactions using central bank digital money are justifiable objections to CBDC, especially in the case of authoritarian

states. The public's greatest fear is that central bank digital currency could lead to the abolition of cash, although central banks like the ECB regularly stress that it is only a matter of creating a complementary form, not to replace cash, and as a precautionary measure in case the latter continues to decline in importance. A related criticism involves the possibility of introducing negative interest on central bank digital currency. It is assumed in the existing system that people also resort to cash when the interest offered by banks is so low that it is more worthwhile to keep money under the mattress. This option could also be excluded, however, by exempting CBDC from interest or introducing a zero-interest bound. The possibility that central bank digital currency could lead to a crowding out of private business models of commercial banks, as well as payment service providers, represents a more substantial criticism: this would mean that the state could displace more efficient forms of allocation. As with the other objections to digital central bank money mentioned, these risks could also be counteracted by appropriate design choices.

The (thus far) four waves of digital currencies are not yet completed; the fourth has only just begun, and they will continue to run concurrently. It is highly likely that people will hold different digital currencies in their digital wallets in the future and use them for different purposes. Whereas the coexistence of different currencies is nothing new in and of itself, the technological possibilities make it more likely that large parts of the population will in fact use them. It is important for central bank currency to be available as an option in the digital sphere without driving out others. In a report by seven central banks, the BIS has presented three key principles to guide the development of CBDC. Firstly, the issuing of CBDC by a central bank should not compromise the goal of monetary and financial stability. Secondly, central bank digital currency should be complementary to, but not replace existing means of payment. Thirdly, introducing CBDC should promote technical innovation and economic efficiency (Bank of Canada et al. 2020). How these and other principles can be implemented is discussed in the next section on digital monetary policy.

**Figure 6 | Timeline Digital Currencies**

## 1. WAVE

**2008** | Bitcoin Whitepaper published on October 31.

**2009** | Bitcoin Genesis Block minded on January 3.

**2010** | Pizza-Day on May 22, first documented purchase of a good with Bitcoin.

**2011** | Exchange Mt. Gox reports loss of 25.000 BTC due to a hack attack.

**2012** | Formation of Bitcoin Foundation in September to support network development.

**2014** | Wikimedia Foundation accepts dona-tions in BTC.

**2016** | Protocol update (Soft fork) „Segwit" is introduced to enhance scalability of the Bitcoin network.

**2018** | China bans Bitcoin in February and extends the ban to all cryptocurrencies in 2021.

**2019** | Bitcoin Future traded on NYSE.

**2020** | MicroStrategy invests USD 250 Mio. in Bitcoin. Massachusetts Mutal Life Insurance Company buys bitcoin worth USD 100 million.

**2021** | Bitcoin becomes legal tender in El Salvador.

**2022** | Central African Republic adopts Bitcoin as legal tender.

## 2. WAVE

**2013** | Vitalik Buterin published Ethereum-Whitepaper.

**2014** | Gavin Wood publishes Ethereum Yellow-Paper in-cluding the smart contract architecture.
Ethereum Foundation (Stiftung Ethereum) established as Swiss non-profit foundation.

**2015** Ethereum-Genesis-Block mined on July 30.
ERC-20-Standard allows developers to create tokens on Ethereum blockchain.

**2016** | SmartContract of the decentralized growth fund „TheDAO" is hacked and Ethereum blockchain is forked (hard fork). Ethereum Classic is created alongside Ethereum.

**2017** | Creation of Enterprise Ethereum Alliance to facilitate the use of Ethereum block-chain technology.
An SEC report finds that tokens offered and sold by „The DAO" were securities.

**2019** | DeFi-SmartContracts contain Tokens worth 2.9 bln USD.

**2020** | Phase 0 of Ethereum 2.0 and the transition to proof-of-stake begins.

**2021** | Christie's auctions Ethereum NFT for USD 69.3 million.

## 3. WAVE

**2014** | Concept for MakerDAO published by Rune Christen-sen and Maker Foundation established.

**2015** | Crypto exchange Bitfinex Adds Tether Tokens (USDT)

**2017** | First community-governed stablecoin (DAI token) can be traded.

**2018** | 2.8 billion Tether tokens are in circulation.

**2019** | The daily trading volume of Tether exceeds that of Bitcoin for the first time.

**2020** | 500 million DAI tokens have been issued.

**2021** | Tether settles with New York State in reserve dispute and pays over $18 million in fines.

**2022** | The algorithmic stable-coin Terra USD collapses and is depegged from the US dollar amidst a crash of major cryptocurrencies.

## 4. WAVE

**2014** | Ecuadorian central bank launches the first CBDC. Due to a lack of trust the project was discontinued in 2017.

**2016** | Numerous central banks begin exploring digital central bank currencies.

**2017** | Uruguayan central bank conducts six-month pilot project for e-peso.
Swedish Riksbank begins development of the e-Krona.

**2018** | In survey, majority of 63 central banks surveyed say they are looking at developing digital central bank money.

**2020** | Chinese cen-tral bank starts pilot project for e-CNY in four cities.
Swiss National Bank tests wholesale CBDC with partners.
Bahamas launches a retail CBDC (Sand Dollar).

**2021** | ECB begins investigation phase for digital euro.
UK Treasury and Bank of England launch task force to develop digital pound.
U.S. Federal Reserve explores adoption of digital dollar.
Eastern Caribbean Currency Union (DCash) and Nigeria (eNaira) Launch CBDC.

# 4. Digital Monetary Policy: Shaping the Fourth Wave of Digital Currencies

There are numerous signs that these four waves of digital currencies are converging on each other and competition between private and public currencies is coming into being. Numerous questions for the future of the global financial system are connected to this. The core task for public actors like central banks in this new area of currency competition is creating robust framework conditions for technological innovation and economic dynamism, on the one hand, and, on the other, securing a monetary and financial system that guarantees monetary and financial stability, as well as financial inclusion, transparency and trust in the system (Carney 2021: 109). The financial system of the future will be at least as diverse as the existing one, but new forms of computing are creating entirely new possibilities. A smart digital currency policy will help more people around the world to gain access to the financial system and to enjoy the benefits of stable currencies.

## 4.1. A Legal Framework for Digital Currency Competition

The cryptocurrencies of the first wave largely emerged without public intervention and have been developing at tremendous speed ever since without relying on any support from governments. At the same time, however, there are already numerous regulatory approaches to digital currencies (Rogoff 2016: 210). Calls for public support measures or special regulations are rarely heard from the crypto community. The industry for the most part only asks for existing law to be applied reliably and predictably or that the peculiarities of the technology are considered. Since its launch, the euro is the only legal tender in Germany and has thus to be accepted as means of payment by all public and private instances (so-called "Annahmezwang" or "mandatory acceptance") (Omlor, 2018: 86). The status of the euro as the only legal tender is not per se a decisive obstacle to the further development of private cryptocurrencies and currency competition. Even before cryptocurrencies emerged, parties to contracts were allowed to agree to settle their debts in foreign currencies or even physical products. Businesses and individuals are thus free to use means of payment other than the euro for their transactions, and numerous online shops have already been accepting payments in cryptocurrencies. Although payment in cryptocurrencies results in the conversion of a sales contract into a barter agreement, this remains largely insignificant for the consumers involved, for example, since, per § 480 of Germany's Civil Code, the rules governing purchase and sale are also applied to barter (Omlor 2019: 329). The single legal tender serves as fallback in the event of a dispute and spares the parties the need to come to an agreement on the way of settling debts. Hence, the legal tender is for the time being at least justified for reasons of efficiency –whether this justification will continue to apply in the long run, given the expected further development that digital currencies, is an open question (Omlor 2019: 340). However, the justification of efficiency does not apply to private digital currencies that are in competition with government-issued currencies. To this extent, the decision of El Salvador and most recently of the Central African Republic to introduce Bitcoin as legal tender is to be viewed critically. Businesses are now forced to have infrastructure available for two legal means of payment. Since the value of Bitcoin is extremely volatile, it is completely unsuitable to serve as unit of account, for example, to express prices. This measure does not give rise to genuine and supposedly welfare enhancing currency competition, because a winner has been picked by the state. Although the emerging infrastructure may encourage merchants to accept other cryptocurrencies with greater macroeconomic added value in the long run, treating Bitcoin as legal tender provides an undeserved head-start to a private currency.

If the government wants to strengthen competition between digital currencies, this will happen less by designating the status as legal tender than by clarifying the legal nature of tokens in private law. In short to middle term it is essential for public authorities to take the new technology into account in both property law and the law of obligations if the state does not want to lose significance in the digital domain, in relation to an emerging private legal order in the sense of a lex cryptographia (Wright/De Filippi, 2015). In 2021, Germany took a first step in the right direction with the introduction of electronic securities through the Electronic Securities Act (eWpG), but just like the EU and the USA – apart from money laundering regulations – it has not yet adapted the law to the new technological developments (Omlor 2019: 332). In addition to clarifying the legal nature of payment tokens, there are numerous issues that the legislature has to address, ranging from the laws on barter and purchase/sale (Omlor 2019: 319) to the handling of digital assets in property law and the law on enrichment (Omlor 2019: 308) to financial services law. Clear and measured rules on the tax treatment of token transactions and profits from price movements could help position Germany and Europe as leaders in private currency competition and digital markets. Reasonable market regulations can also strengthen the attractiveness of jurisdictions as a location in the competition for digital currencies. In principle, it is a welcome development that the European Commission has introduced transparency requirements for stablecoins providers as part of the MiCA Regulation. When regulating digital currency and the underlying technology that promises to be the base of a more user-centric and inclusive financial system and digital sphere, however, great

care should be taken in every form of regulation, in order not to stifle innovation and to avoid rules that only large actors are able to comply with. To this end, regulators need to be mindful of the particularities of the different digital currencies and not to adopt a one-size-fits-all approach for new technologies. This particularly concerns issues such as privacy and anti-money laundering regulation. As described in Chapter 2, the use of crypto currencies for illicit activity lays below the rates of regular currencies. The past has proven that even if fully decentralized systems like bitcoin are used to launder money, competent authorities can seize asset and identify illicit users without over-burdened regulation and treating all crypto-asset users as criminals. In order to set effective standards for digital currencies, regulatory requirements need to be proportional.

## 4.2. Digital Central Bank Money as a Complementary Form of Money

Especially in countries or currency areas with a stable national or supranational currency, an independent central bank and the rule of law, the development of central bank digital currencies is an important addition to cash. In the upcoming decisions on the exact form of such, central banks should, above all, be guided by the goal of financial inclusion and of providing a digital equivalent to cash. In countries in which many people do not have bank accounts, CBDCs provide the potential to create reliable access to the financial system. More than a billion people worldwide have neither an account with a financial institution nor a mobile money provider available to them – and could thus benefit from digital central bank money (Demirgüç-Kunt 2018: 35). But, considering the loss in the significance of cash, this point will also become increasingly important in economies with more inclusive financial systems. Central bank digital currency should always be complementary to cash and not get ahead of the trend.

To be both complementary and equivalent to cash, central bank digital currency must represent a direct claim on the central bank and ensure comparable anonymity to paying with cash. A DLT-based token CBDC is most suitable for this purpose: one that can be used almost as anonymously in a hybrid form up to an appropriate daily limit, but that also, thanks to the record of transactions, allows for identification of the parties for the purpose of preventing and prosecuting illicit activities like money laundering. For larger transactions, in which identification of the parties is regarded as necessary due to money laundering, it is possible to verify the identities of the owners of the sender and recipient wallets via intermediaries or directly at the central bank. The development of secure digital identities by individual countries or the European Union would be useful to this end. For the purpose of privacy protection and protection against invasive government action, identification via private intermediaries is preferable to direct identification at central banks. CBDCs could thus also satisfy the identity verification requirements (KYC) that are needed to impede misuse of the currency for money laundering or terrorist financing, but in a way that protects users' privacy. The identities of parties would thus be verifiable ex post in the case of large CBDC transactions, whereas extensive, cash-like anonymity would be ensured for smaller transactions thanks to an anonymous wallet, sometimes wrongly termed as "unhosted wallets". An appropriate compromise between fighting crime and respecting privacy would make it more likely that the currency is accepted as means of payment by the general public. Businesses and individuals would have direct access to digital central bank money in such a hybrid, two-tier model, but they could still engage intermediaries, for example, to provide user-friendly administration of the identified CBDC wallets (private keys).

An important choice that needs to be made in designing CBDC is related to the issue of whether digital central bank money should accrue interest when it is in the user wallet. In theory, digital central bank money offers the possibility of directly setting positive, as well as negative, interest rates (Brunnermeier 2019 et al.: 27; Kiff et al. 2020: 11; Leibbrandt/De Teran 2021: 212). Unlike in the case of cash, there would be no possibility here of withdrawing money from the system and keeping it at home to avoid negative interest. This possibility jeopardizes the acceptance of digital central bank money and hence should be technically ruled out. Issues of data protection in CBDC transactions and of limiting the central bank's access will have a decisive influence on whether central bank digital currency is a success. Overall, in liberal democracies with well-functioning rule of law and an independent central bank, CBDCs, if appropriately designed, offer great potential for financial inclusion and the provision of a secure, low-risk and generally accepted complement to cash, which brings all the functions of classical money into the digital age.

In countries with unstable national currencies – i.e. countries with high rates of inflation – the probability is high that central bank digital currency will encounter similar obstacles to acceptance as the original analog currency. A central bank digital currency can only be as good as the original national or supranational currency and its institutions. Usually countries without a stable currency also lack independent central banks. Apart from a lack of acceptance, there is also the danger, depending on the technical design, of the government exploiting possibilities to gain direct access to citizens' digital money. But with a robust technical design, central bank digital currency that is issued by an independent central bank can also create greater trust in a CBDC and thus combat inflation. In the case of programmable money, there would even be the possibility of using central bank digital currency to combat corruption. Nonetheless, great care should be taken with programmable central bank money due to possibly far-reaching governmental interference in economic transactions – a risk that is particularly great in countries that have weak rule of law and a lack of good governance. This is another reason why the introduction of

central bank digital currency in authoritarian states involves substantial risks and creates enormous potential for abuse by authoritarian regimes. For instance in the People's Republic of China the possibility that the electronic yuan or digital renminbi will be integrated into the existing surveillance systems of the communist one-party state, in order to monitor and influence the spending behavior of individuals creates justified fears (Work 2021). In technical terms, programmable central bank money would create the possibility of limiting expenditure to specific purposes or accessing CBDC assets directly. If cash were completely replaced by CBDC, an authoritarian regime's possibilities for restricting the consumption behavior of the entire population or just of opposition groups would be almost limitless. Whereas democratic procedures and the rule of law set narrow limits to such a use in liberal democracies, dictatorships could employ central bank digital currency as an unprecedented instrument of surveillance and control. The development and use of CBDC by authoritarian regimes also presents challenges for liberal democracies. As authoritarian regimes such as China are progressing fast with their effort to create CBDC, international standards could thus be set that jeopardize the mechanisms of the rule of law. Moreover, the provision of digital currencies and an alternative financial infrastructure could allow for the circumvention of sanctions regimes that help, among other things, to punish human rights violations (Work 2021). Hence, speed also plays a role for liberal democracies in the development of functional central bank digital currency. In their increasing competition with state-capitalist autocracies, they have to set standard by showing how central bank digital currency can be used effectively in the context of the rule of law. Consequently, it is important for the competition with authoritarian systems to design the infrastructure and identification requirements in such a way that they do not lead to insurmountable barriers to access for users from economically less developed regions without a functioning system of identification.

## 4.3. Implications for the Global Financial System

Apart from the question of setting standards for development, use and abuse of central bank digital currency, digital currencies can also have implications for the global financial system and the global financial safety net. These implications concern the nature of global financial markets and the significance of intermediaries no less than central banks and international organizations, as well as regimes in the global world of finance.

Up until now, the global financial system has been largely shaped by the dollar as reserve currency, and the dominance of the dollar appears to have increased rather than diminished during the 2007 global financial crisis and the COVID-19 pandemic (Tooze 2018; 2021). The Federal Reserve made liquidity available in the form of dollars during both crises, thus saving banks in some parts of the world from liquidity bottlenecks. Around 40 percent of all transactions worldwide are transacted in dollars, the dollar is involved in 88 percent of all foreign exchange transactions, and about 60 percent of assets held by central banks are denominated in dollars (Kempa 2018; Prasad 2021: 278). Whether the Federal Reserve's hesitancy to develop a digital version of the greenback and the speed with which the Chinese central bank is creating the e-RMB will really help to bring about a shift in power in the global financial system appears doubtful at least for the moment. Likewise, cryptocurrencies such as Bitcoin will not be able to threaten the dominance of the dollar as currency of reference, at least in the short term (Prasad 2021: 312). It is equally conceivable that a digital version of the dollar will lead to a digital dollarization, since the dollar will be even more readily available for everyday use (Brunnermeier et al. 2019: 20; Leibbrandt/De Teran 2021: 213; Prasad 2021: 15). The strength of the dollar can also be seen in the market for digital currencies where all major stablecoins use the greenback at reference currency.

But even if the extent of the changes remains unclear for the moment, the development of digital currencies will entail changes in the global financial system. These will, for example, affect dominant actors like the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which has been responsible for processing a considerable part of cross-border payments up to now and is being challenged by innovative financial technology and digital currencies. Thanks to lower transaction costs, digital currencies may in the future make established intermediaries like correspondent banks redundant in cross-border transactions (IMF 2020). The more prevalent digital currencies become, and the more central banks develop digital currencies (CBDCs), the more international organizations and their member states will be forced to confront the challenge of creating global rules for cross-border transactions to prevent fragmentation into digital currency areas and a negative impact on trade flows (Brunnermeier et al. 2019). In addition to the classical issues of the global financial system, issues regarding data use, data protection, consumer rights, digital identity, and competition law, among others, need to be addressed in the context of the digital economy (IMF 2020: 8; Brunnermeier et al. 2019). Furthermore, the interoperability and convertibility of digital currencies are also relevant. From a competition policy point of view, there is the danger that large tech concerns could create technical monopolies (Brunnermeier 2019: 17). In light of different possibilities of technical design – particularly for digital central bank currency – the interoperability of digital currencies can also be of significance for general acceptance.

With competition between digital currencies and a greater proliferation of non-government-issued digital currencies, new mechanisms will be needed to ensure global financial

stability; for many digital currencies, there is no default lender of last resort that could provide liquidity in a crisis. To this end, former Bank of England Governor Mark Carney has proposed a synthetic, digital international currency that could be used for global transactions, but also as a means for storing value or safe asset (Prasad 2021: 301). A global stablecoin of this sort would be backed by a currency basket consisting of relevant currencies and would be conceivable in a variety of forms (Brunnermeier 2019: 22; IMF 2020; Prasad 2021: 301). Carney's (2019) proposal envisages a Synthetic Hegemonic Currency (SHC) issued by a public authority – for instance, a network of central banks – that is based on a basket of currencies and is meant to function as international reserve currency. The International Monetary Fund's Special Drawing Rights (SDR), which are already based on a basket of currencies including the major international currencies (euro, dollar, yen, pound and renminbi), could serve as a blueprint for the development of a synthetic global digital currency (Prasad 2021: 304). A global stablecoin would be equally conceivable: one that is issued either by private parties or by a public authority and that is backed by both established cryptocurrencies and national or supranational public currencies. In any case, digital currencies offer us the possibility of getting closer to a true global currency, such as was already discussed at the Bretton Woods Conference in 1944. At the moment, it is difficult to assess the impact the rise of digital currencies will have on the global financial system and the global financial safety net, but, in any case, global cooperation will be required to ensure that digital currencies can contribute to greater financial inclusion, as well as financial stability and a dynamic global economy

### 4.4. Strengthening Financial Innovation

The emergence of digital currencies in combination with new decentralized computing platforms like Ethereum points to a loss in the significance of large financial intermediaries in the long run and at the same time offers the possibility of a far more inclusive financial economy. For this not to have negative consequences for the allocation of resources and the economy as a whole, innovative financial products that make use of the peer-to-peer approach have to be strengthened. Hence, it is advisable to reform legal provisions on investment and the protection of investors, in order to give small investors a greater scope of action in the decentralized financial (DeFi) domain and to take advantage of the opportunity for democratizing the financial economy. One focus here should be new forms of crowdfunding and the new forms of governance, peer-to-peer lending and market making that are based on them. Innovative financial products are of crucial importance for increasing prosperity and resource allocation precisely in regions with an underdeveloped financial infrastructure. DeFi's large degree of independence from institutional structures and the relatively limited susceptibility to corruption that is connected to this offer opportunities precisely for regions with weak institutions and legal systems. Furthermore, the internationalization associated with a decentralized financial space can also give previously excluded parts of the population access to financially strong capital markets and banking services on a previously unimaginable scale.

In the more distant future, we need also to think about a special legal form for decentralized autonomous organizations, in order to promote their regional anchoring and to secure the spheres of influence of legal orders on the organizational form of the digital age (Greilich, 2020).

# 5. Four Principles for the Future of Money

Digital currencies are no longer a niche topic. Just like the proliferation of paper money and the emergence of central banks and card payments, digital currencies will change the way in which people make payments and invest money. Many people often associate just one cryptocurrency with the terms "digital currencies" or "cryptocurrencies": Bitcoin. The emergence of Bitcoin was undoubtedly a technological milestone, but numerous new digital currency projects have emerged in the last decade – and still others are in the development stage. This policy paper has provided an overview of the diversity of digital currencies and a classification of their different phases of development. The four waves of digital currencies reflect the different functions, applications, and organizational forms of digital currencies, as well as the source of their value. The classification into waves is based on the assumption that the development of the different developmental phases is not completed yet and that the waves run or will run concurrently. The fourth wave in particular, involving central bank digital currency as the key innovation, is still just emerging. This logic of waves and the practical recommendations based on it are also shaped by a second assumption: there is no question whether there is competition among digital currencies, i.e. a situation in which people hold different currencies in their digital wallet and use them for different purposes. This competition is already underway and will continuously expand. Thus far, only a relatively small share of the population uses digital currencies, but this proportion is constantly and rapidly increasing. There are many signs that this trend will also extend

to digital currencies and other financial technology (FinTech) innovations. The state is reacting both with the development of digital central bank money and regulation and has to create framework conditions for the new currency era in the medium term. Policies should be guided by four principles:

## 1. Innovation

The framework conditions for digital currencies and the development of new government-sponsored, public means of payment like digital central bank money should be designed to promote economic dynamism and innovation. At first, some regulators regarded the emergence of digital currencies with skepticism and tried to contain it with legal hurdles and prohibitions. This may be – at least to some extent - doable in authoritarian regimes such as the People's Republic of China, but it is neither a desirable nor a promising approach in countries with market economies and free societies. The state's monopoly on money is not threatened by the rise of digital currencies and can even be modernized thanks to the development of central bank digital currency. The goal of the state's monopoly on money was never to marginalize other currencies, but rather to provide a reliable national currency as legal tender and public good. Hence, the state should be open to technological innovation in the financial and monetary spheres. Experience shows that this leads to greater economic dynamism and contributes to innovation in other sectors of the economy.

## 2. Inclusion

One of the areas in which digital currencies hold great promise is in fostering more inclusion. Access to digital currencies can be gained using a mobile device even without a functioning financial system. People in unstable countries are already using digital currencies as an alternative to unstable national currencies. Precisely where access to the financial system is more difficult or costly, digital currencies offer the possibility of greater financial participation. Digital currencies can also allow for cheaper and faster transactions in industrialized countries. Interoperability is a decisive factor especially for digital central bank currency, but also for platform currencies. A fragmented monetary system involving technical hurdles would severely limit the benefits of greater accessibility and hence also of broad financial inclusion. In designing central bank digital currency, the architecture in which it is embedded will also be important. Central banks or intermediaries must ensure that people with less affinity for technology will still be able to access (digital) central bank currency. This also includes introducing digital central bank money to complement cash, not to replace it.

## 3. Stability

The independent central bank with a mandate to preserve monetary stability has made a major contribution to warding off inflation in many parts of the world. Even amidst short periods of above average deflation or inflation, for many people, this means that they need not fear that their savings will be devalued or that they can not afford daily goods. This provision of stable money as a public good should also be a guiding principle for the development of central bank digital currency in the new currency era. In countries in which there have not been any stable national currency up to now, both private and better-managed public digital currencies can represent alternatives.

## 4. Freedom

The way in which people pay always has implications for individual freedom as well. Digital currencies offer people the opportunity to store their money in an inflation-proof manner, to circumvent capital controls and, depending on the design, also to pay anonymously in the digital domain. In countries with unstable currencies or deficient rule of law access to digital currencies offers more independence from state structures. However, even in established liberal democracies, aspects like data protection, privacy protection and free choice of forms of payment and currency forms are key to the regulation and design of digital currencies.

The new currency era has only just begun, and there are still many open questions. It is clear, however, that technological innovation in the financial domain also has an impact on the competition between liberal democratic and autocratic state capitalist orders. In authoritarian regimes, public digital currencies can – and will – be used as an instrument of surveillance and control or to circumvent sanctions for human rights violations. The hesitancy of Western central banks to develop digital central bank money and the People's Republic of China's rush to do so has led to China having at least a slight head start in this new currency era. Hence, it is even more important that liberal democracies act more decisively in developing digital central bank money, create robust frameworks and regulations for digital currencies and financial technology, and, in so doing, set the standards for the future of money not by way of prohibitions, but by way of appropriate legal measures and innovation-friendly regulation.

# References


**Adler, D.** (2018). *„Silk Road: The Dark Side of Cryptocurrency"*, Fordham Journal of Corporate & Financial Law, 21 February. Available at: https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/ (Abgerufen am: 26.07.2021).

**Agur, I., Ari, A. & Dell'Ariccia, G.** (2021). *Designing central bank digital currencies.* IMF Working Paper WP/19/252.

**Allen, S., Čapkun, S., Eyal, I., Fanti, G., Ford, B. A., Grimmelmann, J., Juels, A., Kostiainen, K., Meiklejohn, S., Miller, A., Prasad, E., Wüst, K. & Zhang, F.** (2020). *Design choices for central bank digital currency: Policy and technical considerations.* National Bureau of Economic Research (NBER) Working Paper No. w27634.

**Antonopoulos, A. M.** (2017). *Mastering Bitcoin: programming the open blockchain.* Second edition. Sebastopol, CA: O'Reilly.

**Armelius, H., Claussen, C. A. & Hull, I.** (2021). *On the Possibility of a cash-like CBDC*, Sveriges Riksbank Staff memo, February 2021.

**Atlantic Council** (2021). Central Bank Digital Currency Tracker. Available at: https://www.atlanticcouncil.org/cbdctracker/ (Accessed: 15.10.2021).

**Auer, R. & Böhme, R.** (2020). *The technology of retail central bank digital currency.* BIS Quarterly Review, March 2020. Basel: Bank for International Settlements.

**Auer, R. & Boehme, R.** (2021). *Central bank digital currency: the quest for minimally invasive technology.* BIS Working Papers, No 948.

**Auer, R. A., Cornelli, G. & Frost, J.** (2020). *Rise of the central bank digital currencies: drivers, approaches and technologies.* CESifo Working Paper, No. 8655.

**Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors Federal Reserve System and Bank for International Settlements** (2020). *Central bank digital currencies: foundational principles and core features.* Report No. 1 in a series of collaborations from a group of central banks. Available at: https://www.bis.org/publ/othp33.pdf (Accessed: 15.10.2021).

**Bank for International Settlements (BIS)** (2021). *Annual Economic Report – Promoting global monetary and financial stability.* Basel: Bank for International Settlements.

**Brunnermeier, M. K., James, H. & Landau, J. P.** (2019). *The digitalization of money* (No. w26300). National Bureau of Economic Research.

**De Best, R.** (2021). Bitcoin energy consumption 2021, Statista. Available at: https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/ (Accessed: 26.07.2021).

**Bindseil, U.** (2019). *Central bank digital currency: Financial system implications and control.* International Journal of Political Economy, 48(4), pp. 303–335.

**Bindseil, U.** (2020). *Tiered CBDC and the financial system*, ECB Working Paper, No. 2351.

**Bitcoin Mining Council** (2021). *Global Bitcoin Mining Data Review* – Q2 2021.

**Bitcoin price today, BTC live marketcap, chart, and info** (2021). CoinMarketCap. Available at: https://coinmarketcap.com/currencies/bitcoin/markets/ (Accessed: 25.07.2021).

**Bofinger, P. & Haas, T.** (2020). *CBDC: Can central banks succeed in the marketplace for digital monies?* CEPR Discussion Paper, DP15489.

**Bradbury, D.** (2013). *„Colored coins paint sophisticated future for Bitcoin"*, CoinDesk, 14 June. Available at: https://www.coindesk.com/markets/2013/06/14/colored-coins-paint-sophisticated-future-for-bitcoin/ (Accessed: 08.09.2021).

**Bundesministerium der Finanzen** (2021). *„Entwurf: Einzelfragen zur ertragsteuerrechtlichen Behandlung von virtuellen Währungen und von Token"*. Available at: https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Steuerarten/Einkommensteuer/2021-06-17-est-kryptowaehrungen.pdf?__blob=publicationFile&v=2 (Accessed: 12.10.2021).

**Buterin, B.** (2014) *„A next-generation smart contract and decentralized application platform"*, white paper, 3, p. 37. Available at: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (Accessed: 12.10.2021).

**Buterin, V., Hitzig, Z. & Weyl, E. G.** (2018). *Liberal Radicalism: A Flexible Design For Philanthropic Matching Funds.* SSRN Scholarly Paper ID 3243656. Rochester, NY: Social Science Research Network.

**Cambridge Center for Alternative Finance** (2021). *Cambridge Bitcoin Electricity Consumption Index* (CBECI). Available at: https://cbeci.org/ (Accessed: 26.07.2021).

**Catalini, C. & Gans, J. S.** (2016). *„Some Simple Economics of the Blockchain"*, MIT Sloan Research Paper, (No. 5191–16).

**Carney, M.** (2021). *Values: Building a Better World for All.* London: William Collins.

**Cecchetti, M. & Schoenholtz, K.** (2021). *Central bank digital currency: The battle for the soul of the financial system.* Available at: https://voxeu.org/article/central-bank-digital-currency-battle-soul-financial-system (Accessed: 15.10.2021).

**ConsenSys** (2019). *„A Short History of #Ethereum"*, ConsenSys, 13 May. Available at: https://consensys.net/blog/blockchain-explained/a-short-history-of-ethereum/ (Accessed: 13.05.2019).

**De, N. & Hochstein, M.** (2021). *Tether Details Reserve Composition for the First Time*, CoinDesk. Available at: https://www.coindesk.com/markets/2021/05/13/tethers-first-reserve-breakdown-shows-token-49-backed-by-unspecified-commercial-paper/ (Abgerufen am: 10.09.2021).

**Digiconomist** (2021). *Bitcoin Energy Consumption Index*, Digiconomist. Available at: https://digiconomist.net/bitcoin-energy-consumption/ (Accessed: 26.07.2021).

**Dyson, B. & G. Hodgson** (2016). *Digital Cash: Why Central Banks Should Start Issuing Electronic Money.* London: Positive Money.

**Ebert, M., Kümmel, M., Jacobs U. H. & M. Hirtschulz** (2021). Sustainable Crypto Currencies Mining is affecting supply chains and the environment, but Germany can help mitigate it. DGAP MEMO, No. 8, October 2021.

**El-Erian, M. A.** (2016). *The only game in town: Central banks, instability, and avoiding the next collapse.* New Haven and London: Yale University Press.

**ethdocs.org** (2016). *History of Ethereum – Ethereum Homestead 0.1 documentation.* Available at: https://ethdocs.org/en/latest/introduction/history-of-ethereum.html (Accessed: 09.09.2021).

**European Central Bank (ECB)** (2020). *Report on a digital euro.* Frankfurt am Main: European Central Bank.

**Evans, E. & Chamberlain, P.** (2015). *Critical waves: Exploring feminist identity, discourse and praxis in western feminism.* Social Movement Studies, 14(4), pp. 396–409.

**Fischer, E. F.** (2021). *Quality and inequality: Creating value worlds with Third Wave coffee.* Socio-Economic Review, 19(1), pp. 111–131.

**Foley, S., Karlsen, J. R. & Putniņš, T. J.** (2019). *Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?* The Review of Financial Studies, 32(5), pp. 1798–1853.

**Fox-Brewster, T.** (2016). *„Craig Wright Claims He's Bitcoin Creator Satoshi – Experts Fear An Epic Scam"*, Forbes, 5 February. Available at: https://web.archive.org/web/20170719025810/ https://www.forbes.com/sites/thomasbrewster/2016/05/02/craig-wright-satoshi-nakamoto-doubt/ (Accessed: 22.07.2021).

**Furman, J. & Hatzius, J.** (2020). *„Update on COVID-19 – US Economic Outlook & Implications of Current Policies for Inflation, Gold and Bitcoin"*, Goldman Sachs.

**Grant Thornton LLP** (2021). *Circle Examination Report July 2021.* Reserve Account Report. Available at: https://www.centre.io/hubfs/pdfs/attestation/2021%20Circle%20Examination%20Report%20July%202021%20Final.pdf?hsLang=en.

**Greilich, K.** (2020). *„Wir brauchen eine neue Gesellschaftsform!"* In: **Bange, M. A.** (ed.) *Rechtsfragen zum gesellschaftlichen und wirtschaftlichen Wandel im Jahr 2020*: Tagungsband Liberale Rechtstagung 2020. Göttingen: Cuvillier Verlag, S. 49-68.

**Groß, J., Herz, B. & Schiller, J.** (2020a). *Bitcoin, Libra und digitale Zentralbankwährungen – ein Geldsystem der Zukunft?* Wirtschaftsdienst, 100(9), S. 712–717.

**Groß, J., Klein, M. & Sandner, P.** (2020b). *Digitale Zentralbankwährungen: Chancen, Risiken und Blockchain-Technologie.* Wirtschaftsdienst, 100(7), S. 545–549.

**Hagelüken, A.** (2020) *Das Ende des Geldes, wie wir es kennen. Der Angriff auf Zinsen, Bargeld und Staatswährungen.* München: C.H. Beck.

**Haigh, A. & Ahmed, N.** (2021). *„Crypto Game Surge Lures Australia's Carnegie on Play-to-Earn-Bloomberg"*, bloomberg.com, 9 August. Available at: https://www.bloomberg.com/news/articles/2021-09-08/crypto-gaming-surge-lures-australia-s-carnegie-on-play-to-earn (Accessed: 10.09.2021).

**Haldane, A.** (2020). Seizing the Opportunities from Digital Finance, Speech given by Andy Haldane Chief Economist and Member of the Monetary Policy Committee, TheCityUK 10th Anniversary Conference, 18. November 2020. London: Bank of England.

**Hayek, F. A.** (1976). *Denationalisation of money: the argument refined.* London: The Institute of Economic Affairs.

**Hilgers, S.** (2021). *„Business and Monetary Policy"*. In: **Kellow, A., Porter, T. & Ronit, K.** (eds.) *Handbook of Business and Public Policy.* Cheltenham, U.K., Northampton MA, USA: Edward Elgar Publishing, pp. 117–192.

**Hughes, E.** (1993). *A Cypherpunk's Manifesto.* Available at: https://www.activism.net/cypherpunk/manifesto.html (Accessed: 22.07.2021).

**Huntington, S. P.** (1991). *Democracy's third wave.* Journal of democracy, 2(2), pp. 12–34.

**Ip, G.** (2021). *„Cryptocurrency Has Yet to Make the World a Better Place"*, Wall Street Journal, 20 May. Available at: https://www.wsj.com/articles/cryptocurrency-has-yet-to-make-the-world-a-better-place-11621519381 (Accessed: 26.07.2021).

**International Monetary Fund (IMF)** (2020). *Digital Money Across Borders: Macro-Financial Implications.* Staff Report. Washington D.C.: International Monetary Fund.

**Kaul, S. et al.** (2021). *Bitcoin – At the Tipping Point*, p. 108. Available at: https://ir.citi.com/peFJTnzeEoMSIAEFlw-H12VeM5d%2BCckWNrsO9lxpmyWezrz5V%2Bx%2FfRvm0gv6cWRpDHGWtIk7sTME%3D.

**Kaulartz, M.** (2016). *„Die Blockchain-Technologie"*, Computer und Recht, (7), pp. 474–480.

**Kempa, B** (2018). *Der US-Dollar als Leitwährung – alternativlos?* Wirtschaftsdienst, 98(10), S.691–710.

**Kiff, M. J., Alwazir, J., Davidovic, S., Farias, A., Khan, M. A., Khiaonarong, M. T., Khiaonarong, T., Malaika, M. Monroe, H., Sugimoto, H., Tourpe, H. & Zhou, P.** (2020). *A survey of research on retail central bank digital currency.* IMF Working Papers, WP/20/104.

**Kutler, J. & Power, C.** (1998). *„Bankrupt Digicash to seek financing, new allies"*, American Banker, 163(216), pp. 163-216.

**Leibbrandt, G. & De Terán, N.** (2021). *The Pay Off: How Changing the Way We Pay Changes Everything.* London: Elliott & Thompson Limited.

**Lober, A. & Weber, O.** (2005). *„Money for Nothing? Der Handel mit virtuellen Gegenständen und Charakteren"*, Multimedia und Recht – Zeitschrift für Informations-, Telekommunikations- und Medienrecht, (10), pp. 653–660.

**Morse, A.** (2021). *„Facebook-backed crypto project Diem to launch US stablecoin – CNET"*, Cnet, 5 December. Available at: https://www.cnet.com/personal-finance/investing/facebook-backed-crypto-project-diem-to-launch-us-stablecoin/ (Accessed: 10.09.2021).

**Nakamoto, S.** (2008a). *„Bitcoin: A Peer-to-Peer Electronic Cash System"*. Available at: https://bitcoin.org/bitcoin.pdf (Abgerufen am: 10.09.2021)

**Nakamoto, S.** (2008b). *„Bitcoin P2P e-cash paper"*, The Cryptography Mailing List. Available at: https://www.mail-archive.com/cryptography%40metzdowd.com/msg09959.html (Accessed: 29.10.2020).

**Nowak, P.** (2021). *Coin oder Token: Wo liegt da der Unterschied?*, computerbild.de. Available at: https://www.computerbild.de/artikel/cb-News-PC-Hardware-Coin-oder-Token-Wo-liegt-da-der-Unterschied-29982675.html (Accessed: 21.09.2021).

**Omlor, S.** (2018). *„Omlor: Blockchain-basierte Zahlungsmittel"*, Zeitschrift für Rechtspolitik (3), S. 85–89.

**Omlor, S.** (2019). *„Kryptowährungen im Geldrecht"*, Zeitschrift für das gesamte Handels- und Wirtschaftsrecht (183), S. 294-345.

**Partington, R.** (2019). *„France to block Facebook's Libra cryptocurrency in Europe"*, the Guardian, 9 December. Available at: http://www.theguardian.com/technology/2019/sep/12/france-block-development-facebook-libra-cryptocurrency (Accessed: 10.09.2021).

**Pilkington, M.** (2016). *„Blockchain Technology: Principles and Applications"*. In: **Olleros, F. X., Zhegu, M. & Elgar, E.** (eds.) *Research Handbook on Digital Transformations*, pp. 225-253.

**Popper, N.** (2015). *Digital gold: The untold story of Bitcoin.* New York: HarperCollins Publishers.

**Prasad, Eswar S.** (2021). *The Future of Money. How the Digital Revolution Is Transforming Currencies and Finance.* Cambridge, MA, USA: The Belknap Press of Harvard University Press.

**Rixecker, K.** (2021). *„Krypto-Games: Wie Videospiele die Blockchain erobern"*, t3n Magazin, 26 May. Available at: https://t3n.de/news/krypto-games-blockchain-spiele-1363231/ (Accessed: 10.09.2021).

**Rogoff, K. S.** (2016). *The Curse of Cash.* Princeton: Princeton University Press.

**Rosenfeld, M.** (2012). *„Overview of Colored Coins"*, white paper [Preprint]. Available at: https://bitcoil.co.il/BitcoinX.pdf (Accessed: 22.09.2021).

**Savelyev, A.** (2017). *„Contract law 2.0: ‚Smart' contracts as the beginning of the end of classic contract law"*, Information & Communications Technology Law, 26(2), pp. 116–134. doi:10.1080/13600834.2017.1301036.

**Schweizerische Nationalbank (SNB), Bank for International Settlements (BIS) & SIX Group AG** (2020). Project Helvetia Settling tokenised assets in central bank money. Verfügbar unter: https://www.bis.org/publ/othp35.pdf (Accessed: 15.10.2021)

**Shapiro, E.** (2018). *„Global Cryptodemocracy is Possible and Desirable"*, arXiv:1804.02049 [cs] [Preprint]. Available at: http://arxiv.org/abs/1804.02049 (Accessed: 09.09.2021).

**Shekhar, S.** (2018). *„Measuring Maker-Dai stability"*, Token-Analyst, 29 March. Available at: https://medium.com/tokenanalyst/measuring-maker-dai-stability-f74c23108128 (Accessed: 10.09.2021).

**Szabo, N.** (1996). *Smart Contracts: Building Blocks for Digital Markets.* Available at: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (Accessed: 31.12.2020).

**Tapscott, D. & Tapscott, A.** (2016). *Blockchain Revolution. How Technology behind Bitcoin is changing money, business, and the World.* New York: Penguin Random House.

**The Economist** (2015). *„The promise of the blockchain – The trust machine | Leaders | The Economist"*, 31 October. Available at: https://www.economist.com/leaders/2015/10/31/the-trust-machine (Accessed: 28.10.2020).

**The Economist** (2019a). *„Facebook wants to create a global currency"*, 22 June. Available at: https://www.economist.com/leaders/2019/06/22/facebook-wants-to-create-a-global-currency (Accessed: 10.09.2021).

**The Economist** (2019b). *„Is Libra doomed?"*, 24 October. Available at: https://www.economist.com/finance-and-economics/2019/10/24/is-libra-doomed (Accessed: 10.09.2021).

**The Economist** (2021). *„Using bitcoin as legal tender"*, 4 September. Available at: https://www.economist.com/finance-and-economics/2021/09/04/using-bitcoin-as-legal-tender (Accessed: 09.09.2021).

**Tooze, A.** (2018). *Crashed: How a decade of financial crises changed the world.* Penguin.

**Tooze, A.** (2021). *Shutdown: How Covid Shook the World's Economy.* Viking.

**Uberti, D.** (2021). *„How the FBI Got Colonial Pipeline's Ransom Money Back"*, Wall Street Journal, 6 November. Available at: https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981 (Accessed: 26.07.2021).

**United States Court of Appeals, Second Circuit** (2017). UNITED STATES OF AMERICA v. ROSS WILLIAM ULBRICHT. Docket No. 15-1815. United States Court of Appeals, Second Circuit. Available at: https://caselaw.findlaw.com/us-2nd-circuit/1862572.html (Accessed: 26.07.2021).

**Vigna, P. & Casey, M. J.** (2015). *Cryptocurrency: How Bitcoin and Cybermoney Are Overturning the World Economic Order.* Random House.

**Wallace, B.** (2011). *„The Rise and Fall of Bitcoin"*, Wired Magazine [Preprint], (December 2011). Available at: https://web.archive.org/web/20140326095105/http://www.wired.com/magazine/2011/11/mf_bitcoin/all/ (Accessed: 22.07.2021).

**Werbach, K.** (2018). *The Blockchain and the New Architecture of Trust.* Cambridge, MA, USA: MIT Press.

**Wieczner, J.** (2021). *„Jack Dorsey Says Bitcoin Is Climate Friendly. Is He Right?"*, Intelligencer [Preprint]. Available at: https://nymag.com/intelligencer/2021/05/jack-dorsey-says-bitcoin-is-climate-friendly-is-he-right.html?utm_source=pocket_mylist (Accessed: 26.07.2021).

**Wright, A. & De Filippi, P.** (2015). *Decentralized Blockchain Technology and the Rise of Lex Cryptographia.* SSRN Scholarly Paper ID 2580664. Rochester, NY: Social Science Research Network.

**Work, A.** (2020). *Crypto RMB: Finance Innovation or New Tool for Control?* Policy Paper. Hong Kong: Global Innovation Hub Friedrich Naumann Foundation for Freedom.

**Work, A.** (2021). *The Rise of e-RMB: Domestic Control, Global Influence.* Taipei: Global Innovation Hub Friedrich Naumann Foundation for Freedom.

**Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S. & Hess, J.** (2008). *The Global Findex Database 2017 Measuring Financial Inclusion and the Fintech Revolution.* Washington D. C.: International Bank for Reconstruction and Development/The World Bank.

**Yilmaz, E. Y.** (2021). *„ERC-20 Token Standard | ethereum.org"*. ethereum.org. Available at: https://ethereum.org/en/developers/docs/standards/tokens/erc-20/ (Accessed: 21.09.2021).

**Yue, F.** (2021). *Tether General Counsel Tells CNBC Audit Is „Months" Away – CoinDesk*, CoinDesk: Bitcoin, Ethereum, Crypto News and Price Data. Available at: https://www.coindesk.com/markets/2021/07/21/tether-general-counsel-tells-cnbc-audit-is-months-away/ (Accessed: 10.09.2021).